DEVOIR N° 2 · 1 MOIS · MARTINS & CIE

Services, supervision et sécurité : PARC01, SECU01 et recette.

Second mois du projet Martins & Cie : monter GLPI 10 et Zabbix sur PARC01, traiter de vrais tickets de support, ouvrir un accès VPN, filtrer la navigation, auditer l'infrastructure depuis SECU01 et faire signer le procès-verbal de recette.

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

1. Semaine 1
   Serveur PARC01 et GLPI 10
   Debian 12, Apache HTTPS, MariaDB, PHP, LDAP
2. Semaine 2
   Gestion de parc et support
   Agents, inventaire, helpdesk, tickets
3. Semaine 3
   Supervision Zabbix
   Agents, modèles, déclencheurs, alertes
4. Semaine 4
   Sécurité et recette finale
   VPN, proxy, SECU01, sauvegardes, PV

Le mois se conclut par la recette complète du cahier des charges (29 tests).

4	12	5	8	29
semaines	missions	tickets à traiter	hôtes supervisés	tests de recette

/20
notation

L'énoncé

i

PRÉAMBULE

Fiche du devoir et consignes

RUBRIQUE	VALEUR
Intitulé	Devoir n° 2 – Services, supervision et sécurité de Martins & Cie
Classe	BTS SIO 1re 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 Martins & Cie v1.0 – chapitres 4, 7, 8, 10, 12, 13 et 14
Point de départ	Instantané `S4-fin` du devoir n° 1 (RFW01, DC01, postes joints au domaine)
Périmètre	Phases 4, 5, 7, 8 et 9 du plan de déploiement : PARC01, SECU01, postes restants, sécurité, recette
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**, instantané en fin de semaine, preuves horodatées rattachées à un test, journal de bord.
- Les comptes par défaut (glpi, tech, normal, post-only, Admin Zabbix, kali, root SSH) sont traités **le jour même** de l'installation.
- SECU01 n'est utilisé que sur l'environnement Martins & Cie, et uniquement pendant la fenêtre d'audit autorisée par écrit (semaine 4). Aucun scan vers Internet ni vers le réseau de l'établissement.

RATTRAPAGE Un binôme dont le socle du devoir n° 1 n'est pas opérationnel reçoit en début de semaine 1 un environnement de référence (RFW01 et DC01 configurés). Le devoir n° 2 reste noté intégralement ; l'usage de cet environnement est simplement mentionné dans le dossier.

CHAPITRE 1

1 Contexte et objectifs

1.1 Mise en situation

Le socle réseau et l'annuaire sont en service. M. Martins souhaite maintenant **maîtriser son parc**, offrir un **support** structuré à ses collaborateurs et **superviser** l'infrastructure. Hervé Nyame, l'expert cybersécurité, doit enfin pouvoir mener un premier audit depuis SECU01. Le mois se termine par la **recette** : M. Martins signera le procès-verbal si les critères d'acceptation du chapitre 12 du CDC sont atteints.

1.2 Objectifs pédagogiques

1. Installer un serveur applicatif Linux (Apache, MariaDB, PHP) en appliquant les bonnes pratiques de sécurité.
2. Déployer GLPI 10 : inventaire automatique, authentification LDAP, gestion des incidents et des demandes.
3. Traiter des tickets de bout en bout selon des niveaux de service définis.
4. Superviser l'infrastructure avec Zabbix et réagir à une alerte.
5. Sécuriser l'accès distant (OpenVPN) et la navigation (proxy, filtrage).
6. Conduire un audit de vulnérabilités encadré et rédiger un rapport.
7. Prononcer une recette et rédiger un dossier d'exploitation.

1.3 Ce qui est attendu à la fin du mois

ÉLÉMENT	ÉTAT ATTENDU
PARC01	Debian 12 durci, Apache en HTTPS, MariaDB locale, GLPI et Zabbix accessibles
GLPI	8 machines inventoriées, utilisateurs importés de l'AD, 5 tickets du scénario traités, base de connaissances
Zabbix	8 hôtes supervisés, déclencheurs et notification, tableau de bord
Postes	4 postes Windows 11 (dont le poste administrateur et WEBDEV01) avec agents GLPI et Zabbix
RFW01	Matrice de flux complète (règles 1 à 10), OpenVPN, proxy et filtrage
SECU01	Kali opérationnel, compte kali désactivé, audit autorisé réalisé et rapporté
Exploitation	Sauvegardes en place, une restauration réussie, PV de recette, dossier d'exploitation

CHAPITRE 2

2 Organisation du travail

2.1 Répartition des rôles

Un étudiant est **technicien support** (GLPI, postes) et l'autre **technicien supervision et sécurité** (Zabbix, RFW01, SECU01). Les rôles s'inversent en semaine 3. En semaine 2, chacun joue aussi le rôle d'**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 cahier des charges complet et votre dossier technique du devoir n° 1.
- Les ISO Debian 12 (netinst) et Kali Linux 2025 ; l'archive GLPI 10 ; l'agent GLPI et l'agent Zabbix pour Windows.
- Un relais SMTP de test fourni par l'enseignant pour les notifications (point 14 du ch. 15) ; à défaut, alertes consultées dans les interfaces.
- Le formulaire d'autorisation d'audit (annexe B), à faire signer par l'enseignant qui joue le rôle de M. Martins.

CHOIX DE VERSIONS Le CDC cite Zabbix 5 et PHP 8.1, que Debian 12 ne fournit pas nativement (point 11 du ch. 15). Vous devez **choisir et justifier** vos versions (par exemple PHP 8.2 natif et Zabbix 7.0 LTS) dans une courte note, après vérification sur les sites des éditeurs de la compatibilité avec GLPI 10.

CHAPITRE 3

3 Calendrier sur quatre semaines

TABLEAU 1 — CALENDRIER DU DEVOIR N° 2

SEMAINE	THÈME	PHASES CDC	JALONS DU POINT D'ÉTAPE
S1	Serveur PARC01 et GLPI 10	4	Note de versions ; GLPI en HTTPS, LDAP, comptes par défaut traités ; T-P05
S2	Gestion de parc et support	5	T-P01, T-P02, T-C01 ; 5 tickets du scénario clos
S3	Supervision Zabbix	4, 7 (partielle)	T-P03, T-P04 ; règles 2 et 6 du tableau 6
S4	Sécurité et recette finale	7, 8, 9	T-R05, T-R06, T-S01 à T-S06 ; PV de recette signé

S1

SEMAINE 1

Serveur PARC01 et GLPI 10

Objectif : un serveur applicatif propre et sécurisé, sur lequel GLPI 10 s'authentifie auprès de l'Active Directory.

M1.1 Installer et durcir PARC01

- Debian 12 sans environnement graphique, nom PARC01, 192.168.10.20/24, passerelle .254, DNS 192.168.10.10, synchronisation horaire sur DC01.
- Créer l'enregistrement DNS parc01.martinscie.lan sur DC01.
- SSH : PermitRootLogin no, authentification par clé pour mbah, sudo pour mbah.
- Pare-feu local (nftables ou ufw) : 22 depuis le poste administrateur, 80/443 et 10051 depuis les VLAN autorisés ; fail2ban ; unattended-upgrades.

M1.2 Monter le socle applicatif

- Apache 2 avec modules ssl, rewrite, headers ; ServerTokens Prod ; certificat (autosigné au minimum) ; redirection HTTP vers HTTPS.
- MariaDB : mysql_secure_installation, bind-address 127.0.0.1, utf8mb4 ; base glpidb et utilisateur dédié aux droits limités à cette base.
- PHP avec les extensions requises par GLPI 10 ; paramètres de production (display_errors Off, date.timezone Europe/Paris).

M1.3 Installer GLPI 10

- Installer GLPI dans /glpi, terminer l'assistant, supprimer install/install.php, sécuriser le répertoire files.
- Changer les mots de passe de glpi, tech, normal et post-only (ou désactiver ceux qui ne servent pas).
- Configurer l'annuaire LDAP vers DC01 (compte de service dédié en lecture), importer les 5 utilisateurs.
- Rédiger la note de choix de versions (PHP, Zabbix).

Jalons du point d'étape

PREUVE ATTENDUE	TEST CDC	VALIDÉ
Connexion SSH de mbah acceptée, root refusé	T-P05	☐
GLPI accessible en https://parc01.martinscie.lan/glpi	EF-P01	☐
Connexion à GLPI avec un compte AD (ex. ldasilva)	EF-P02	☐
Plus aucun avertissement de sécurité sur la page d'accueil de GLPI	T-S04	☐
Règle n° 2 ajoutée sur RFW01 (VLAN 20 → PARC01 en 80/443) ; instantané `S1-fin`	EF-R04	☐

PIÈGE CLASSIQUE Si le compte de service LDAP utilise le compte mbah ou un administrateur du domaine, la note de sécurité est perdue : créez un compte dédié, non privilégié, au mot de passe non expirant mais long et unique.

S2

SEMAINE 2

Gestion de parc et support

Objectif : un parc entièrement inventorié et un helpdesk utilisé dans des conditions réalistes.

M2.1 Compléter le parc

- Installer WEBDEV01 et le poste administrateur (Windows 11 Pro), les joindre au domaine ; installer les RSAT sur le poste administrateur.
- Installer l'agent GLPI sur les 4 postes et sur DC01 ; sur PARC01 et SECU01 (agent Linux) ; RFW01 est saisi à la main ou par SNMP.
- Bonus : déploiement de l'agent par GPO ou script de démarrage.

M2.2 Configurer GLPI

- Entité Martins & Cie ; lieux et groupes GLPI Direction, Secrétariat, Développement web, Administration, Sécurité.
- Profils : mbah Super-Admin et Technicien ; autres comptes Self-Service ; hnyame observateur des tickets de catégorie Sécurité.
- Catégories Incident, Demande, Sécurité ; niveaux de service (prise en compte 4 h ouvrées, résolution 2 jours ouvrés).
- Notifications par courriel (relais SMTP fourni) : création, attribution, résolution.

M2.3 Base de connaissances

- Publier au moins 3 articles pour les utilisateurs : changer son mot de passe, accéder à un dossier partagé, ouvrir un ticket.
- Déposer un raccourci vers le portail GLPI sur le bureau des postes (GPO).

M2.4 Scénario de tickets à traiter

Chaque ticket est ouvert par l'utilisateur concerné (connexion GLPI avec son compte AD), puis pris en charge, suivi et résolu par le technicien. La solution est rédigée de façon à pouvoir devenir un article de la base de connaissances.

TABLEAU 2 — TICKETS DU SCÉNARIO

N°	DEMANDEUR	TYPE	DESCRIPTION	PRIORITÉ ATTENDUE
1	ldasilva	Incident	« Je ne vois plus le lecteur Secrétariat depuis ce matin. » (l'enseignant aura retiré ldasilva d'un groupe)	Haute
2	cgrimeau	Demande	Installation de Visual Studio Code et de Git sur WEBDEV01	Moyenne
3	smartins	Incident	Compte verrouillé après plusieurs essais de mot de passe	Haute
4	hnyame	Sécurité	Le port 22 de PARC01 répond depuis le VLAN 20 : est-ce normal ?	Haute
5	smartins	Demande	Arrivée d'une nouvelle comptable la semaine prochaine : compte, groupe, accès en lecture au dossier Administration	Moyenne

À RÉDIGER Pour le ticket n° 5, produisez la **procédure d'arrivée d'un utilisateur** (compte, groupe métier, groupe d'accès, poste, GLPI). Elle sera reprise dans le dossier d'exploitation.

Jalons du point d'étape

PREUVE ATTENDUE	TEST CDC	VALIDÉ
Les 8 machines dans l'inventaire GLPI avec matériel et logiciels	T-P01	☐
Ticket créé par ldasilva, attribué et clos par mbah, notifications reçues	T-P02	☐
Les 5 tickets du scénario résolus, avec suivis et respect des niveaux de service	EF-P02	☐
Systèmes, ressources et agents des postes conformes au tableau 8 du CDC	T-C01	☐
3 articles de la base de connaissances ; instantané `S2-fin`	–	☐

S3

SEMAINE 3

Supervision Zabbix

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

M3.1 Installer Zabbix

- Installer Zabbix (version justifiée en S1) avec MariaDB : base zabbix et utilisateur dédié ; interface web sous /zabbix en HTTPS.
- Changer le mot de passe du compte Admin ; créer un compte nominatif pour mbah ; authentification LDAP si la version le permet.

M3.2 Superviser les hôtes

- Agent Zabbix sur DC01, PARC01, SECU01 et les 4 postes ; pfSense par SNMP (v2c à communauté non triviale ou v3) ; ping ICMP pour tous.
- Modèles Windows by Zabbix agent, Linux by Zabbix agent, pfSense SNMP, ICMP Ping ; groupes d'hôtes Serveurs et Postes.
- Ajouter les règles n° 2 (10051) et n° 6 (PARC01 → 10050 et 161/UDP) sur RFW01 ; vérifier le pare-feu Windows des hôtes.

M3.3 Alerter et présenter

- Déclencheurs du tableau 16 du CDC : hôte injoignable > 3 min, disque > 85 %, CPU > 90 % pendant 10 min, services DNS, DHCP, AD DS, apache2, mariadb.
- Média courriel pour mbah, action sur les sévérités Haute et Désastre ; bonus : création automatique d'un ticket GLPI.

- Tableau de bord « Martins & Cie » : état des hôtes, problèmes en cours, graphes CPU et mémoire des serveurs.
- Rétention : historique 30 jours, tendances 1 an ; vérifier l'espace disque restant sur PARC01.

Jalons du point d'étape

PREUVE ATTENDUE	TEST CDC	VALIDÉ
8 hôtes disponibles (icône verte), données récentes	T-P03	☐
Arrêt du service DNS sur DC01 : problème levé en moins de 5 minutes, notification reçue, retour à la normale constaté	T-P04	☐
Tableau de bord présenté en démonstration	EF-P03	☐
Règles n° 2 et 6 en place sur RFW01 ; instantané `S3-fin`	EF-R04	☐

POUR ALLER PLUS LOIN Mesurez le temps de détection réel d'une panne (arrêt brutal d'une VM) et comparez-le au délai annoncé par le déclencheur. Expliquez l'écart.

S4 SEMAINE 4

Sécurité, audit et recette

Objectif : fermer les dernières portes, auditer, sauvegarder, puis faire signer la recette.

M4.1 Accès distant et navigation

- OpenVPN sur RFW01 : CA interne, certificat serveur, certificat pour mbah, authentification LDAP, UDP 1194, tunnel 10.8.0.0/24, AES-256-GCM, tls-crypt.
- Règles sur l'interface OpenVPN : mbah vers le VLAN 10 seulement ; règle n° 9 sur le WAN ; redirection de port sur la box si disponible (sinon test depuis le réseau amont).
- Proxy Squid et filtrage d'URL sur le VLAN 20 (règle n° 3) ; liste de catégories bloquées validée par « la direction » (l'enseignant).

M4.2 Audit depuis SECU01

- Installer Kali Linux 2025 (192.168.10.30), créer le compte hnyame, désactiver le compte kali, chiffrer le disque, instantané avant campagne.
- Faire signer l'autorisation d'audit (annexe B) ; activer la règle n° 8 **uniquement** pendant la fenêtre autorisée.

- Scan nmap des VLAN 10 et 20, puis analyse de vulnérabilités de PARC01 et DC01 (OpenVAS / Greenbone).
- Rédiger un rapport d'audit : périmètre, méthode, constats classés par criticité, recommandations, corrections appliquées et vérifiées.

M4.3 Sauvegarder et recetter

- Mettre en place les sauvegardes du tableau 21 : état du système de DC01, partages, dump des bases glpidb et zabbix, config.xml.
- Réaliser une restauration : un fichier d'un partage, un objet AD supprimé, la base GLPI.
- Dérouler l'ensemble du plan de tests (tableau 23 du CDC, 29 tests) et remplir le PV de recette.
- Rédiger le dossier d'exploitation et le guide utilisateur de 2 pages.

Jalons du point d'étape

PREUVE ATTENDUE	TEST CDC	VALIDÉ
Tunnel VPN établi avec mbah, autre compte refusé	T-R05	☐
Page de blocage d'une catégorie interdite, événement journalisé	T-R06	☐
Connexion hnyame sur SECU01, compte kali désactivé	T-S01	☐
Scan nmap autorisé, visible dans les journaux de RFW01, rapport rédigé	T-S02	☐
Aucun mot de passe en clair dans les livrables	T-S03	☐
Comptes par défaut traités (admin, Admin, glpi, kali, root SSH)	T-S04	☐
Restauration d'un fichier, d'un objet AD et de la base GLPI	T-S05	☐
Aucune vulnérabilité critique ou élevée non traitée sur PARC01 et DC01	T-S06	☐
PV de recette signé ; instantané `S4-fin`	–	☐

CADRE LÉGAL Un scan sans autorisation écrite, ou hors du périmètre Martins & Cie, entraîne la note de 0 au critère « Audit » et un signalement. Le fait d'accéder ou de 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, GLPI, Zabbix, VPN, proxy, SECU01, sauvegardes ; 15 à 25 pages hors annexes	PDF
Note de versions	Choix argumenté de PHP et Zabbix (rendue en S1)	PDF
Export GLPI	Liste des 5 tickets du scénario avec suivis et solutions ; articles de la base de connaissances	PDF
Rapport d'audit	Autorisation signée, méthode, constats, recommandations, corrections	PDF
Dossier d'exploitation	Démarrage et arrêt, sauvegarde et restauration, arrivée et départ d'un utilisateur, ajout d'un poste, gestion des droits	PDF
Guide utilisateur	Connexion, dossiers, ticket, VPN (2 pages)	PDF
PV de recette	Les 29 tests du tableau 23 avec résultat, preuve, écarts ; signatures	PDF
Scripts et configurations	Scripts de sauvegarde, config.xml, fichiers de configuration anonymisés	Archive .zip

CHAPITRE 9

9 Évaluation

TABLEAU 4 — GRILLE D'ÉVALUATION

CRITÈRE	ATTENDUS	POINTS
Serveur PARC01	Socle LAMP durci, SSH, pare-feu local, choix de versions justifié	3
GLPI et support	Inventaire complet, LDAP, profils, 5 tickets traités avec qualité, base de connaissances	4
Supervision Zabbix	8 hôtes, déclencheurs pertinents, alerte démontrée, tableau de bord	3
Sécurité réseau	Matrice de flux complète, OpenVPN durci, proxy et filtrage	3
Audit SECU01	Cadre respecté, rapport exploitable, corrections vérifiées	2
Sauvegarde et recette	Restaurations réussies, PV de recette complet et 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 Audit. Retard de rendu : −1 point par jour ouvré.

9.1 Compétences du référentiel mobilisées

BLOC	COMPÉTENCE	OÙ
Bloc 1	Gérer le patrimoine informatique	Inventaire GLPI, choix de 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	Base de connaissances, guide utilisateur, recette
Bloc 2 SISR	Exploiter, dépanner et superviser une solution d'infrastructure réseau	Zabbix, alertes, dossier d'exploitation
Bloc 3	Garantir la disponibilité, l'intégrité et la confidentialité des services	Sauvegardes, restauration, VPN
Bloc 3	Sécuriser les équipements et les usages des utilisateurs	Durcissement, proxy, audit SECU01

A

ANNEXE

Journal de bord

Même modèle que pour le devoir n° 1, à compléter à chaque séance.

MODÈLE DE JOURNAL DE BORD

DATE	ÉTUDIANT	TÂCHES RÉALISÉES	PROBLÈME RENCONTRÉ	SOLUTION / PISTE	TEST VALIDÉ

B

ANNEXE

Autorisation d'audit SECU01

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

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 et 192.168.20.0/24, à l'exclusion 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, accès aux données des dossiers partagés, tout trafic vers Internet
Engagements	Instantané avant campagne, journalisation, rapport remis sous 48 h, signalement immédiat de toute découverte critique
Signatures	Demandeur : ..... Direction : .....

MOIS PRÉCÉDENT
← Devoir n° 1 – Socle réseau et annuaire

PORTAIL SISR1
Rubrique Devoirs →

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