PROJET INTÉGRATEUR BTS

SIO (SISR & SLAM) — CIEL

StadiumCompany — Infrastructure Réseau & Applicative

Cahier des Charges

BTS SIO SISR	BTS SIO SLAM	BTS CIEL
Réseau & Sécurité	Développement Web	Supervision & VPN

1. Contexte du Projet — StadiumCompany

1.1 Présentation de l'Entreprise

StadiumCompany est une entreprise qui gère un grand stade multi-événements. Initialement dotée d'une infrastructure réseau avancée lors de sa construction, l'entreprise a progressivement ajouté des équipements et des connexions sans vision d'ensemble. Cette croissance non maîtrisée a engendré des problèmes de bande passante, de gestion du trafic et de sécurité, limitant la capacité de la société à offrir des services de qualité à ses clients.

Face à ces enjeux, la direction de StadiumCompany a décidé de moderniser son infrastructure informatique. Ne disposant pas de l'expertise nécessaire en interne, elle a fait appel à des experts pour concevoir, déployer et administrer cette nouvelle architecture en plusieurs phases.

1.2 Organisation de l'Entreprise

StadiumCompany emploie 170 personnes à temps plein, réparties comme suit :

- 35 dirigeants et responsables
- 135 employés permanents
- 80 intérimaires pour les événements spéciaux

L'entreprise se compose de 7 services principaux au sein du stade :

Service	Effectif / Équipement	Rôle
Administration	170 collaborateurs	Gestion administrative globale
Équipes	164 collaborateurs	Coordination des équipes opérationnelles
WiFi	100 utilisateurs	Réseaux sans fil internes
Caméra IP	80 caméras	Vidéosurveillance
VIP-Presse	80 collaborateurs	Accueil VIP et relations presse
Fournisseurs	44 collaborateurs	Relations fournisseurs & partenaires
Restaurant	14 collaborateurs	Restauration interne

1.3 Architecture des Sites

L'entreprise dispose de trois sites distincts interconnectés :

- Site 1 — Stade : Site principal hébergeant l'ensemble de l'infrastructure informatique (serveurs, équipements réseau, administration).
- Site 2 — Billetterie : Bureau en centre-ville dédié à la vente de billets, connecté via DSL/VPN.
- Site 3 — Boutique Souvenirs : Point de vente spécialisé, également connecté via DSL/VPN.

Le stade est construit sur deux niveaux reliés par des câbles à fibre optique. Les équipements réseau sont de marque CISCO. Les sites distants (billetterie et boutique) sont connectés via VPN sur liaison DSL.

1.4 Architecture Réseau Cible du Projet

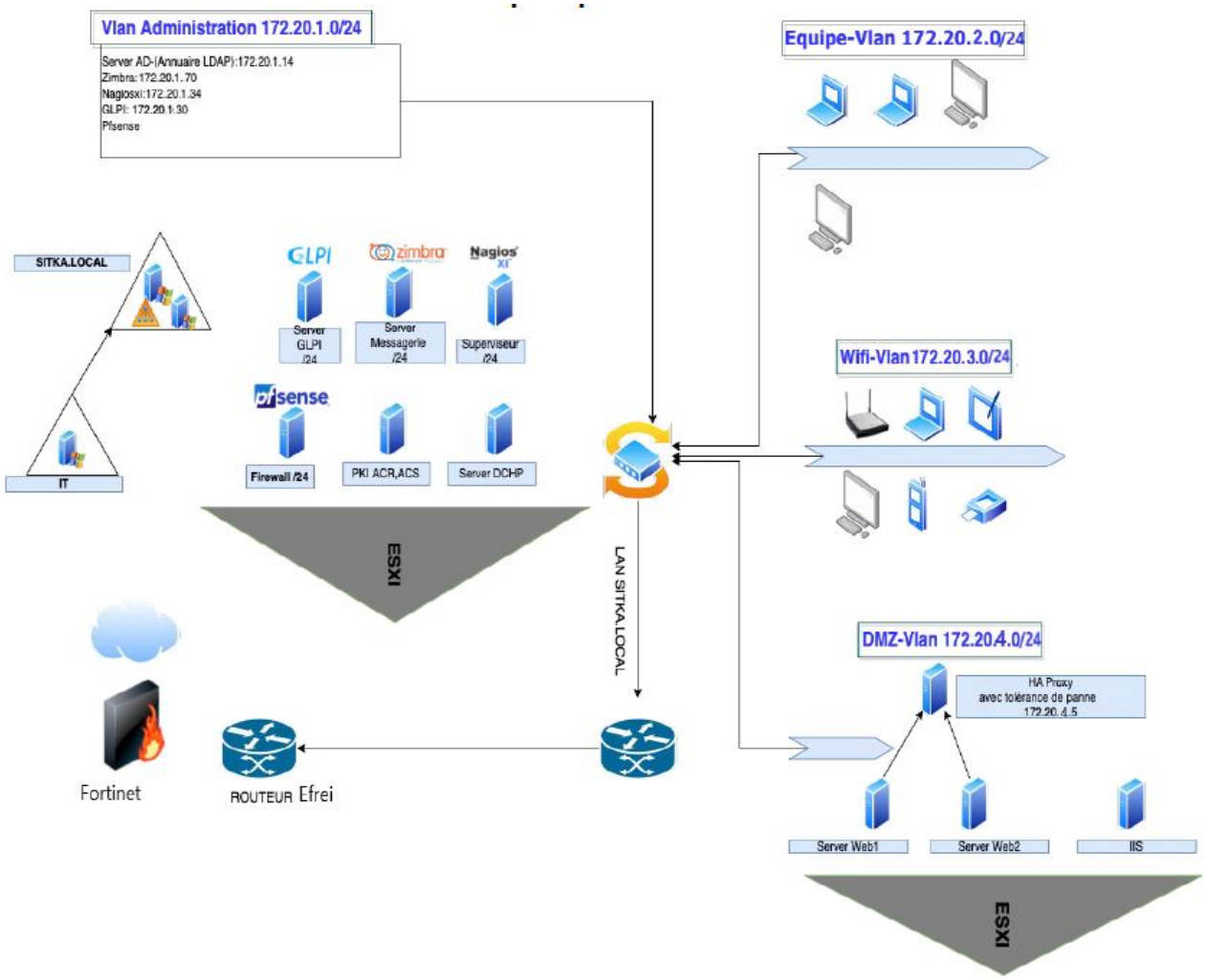
Dans le cadre de ce projet pédagogique, l'infrastructure réseau s'articule autour d'un hyperviseur VMware hébergeant des machines virtuelles segmentées en VLANs gérés par un pare-feu pfSense. L'architecture retenue est la suivante :

VLAN	Réseau	Contenu
VLAN Administration (Serveurs)	172.20.1.0/24	Windows Server AD, GLPI, Serveur Web, BDD, Nagios
VLAN Équipes (Users)	172.20.2.0/24	Postes de travail des employés
VLAN WiFi	172.20.3.0/24	Points d'accès WiFi et terminaux sans fil
DMZ	172.20.4.0/24	Serveurs accessibles depuis Internet (Web, Proxy)

Les adresses clés de l'infrastructure sont :

- Serveur AD (Annuaire LDAP) : 172.20.1.14
- Serveur Zimbra (Messagerie) : 172.20.1.70
- Serveur Nagios (Supervision) : 172.20.1.30
- Serveur GLPI (Helpdesk) : 172.20.1.34
- Pare-feu pfSense : interface de gestion sur le réseau Administration

Schéma infrastructure :



1.5 Rôle de Chaque Filière dans le Projet

Ce projet est conçu pour être réalisé de manière collaborative entre trois filières BTS. Chaque équipe prend en charge un domaine spécifique tout en s'intégrant dans l'architecture commune :

Filière	Domaine	Livrables principaux
BTS SIO SISR	Infrastructure réseau, VLANs pfSense, Active Directory, GLPI	VLANs configurés, AD fonctionnel, GLPI déployé
BTS SIO SLAM	Développement site web StadiumCompany (réservations, services)	Site web hébergé sur VM Linux, BDD MySQL, PHP/HTML/CSS/JS
BTS CIEL	Supervision réseau (Nagios), VPN pfSense pour accès distant	Nagios opérationnel, alertes configurées, VPN actif

PARTIE 1 — BTS SIO SISR : Infrastructure, Réseau & Services

2. Mission BTS SIO SISR — Infrastructure Réseau & Administration

Les étudiants SISR ont la responsabilité de concevoir, déployer et administrer l'ensemble de l'infrastructure réseau et systèmes de StadiumCompany. Leur travail constitue le socle sur lequel toutes les autres missions reposent.

2.1 Objectifs Pédagogiques

- Maîtriser la configuration d'un pare-feu pfSense avec segmentation VLAN
- Déployer et administrer un Active Directory sous Windows Server 2022
- Installer et configurer GLPI comme outil de gestion de parc et helpdesk
- Mettre en place un serveur DHCP et DNS dans un environnement segmenté
- Comprendre les enjeux de sécurité dans une architecture multi-VLAN

2.2 Architecture Réseau à Déployer

2.2.1 Schéma des VLANs

L'infrastructure pfSense doit segmenter le réseau en deux VLANs principaux accessibles depuis l'hyperviseur VMware :

VLAN	Réseau	ID VLAN	Services hébergés
VLAN Serveurs (Administration)	172.20.1.0/24	VLAN 10	AD (172.20.1.14), GLPI (172.20.1.34), Web+BDD SLAM, Nagios CIEL (172.20.1.30)
VLAN Users (Employés)	172.20.2.0/24	VLAN 20	Postes de travail employés — accès à tous les services (AD, GLPI, Web, Supervision)

> *Règle de filtrage inter-VLAN : Les utilisateurs du VLAN Users (172.20.2.0/24) doivent pouvoir accéder à tous les services du VLAN Serveurs. En revanche, les serveurs ne peuvent initier des connexions vers le VLAN Users que pour des réponses légitimes.*

2.2.2 Configuration pfSense

pfSense joue le rôle de firewall et routeur inter-VLAN. Les étudiants SISR doivent réaliser les étapes suivantes :

1. Installer pfSense sur une machine virtuelle avec au moins 3 interfaces réseau (WAN, VLAN Serveurs, VLAN Users).
2. Créer les interfaces VLAN (ID 10 et ID 20).
3. Configurer les règles de firewall inter-VLAN pour autoriser les flux nécessaires (voir tableau des flux).
4. Activer le serveur DHCP pfSense sur le VLAN Users (plage : 172.20.2.50 à 172.20.2.200).
5. Configurer les options DHCP : passerelle = IP pfSense sur VLAN Users, DNS = IP du serveur AD.
6. Configurer le NAT pour permettre aux deux VLANs d'accéder à Internet.

2.2.3 Tableau des flux inter-VLAN

Source	Destination	Ports / Protocoles	Action
VLAN Users	VLAN Serveurs (AD)	TCP 389 (LDAP), 636, 88, 445	**AUTORISER**
VLAN Users	VLAN Serveurs (GLPI)	TCP 80, 443	**AUTORISER**
VLAN Users	VLAN Serveurs (Web SLAM)	TCP 80, 443	**AUTORISER**
VLAN Users	VLAN Serveurs (Nagios)	TCP 80, 443	**AUTORISER**
VLAN Users	Internet	TCP 80, 443, DNS	**AUTORISER**
VLAN Serveurs	Internet	TCP 80, 443, DNS, NTP	**AUTORISER**
VPN Externe (CIEL)	VLAN Serveurs	Tous services admin	**AUTORISER**
Tout autre flux	Inter-VLAN non listé	Tous	**REFUSER**

2.3 Active Directory — Windows Server 2022

2.3.1 Installation et Configuration

Le serveur Active Directory constitue le cœur de l'authentification de toute l'infrastructure. Il est installé sur Windows Server 2022 avec l'adresse IP statique 172.20.1.14 dans le VLAN Serveurs.

Étapes de déploiement :

7. Installer Windows Server 2022 sur une VM — attribuer l'IP 172.20.1.14/24.
8. Promouvoir le serveur en contrôleur de domaine — domaine : stadiumcompany.com.
9. Configurer le rôle DNS sur ce serveur (zone directe : stadiumcompany.com, zone inverse : 172.20.x).
10. Configurer le rôle DHCP pour le VLAN Serveurs (adresses fixes sur serveurs).

2.3.2 Structure des Unités Organisationnelles (OU)

La structure de l'annuaire doit refléter l'organisation de StadiumCompany. Créer les OU suivantes :

- OU=StadiumCompany > OU=Services > OU=Administration
- OU=StadiumCompany > OU=Services > OU=Equipes
- OU=StadiumCompany > OU=Services > OU=WiFi
- OU=StadiumCompany > OU=Services > OU=VIP-Presse
- OU=StadiumCompany > OU=Services > OU=Fournisseurs
- OU=StadiumCompany > OU=Services > OU=Restaurant

- OU=StadiumCompany > OU=Groupes
- OU=StadiumCompany > OU=Serveurs

2.3.3 Gestion des Utilisateurs et Groupes

Convention de nommage des comptes utilisateurs :

- Login : première lettre du prénom + nom de famille (ex : jdupont pour Jean Dupont)
- En cas de doublon : ajout d'un chiffre de 1 à 10 (ex : jdupont1, jdupont2)
- Chaque utilisateur dispose d'un dossier personnel et d'un profil centralisé

Groupes à créer (format G_xxxx) :

- G_Administration — groupe des employés du service Administration
- G_Equipes — groupe des membres des équipes sportives
- G_WiFi — groupe des gestionnaires WiFi
- G_VIP_Presse — groupe VIP et presse
- G_Fournisseurs — groupe fournisseurs
- G_Restaurant — groupe restaurant
- GP_Admin — groupe des administrateurs IT (privilèges élevés)

2.3.4 GPO — Politiques de Groupe

Configurer les GPO suivantes :

11. Politique de complexité des mots de passe (domaine) : longueur minimum 8 caractères, complexité activée, expiration 90 jours.
12. Redirection des dossiers utilisateurs vers le serveur de fichiers.
13. Déploiement du client GLPI sur les postes de travail.
14. Configuration des proxys et des pages d'accueil navigateur pointant vers le site StadiumCompany (SLAM).

2.4 GLPI — Gestion du Parc & Helpdesk

2.4.1 Présentation de GLPI

GLPI (Gestionnaire Libre de Parc Informatique) est un outil open source de gestion de parc informatique et de helpdesk. Il sera installé sur une VM Linux Debian dans le VLAN Serveurs (IP : 172.20.1.34).

2.4.2 Installation

Prérequis techniques :

- Système : Debian 12 ou Ubuntu Server 22.04 LTS
- Pile LAMP : Apache2, MySQL/MariaDB, PHP 8.1+
- GLPI version stable la plus récente

Étapes d'installation :

15. Préparer la VM Linux avec IP statique 172.20.1.34/24, passerelle = IP pfSense.
16. Installer Apache2, MariaDB, PHP et les extensions requises (php-ldap, php-curl, php-gd...).
17. Télécharger GLPI depuis glpi-project.org et déployer dans /var/www/html/glpi.
18. Créer la base de données MySQL et l'utilisateur dédié GLPI.
19. Finaliser l'installation via l'interface web (http://172.20.1.34/glpi).

2.4.3 Configuration et Synchronisation Active Directory

La synchronisation AD/LDAP est indispensable pour que les utilisateurs se connectent à GLPI avec leurs identifiants du domaine stadiumcompany.com. Configuration :

20. Dans GLPI > Configuration > Authentification > Annuaire LDAP, ajouter le serveur AD.
21. Renseigner : Hôte = 172.20.1.14, Port = 389 (ou 636 pour LDAPS), BaseDN = DC=stadiumcompany,DC=com.
22. Tester la connexion et importer les utilisateurs et groupes.
23. Configurer les profils GLPI selon les groupes AD (G_xxxx → profil Self-Service, GP_Admin → profil Admin).

2.4.4 Configuration du Helpdesk

Paramètres à configurer :

- Catégories de tickets : Matériel, Logiciel, Réseau, Accès, Autre
- File de tickets par service (Administration, Équipes, Restaurant, etc.)
- Notifications automatiques par email lors de création/mise à jour de ticket
- Collecteur d'emails : support@stadiumcompany.com → création automatique de tickets
- Niveaux d'escalade et SLA (délais de résolution par priorité)

2.4.5 Déploiement de l'Agent Inventaire

L'agent GLPI (FusionInventory ou GLPI Agent) doit être déployé sur tous les postes du VLAN Users via GPO. Il remonte automatiquement :

- L'inventaire matériel (processeur, RAM, disques, cartes réseau)
- Les logiciels installés et leurs versions
- Les mises à jour Windows disponibles

2.5 Plan de Travail et Documents à Produire

Documents à produire	Documents à produire (suite)
Dossier de choix des solutions (AD, GLPI)	Procédure de création d'utilisateurs AD
Schéma réseau détaillé avec adressage IP	Documentation des GPO appliquées

Rapport d'installation pfSense + VLANs	Guide d'utilisation GLPI pour les employés
Rapport d'installation Windows Server + AD	Tests et validation des flux inter-VLAN
Rapport d'installation et config GLPI	Bilan de projet SISR

PARTIE 2 — BTS SIO SLAM : Développement Web StadiumCompany

3. Mission BTS SIO SLAM — Site Web StadiumCompany

Les étudiants SLAM ont la responsabilité de concevoir et développer le site web officiel de StadiumCompany, hébergé dans le VLAN Serveurs. Ce site doit proposer l'ensemble des services numériques de l'entreprise : présentation, réservations, billetterie, gestion des événements et espace collaborateur.

3.1 Objectifs Pédagogiques

- Concevoir et structurer un projet web multi-pages avec une architecture claire (MVC ou équivalent)
- Maîtriser le développement front-end : HTML5, CSS3, JavaScript moderne (ES6+)
- Développer les fonctionnalités back-end en PHP (PDO, sessions, sécurité)
- Concevoir et administrer une base de données MySQL/MariaDB
- Déployer un serveur web Apache sur Linux (VLAN Serveurs)
- Intégrer l'authentification via l'Active Directory (LDAP) déployé par les SISR

3.2 Infrastructure Technique

3.2.1 Serveur d'Hébergement

Le site web est hébergé sur une VM Linux dédiée dans le VLAN Serveurs :

- Système d'exploitation : Debian 12 ou Ubuntu Server 22.04 LTS
- Adresse IP statique : 172.20.1.50/24 (dans le VLAN Administration)
- Serveur web : Apache2 avec mod_rewrite et mod_ssl activés
- PHP 8.1+ avec extensions : php-pdo, php-mysql, php-ldap, php-gd, php-curl, php-mbstring
- Base de données : MariaDB 10.x sur la même VM (ou VM séparée selon la complexité)

> *Le site web doit être accessible depuis le VLAN Users (172.20.2.0/24) et depuis Internet via la DMZ. Les règles pfSense permettent ce double accès (les SISR configurent ces règles sur indication des SLAM).*

3.2.2 Stack Technique

Couche	Technologie	Usage
Front-end	HTML5, CSS3, JavaScript ES6+	Structure, style et interactivité des pages
Framework CSS	Bootstrap 5 ou Tailwind CSS	Responsive design, composants UI
JavaScript	Vanilla JS + Fetch API / jQuery	Dynamisme, appels AJAX, validations
Back-end	PHP 8.1+	Logique métier, traitement des formulaires
Base de données	MariaDB / MySQL	Stockage des réservations, événements, users
Authentification	PHP LDAP + Sessions	Connexion via AD stadiumcompany.com
Serveur	Apache2 sur Linux Debian	Hébergement du site dans le VLAN Serveurs
Sécurité	HTTPS (SSL auto-signé), PDO, XSS/CSRF	Protection des données et des formulaires

3.3 Structure du Site Web

3.3.1 Pages Publiques (accessibles sans connexion)

Les pages publiques constituent la vitrine de StadiumCompany. Elles sont accessibles depuis Internet.

- Page d'Accueil (index.php) — Présentation générale du stade, actualités, événements à venir, photos, vidéos de présentation. Bannière dynamique avec diaporama JavaScript.
- À Propos — Histoire de StadiumCompany, chiffres clés (170 employés, capacité du stade), valeurs, organigramme des services.
- Événements — Calendrier des matchs et concerts à venir. Filtres par catégorie (sport, musique, spectacle). Affichage des disponibilités en temps réel depuis la base de données.
- Billetterie Publique — Consultation des places disponibles, tarifs, catégories (Pelouse, Tribune, VIP, Loge). Panier de réservation et paiement simulé.
- Restauration — Présentation du restaurant de luxe du stade, menus, galerie photos, formulaire de réservation de table.
- Boutique Souvenirs — Catalogue des articles disponibles, accès à la boutique en ligne (avec ou sans compte).
- Contact — Formulaire de contact, plan d'accès, adresses des trois sites (Stade, Billetterie, Boutique), coordonnées.
- Mentions Légales et CGU

3.3.2 Espace Privé — Authentification via AD

L'espace privé est accessible aux employés et administrateurs via leurs identifiants Active Directory. La connexion se fait par PHP LDAP sur le serveur AD (172.20.1.14).

- Page de Connexion (login.php) — Formulaire login/mot de passe avec authentification LDAP. Gestion des erreurs (compte inexistant, mot de passe incorrect, compte verrouillé). Redirection vers le tableau de bord selon le profil.
- Tableau de Bord Employé — Vue personnalisée selon le service (Administration, Équipes, VIP, etc.). Accès rapide aux services internes.
- Gestion des Réservations (Admin) — Interface CRUD pour gérer les événements, les créneaux de réservation, les places disponibles. Visualisation statistique (graphiques JavaScript — Chart.js).
- Gestion des Utilisateurs (Admin) — Consultation de l'annuaire AD synchronisé. Attribution de rôles et permissions sur le site.
- Espace VIP / Presse — Accès aux accréditations, demandes de passes presse, programme VIP personnalisé.
- Gestion Concessions et Fournisseurs — Espace dédié pour les fournisseurs (commandes, factures, planning d'intervention).

3.4 Base de Données — Modèle de Données

3.4.1 Tables Principales

Le modèle de données doit couvrir l'ensemble des fonctionnalités du site. Voici les tables à concevoir :

Table	Champs principaux	Description
evenements	id, titre, type, date_debut, date_fin, capacite, statut	Matchs, concerts, spectacles organisés au stade
categories_evenement	id, nom, couleur, icone	Sport, Musique, Spectacle, Autre
places	id, id_evenement, categorie, numero, prix, statut	Places disponibles par événement (Pelouse, Tribune, VIP, Loge)
reservations	id, id_user, id_evenement, id_place, date_resa, statut, montant	Réservations effectuées par les visiteurs
utilisateurs_web	id, login_ad, email, prenom, nom, service, role, date_creation	Comptes web synchronisés depuis l'AD
reservations_restaurant	id, nom_client, email, date, nb_couverts, commentaire, statut	Réservations de tables au restaurant
articles_boutique	id, nom, description, prix, stock, photo, categorie	Articles disponibles en boutique
commandes	id, id_user, date_commande, montant_total, statut	Commandes de la boutique en ligne
actualites	id, titre, contenu, photo, date_publication, auteur, visible	Articles et news du site
contacts	id, nom, email, sujet, message, date, traite	Messages du formulaire de contact

3.5 Fonctionnalités Techniques Détaillées

3.5.1 Authentification LDAP

L'authentification des employés doit utiliser le protocole LDAP pour se connecter à l'Active Directory déployé par les SISR. Exemple de code PHP :

```
// Connexion LDAP à l'AD StadiumCompany $ldap = ldap_connect('172.20.1.14', 389);
ldap_set_option($ldap, LDAP_OPT_PROTOCOL_VERSION, 3); $bind = ldap_bind($ldap, $login .
```

```
'@stadiumcompany.com', $password); if ($bind) { /* Authentification réussie — démarrer la session */ }
```

3.5.2 Système de Réservation

Le module de réservation de billets est la fonctionnalité centrale du site. Il doit :

24. Afficher les événements disponibles avec leur plan de salle (représentation visuelle des zones).
25. Permettre la sélection de places avec vérification en temps réel de la disponibilité (AJAX + PHP).
26. Gérer un panier temporaire en session PHP.
27. Générer une confirmation de réservation avec un numéro unique et un QR code (bibliothèque PHP QR Code).
28. Envoyer un email de confirmation (PHP mailer ou mail() natif).

3.5.3 Interface Administration (Back-office)

L'interface d'administration doit être sécurisée (accessible uniquement aux membres du groupe GP_Admin de l'AD) et permettre :

- Création / modification / suppression d'événements avec upload de photos
- Gestion des places et des tarifs par événement
- Visualisation des réservations avec filtres et exports CSV/PDF
- Gestion du contenu du site (actualités, pages statiques)
- Statistiques et graphiques de fréquentation (Chart.js)
- Gestion des messages de contact reçus

3.5.4 Design et Ergonomie

Le design du site doit refléter l'identité professionnelle et dynamique d'un stade modern. Exigences :

- Responsive Design : le site doit s'adapter aux mobiles, tablettes et écrans larges (Bootstrap 5 ou CSS Grid + Flexbox).
- Charte graphique cohérente : couleurs principales du stade, logo, typographie professionnelle (Google Fonts).
- Accessibilité : contrastes suffisants, attributs alt sur les images, navigation au clavier.
- Performance : images optimisées, lazy loading, minification CSS/JS.
- Animations CSS3 : transitions fluides, effets de survol, reveal au scroll (Intersection Observer API).

3.5.5 Sécurité Back-end

Mesures de sécurité obligatoires à implémenter :

- Utilisation exclusive de PDO avec requêtes préparées (protection injection SQL)
- Validation et sanitisation de toutes les entrées utilisateur (htmlspecialchars, filter_input)
- Tokens CSRF sur tous les formulaires
- Protection contre les attaques XSS (en-têtes Content-Security-Policy)
- Sessions PHP sécurisées (session_regenerate_id, httponly, secure cookies)
- Hashage des mots de passe locaux avec password_hash() / password_verify()

3.6 Livrables et Documents à Produire

- Maquettes filaires (wireframes) de toutes les pages — outil au choix (Figma, draw.io...)
- Modèle Conceptuel de Données (MCD) et Modèle Physique de Données (MPD)
- Dictionnaire des données (description de toutes les tables et champs)
- Spécifications fonctionnelles détaillées
- Code source complet versionné (Git recommandé)
- Script SQL de création de la base de données avec données de test
- Documentation technique d'installation et déploiement du serveur web
- Manuel utilisateur (guide de navigation et d'utilisation du site)
- Rapport de tests (tests fonctionnels, tests de sécurité, tests de compatibilité)

PARTIE 3 — BTS CIEL : Supervision Réseau & VPN

4. Mission BTS CIEL — Supervision & Accès Distant Sécurisé

Les étudiants CIEL ont la responsabilité de mettre en place la supervision de l'ensemble de l'infrastructure réseau et systèmes de StadiumCompany, ainsi qu'une solution VPN pour permettre l'accès distant sécurisé aux ressources internes de l'entreprise.

4.1 Objectifs Pédagogiques

- Installer et configurer une solution de supervision open source (Nagios XI ou Nagios Core)
- Maîtriser les protocoles de supervision : SNMP, ICMP, TCP port checks
- Configurer la surveillance des serveurs Windows et Linux (agents NRPE/NSClient++)
- Intégrer Nagios avec Active Directory / LDAP pour l'authentification
- Mettre en place des alertes automatiques (email, SMS)
- Configurer un VPN OpenVPN sur pfSense pour les accès externes
- Documenter une infrastructure de supervision complète

4.2 Mission 1 — Supervision avec Nagios

4.2.1 Présentation de la Solution

Nagios est la solution de supervision open source retenue par StadiumCompany. Il sera installé sur une VM Linux dans le VLAN Serveurs à l'adresse 172.20.1.30, accessible depuis le VLAN Users et via le VPN.

> *Nagios XI (version commerciale avec interface graphique avancée) ou Nagios Core (version open source avec interface classique) peuvent être utilisés. Nagios XI est recommandé pour sa facilité d'administration et son intégration LDAP native.*

4.2.2 Installation de Nagios

Prérequis serveur Nagios :

- VM Linux : Debian 12 ou CentOS/Rocky Linux
- IP statique : 172.20.1.30/24, passerelle = IP pfSense
- RAM minimum : 2 Go, Disque : 20 Go
- Accès Internet pour les téléchargements initiaux

Étapes d'installation Nagios Core :

29. Installer les prérequis : Apache2, PHP, GCC, Make, OpenSSL.
30. Créer l'utilisateur et le groupe nagios (et nagcmd pour les commandes externes).
31. Télécharger et compiler Nagios Core depuis les sources officielles (nagios.org).
32. Installer les plugins Nagios (nagios-plugins) pour disposer des checks standards.

33. Configurer Apache pour l'accès à l'interface web Nagios (http://172.20.1.30/nagios).
34. Démarrer les services Nagios et Apache, activer le démarrage automatique.

4.2.3 Éléments à Superviser

Nagios doit surveiller l'ensemble des éléments actifs de l'infrastructure :

Élément	IP / Adresse	Services / Métriques supervisés
pfSense (Firewall)	172.20.1.1	Ping, SNMP (CPU, RAM, interfaces réseau, trafic)
Serveur AD (Win Server 2022)	172.20.1.14	Ping, DNS (TCP 53), LDAP (TCP 389), CPU, RAM, disque (NSClient++)
Serveur GLPI (Linux)	172.20.1.34	Ping, HTTP (TCP 80/443), MySQL (TCP 3306), CPU, RAM, disque (NRPE)
Serveur Web SLAM (Linux)	172.20.1.50	Ping, HTTP (TCP 80/443), Apache, CPU, RAM, disque (NRPE)
Routeur Cisco (Stade)	172.20.x.x	Ping, SNMP (interfaces, trafic, erreurs)
Switchs Cisco	172.20.x.x	Ping, SNMP (ports, VLAN, état des interfaces)
Site Billetterie (distant)	IP DSL	Ping VPN, disponibilité du lien
Site Boutique (distant)	IP DSL	Ping VPN, disponibilité du lien
Imprimantes réseau	172.20.x.x	SNMP (état, niveaux d'encre, papier)

4.2.4 Configuration des Agents

Pour superviser les serveurs de manière détaillée (CPU, RAM, disque, processus), des agents doivent être installés sur chaque machine :

- Serveurs Linux (GLPI, Web SLAM, Nagios lui-même) : installer l'agent NRPE (Nagios Remote Plugin Executor). Configuration dans /etc/nagios/nrpe.cfg pour autoriser les connexions depuis le serveur Nagios.
- Serveur Windows (AD Windows Server 2022) : installer NSClient++ (ncpa.cfg). Configurer les modules check_cpu, check_memory, check_drivesize, check_service.
- Équipements Cisco (routeurs, switchs) : activer SNMP v2c ou v3 sur chaque équipement. Configurer la community string et les OIDs à surveiller.

Checks à configurer par service supervisé :

- check_ping : vérification de la disponibilité réseau (latence, perte de paquets)
- check_http / check_https : vérification des services web (site SLAM, GLPI, Nagios)
- check_dns : vérification du serveur DNS sur l'AD
- check_ldap : vérification du service LDAP de l'Active Directory
- check_mysql : vérification de la base de données MariaDB (GLPI, site SLAM)
- check_disk / check_nrpe!check_disk : surveillance de l'espace disque
- check_load / check_cpu : surveillance de la charge processeur
- check_mem : surveillance de la mémoire disponible

4.2.5 Intégration Nagios avec Active Directory (LDAP)

L'intégration AD/LDAP permet aux employés de s'authentifier sur l'interface Nagios avec leurs identifiants du domaine stadiumcompany.com. Configuration :

35. Installer le module d'authentification LDAP pour Nagios (mod_authnz_ldap pour Apache).
36. Modifier la configuration Apache de Nagios pour utiliser l'authentification LDAP :

> *AuthType Basic AuthName "StadiumCompany — Nagios" AuthBasicProvider ldap AuthLDAPURL ldap://172.20.1.14:389/DC=stadiumcompany,DC=com AuthLDAPBindDN "CN=nagios_service,OU=Services,DC=stadiumcompany,DC=com" Require ldap-group CN=GP_Admin,OU=Groupes,DC=stadiumcompany,DC=com*

37. Créer un compte de service AD dédié à Nagios (nagios_service) avec droits en lecture sur l'annuaire.
38. Tester l'authentification en se connectant à http://172.20.1.30/nagios avec un compte du domaine.

4.2.6 Configuration des Alertes

Nagios doit notifier automatiquement les administrateurs en cas d'incident. Configuration des notifications :

- Contacts : créer les contacts administrateurs avec leur adresse email (adresses du domaine @stadiumcompany.com).
- Groupes de contacts : G_Admin_Nagios regroupant tous les administrateurs à notifier.
- Périodes de notification : 24h/24, 7j/7 pour les serveurs critiques (AD, pfSense).
- Seuils d'alerte : WARNING à 80% d'utilisation CPU/RAM, CRITICAL à 95%.
- Notification par email : configurer Postfix ou un relais SMTP pour l'envoi des emails d'alerte.
- Escalade : si un problème persiste plus de 30 minutes, escalade vers le responsable IT.

4.2.7 Rapports et Tableaux de Bord

Configurer les fonctionnalités de reporting de Nagios :

- Rapports de disponibilité mensuels par hôte et par service (pourcentage de temps en ligne).
- Graphiques de performance : évolution de la charge CPU, RAM, trafic réseau dans le temps (PNP4Nagios ou Nagiosgraph pour la génération de graphes RRD).
- Cartographie réseau : créer une vue topologique de l'infrastructure dans l'interface Nagios (module Network Map).
- Rapport d'incidents : historique des alertes, temps de résolution, tendances.

4.3 Mission 2 — VPN OpenVPN via pfSense

4.3.1 Objectif

Le VPN permet aux utilisateurs externes (administrateurs, télétravailleurs, sites distants) d'accéder de manière sécurisée aux ressources internes du réseau StadiumCompany comme s'ils étaient physiquement présents dans l'entreprise.

> *Les VPN inter-sites (Stade ↔ Billetterie et Stade ↔ Boutique) sont déjà décrits dans l'architecture globale. La mission CIEL se concentre sur le VPN d'accès distant (Remote Access VPN) pour les administrateurs et télétravailleurs.*

4.3.2 Configuration OpenVPN sur pfSense

pfSense intègre nativement OpenVPN. Les étudiants CIEL doivent configurer :

39. Créer une Autorité de Certification (CA) interne dans pfSense (Système > Gestionnaire de certificats > CA).
40. Créer un certificat serveur signé par cette CA pour le serveur OpenVPN.
41. Créer le serveur OpenVPN (VPN > OpenVPN > Serveurs) avec les paramètres :
    - Mode : Remote Access (SSL/TLS + User Auth)
    - Protocole : UDP sur le port 1194
    - Réseau tunnel : 10.8.0.0/24 (plage d'adresses pour les clients VPN)
    - Réseau local : 172.20.1.0/24, 172.20.2.0/24 (VLANs internes accessibles)
    - Chiffrement : AES-256-GCM, authentification SHA256
    - DNS push : IP du serveur AD (172.20.1.14) pour la résolution du domaine
42. Créer les règles de firewall pfSense pour autoriser le trafic VPN entrant (WAN vers port 1194/UDP) et le trafic des clients VPN vers les VLANs internes.
43. Créer les comptes utilisateurs VPN dans pfSense (ou intégrer avec l'AD via RADIUS/LDAP).
44. Exporter le fichier de configuration client (.ovpn) avec le paquet pfSense OpenVPN Client Export.
45. Tester la connexion depuis un poste externe avec le client OpenVPN officiel.

4.3.3 Intégration VPN avec l'Active Directory

Pour une gestion centralisée des accès VPN, configurer l'authentification via l'AD StadiumCompany :

46. Installer et configurer un serveur RADIUS (FreeRADIUS) sur une VM dans le VLAN Serveurs, ou utiliser Windows NPS (Network Policy Server) sur le serveur AD.
47. Configurer pfSense pour utiliser ce serveur RADIUS comme backend d'authentification OpenVPN.
48. Créer un groupe AD dédié (ex: G_VPN_Users) pour contrôler quels utilisateurs ont accès au VPN.
49. Tester l'authentification : un membre de G_VPN_Users doit pouvoir se connecter au VPN, un non-membre doit être refusé.

4.3.4 Vérification et Tests

Tests obligatoires à documenter :

- Connexion VPN depuis un poste externe (VM avec IP dans un autre réseau) et vérification de l'IP tunnel attribuée (10.8.0.x).
- Accès à l'interface Nagios (http://172.20.1.30/nagios) depuis le client VPN.
- Accès au serveur AD (ping 172.20.1.14) et à GLPI depuis le client VPN.
- Vérification que le client VPN ne peut pas accéder aux ressources internes sans être connecté au VPN.
- Test de déconnexion VPN et vérification des logs pfSense.

4.4 Plan de Travail et Documents à Produire

Documents à produire	Documents à produire (suite)
Procédure d'installation Nagios Core/XI	Documentation des alertes et contacts Nagios
Procédure d'installation des plugins Nagios	Procédure de configuration OpenVPN sur pfSense
Rapport de configuration des agents NRPE/NSClient++	Guide de connexion VPN pour les utilisateurs

Configuration SNMP sur les équipements Cisco	Rapport de tests VPN (captures d'écran)
Rapport d'intégration Nagios + AD/LDAP	Bilan de projet CIEL

5. Coordination et Points d'Intégration entre Filières

Ce projet repose sur une collaboration étroite entre les trois filières. Chaque équipe dépend des livrables des autres. Le tableau ci-dessous récapitule les points d'intégration critiques :

Besoin	Qui en a besoin	Qui le fournit	Priorité
IP et accès au serveur AD (172.20.1.14)	SLAM (auth LDAP), CIEL (Nagios LDAP, VPN RADIUS)	SISR	**HAUTE**
VLANs pfSense opérationnels	SLAM (accès serveur web), CIEL (accès Nagios, VPN)	SISR	**HAUTE**
Règles firewall pour le site web	SLAM (accès depuis VLAN Users et Internet)	SISR	**HAUTE**
Règles firewall pour Nagios	CIEL (accès interface depuis VLAN Users et VPN)	SISR	**HAUTE**
Compte de service AD pour Nagios	CIEL (intégration LDAP Nagios)	SISR	**MOYENNE**
Compte de service AD pour GLPI	SISR (synchro LDAP GLPI)	SISR	**MOYENNE**
IP et URL du site web	CIEL (supervision HTTP du site)	SLAM	**MOYENNE**
IP et accès à la VM Linux	CIEL (installation agent NRPE)	SLAM	**MOYENNE**
Config VPN pour test accès distant	SLAM (test site depuis VPN)	CIEL	**BASSE**
Alertes Nagios pour tous les services	SISR + SLAM (savoir si leurs serveurs tombent)	CIEL	**BASSE**

> *Recommandation : Organiser une réunion de lancement commune entre les trois équipes pour établir un calendrier de livraisons partielles. Les SISR doivent livrer l'AD et les VLANs en premier, car tous les autres dépendent de cette infrastructure.*

5.1 Ordre de Déploiement Recommandé

50. SISR — Semaine 1-2 : Installation pfSense, création des VLANs 10 et 20, règles de base.
51. SISR — Semaine 2-3 : Installation Windows Server 2022, promotion contrôleur de domaine, création des comptes de service.
52. SLAM & CIEL — Semaine 3 : Démarrage possible une fois les VLANs et l'AD opérationnels.
53. SLAM — Semaine 3-6 : Développement du site web en parallèle, déploiement de la VM Apache.
54. CIEL — Semaine 3-5 : Installation Nagios et configuration des premiers checks, démarrage VPN.
55. SISR — Semaine 4-5 : Installation et configuration GLPI, synchronisation AD.
56. Tous — Semaine 6-7 : Tests d'intégration croisés, corrections, documentation.
57. Tous — Semaine 8 : Présentation finale et démonstration du projet complet.

6. Critères d'Évaluation

6.1 SISR — Grille d'Évaluation

Critère	Pondération	Indicateurs de réussite
Configuration pfSense / VLANs	25%	VLANs opérationnels, flux inter-VLAN conformes aux règles
Active Directory	25%	AD fonctionnel, OU et GPO configurées, authentification OK
GLPI	25%	GLPI installé, synchro AD, helpdesk configuré, agent déployé
Documentation	15%	Rapports complets, schémas réseau, procédures claires
Tests et validation	10%	Tests documentés, captures d'écran, résultats conformes

6.2 SLAM — Grille d'Évaluation

Critère	Pondération	Indicateurs de réussite
Qualité du code PHP/SQL	25%	Code propre, requêtes préparées PDO, architecture MVC
Front-end HTML/CSS/JS	20%	Design professionnel, responsive, animations, ergonomie
Fonctionnalités	25%	Réservations, auth LDAP, back-office, toutes pages opérationnelles
Sécurité	15%	CSRF, XSS, injection SQL protégés, HTTPS
Documentation	15%	MCD, MPD, specs fonctionnelles, guide utilisateur

6.3 CIEL — Grille d'Évaluation

Critère	Pondération	Indicateurs de réussite
Installation Nagios	25%	Nagios opérationnel, interface accessible, agents installés
Supervision des éléments	25%	Tous les hôtes et services supervisés, checks configurés
Intégration LDAP / AD	15%	Authentification Nagios via AD fonctionnelle
VPN OpenVPN	20%	VPN opérationnel, accès distant aux ressources internes validé

Alertes et documentation	15%	Alertes email configurées, procédures rédigées, tests OK