Projet StadiumCompany - Spécifications Techniques

Référence : Épreuve E6 - Administration des systèmes et des réseaux (SISR) - Session 2026

Date : 12 février 2026

1. Le Contexte

Ce document constitue le cahier des charges pour la modernisation de l'infrastructure des systèmes et réseaux de l'entreprise StadiumCompany. Il est spécifiquement conçu pour servir de support aux réalisations professionnelles dans le cadre de l'épreuve E6 du BTS SIO, option SISR.

Mission Générale

En tant que technicien supérieur en administration des systèmes et des réseaux, vous intégrez l'équipe de la Direction des Systèmes d'Information (DSI) de StadiumCompany. Votre mission principale est de prendre en charge la refonte, la sécurisation et la supervision de l'ensemble de l'infrastructure informatique. Vous devrez concevoir, déployer et maintenir des solutions robustes, sécurisées et hautement disponibles pour répondre aux nouveaux enjeux de l'entreprise.

Objectifs Pédagogiques

Ce projet vise à évaluer votre capacité à mobiliser les compétences du bloc "Administration des systèmes et des réseaux" :

- **Concevoir une solution d'infrastructure réseau :** Analyser les besoins, proposer une architecture (plan d'adressage, VLANs, DMZ), et justifier les choix techniques.
- **Installer, tester et déployer une solution d'infrastructure réseau :** Mettre en œuvre des services systèmes (AD, DNS, DHCP), des équipements d'interconnexion (routeurs, commutateurs Cisco), et des solutions de sécurité (pare-feu, VPN).
- **Exploiter, dépanner et superviser une solution d'infrastructure réseau :** Mettre en place des outils de supervision (Nagios XI), de gestion de parc (GLPI), de sécurité (SIEM), et assurer la continuité de service (redondance, sauvegarde).

Livrables Attendus

À l'issue du projet, vous devrez fournir un ensemble de documents et de configurations techniques démontrant la réalisation des missions, notamment :

- Schémas d'architecture réseau (logique et physique).
- Documentation technique complète (configurations des équipements, procédures d'installation et d'administration).

- Rapports de tests (validation des services, tests de panne, tests de sécurité).
- Guides utilisateurs pour les services déployés (Helpdesk, connexion Wi-Fi).
- Accès fonctionnels aux plateformes de gestion (GLPI, Nagios XI, SIEM).

2. Le Cahier des Charges Général

StadiumCompany gère un grand stade dont le réseau de communication, initialement performant, a subi des ajouts successifs non planifiés. Cette croissance organique a engendré des problèmes de performance, de gestion du trafic et de sécurité, limitant la capacité de l'entreprise à offrir des services de qualité et à organiser de nouveaux types d'événements comme des concerts.

L'entreprise emploie 170 personnes à temps plein et fait appel à 80 intérimaires lors des événements. Elle est répartie sur trois sites :

- **Le Stade :** Site principal abritant le siège social, le centre administratif et l'hébergement de l'infrastructure informatique.
- **La Billetterie :** Site distant en centre-ville, dédié à la vente de billets.
- **Le Magasin :** Site distant pour la vente de produits dérivés.

La direction a décidé de lancer un projet de modernisation complet de son système d'information avec les objectifs suivants :

- **Restructurer et segmenter** le réseau pour isoler les services et améliorer la sécurité.
- **Centraliser l'administration** des utilisateurs et des ressources via un annuaire d'entreprise.
- **Garantir la haute disponibilité** des services critiques par la mise en place de redondance.
- **Sécuriser les interconnexions** entre les sites et l'accès à Internet.
- **Déployer un accès Wi-Fi** différencié pour les employés et les visiteurs.
- **Mettre en place des outils de supervision et de gestion de parc** pour une administration proactive.

Contraintes techniques imposées:

- Utilisation d'équipements **Cisco** pour les routeurs et commutateurs.
- Utilisation de la plage d'adressage IP privée **172.20.0.0/22** pour le réseau interne du stade.
- Production d'une **documentation exhaustive** pour chaque solution mise en œuvre.

3. Les Missions Détaillées

Le projet se décompose en plusieurs missions progressives, permettant de construire l'infrastructure étape par étape.

Mission 1 : Restructuration de l'Infrastructure Réseau

Contexte

Le réseau actuel est "à plat";, source de lenteurs et de risques de sécurité. Il est impératif de le segmenter logiquement pour isoler les flux et d'établir un plan d'adressage cohérent.

Travaux à réaliser

- Concevoir un plan d'adressage IP basé sur la plage 172.20.0.0/22.
- Mettre en place une segmentation par VLANs pour les différents services : Administration, Équipes, WiFi, Caméras IP, VIP-Presse, Fournisseurs, Restaurant.
- Configurer les commutateurs Cisco : création des VLANs, affectation des ports en mode access, et configuration des liaisons inter-commutateurs en mode trunk.
- Configurer le routage inter-VLAN sur le routeur principal.
- Tester la communication au sein de chaque VLAN et entre les VLANs autorisés.

Livrables attendus

- Schéma de l'architecture réseau avec VLANs.
- Tableau d'adressage IP et des VLANs.
- Fichiers de configuration des équipements Cisco.

Mission 2 : Infrastructure et Administration des Services Informatiques

Contexte

Pour centraliser la gestion des utilisateurs et des ressources, l'entreprise a besoin de services d'annuaire, d'adressage et de nommage fiables, basés sur un environnement Microsoft Windows Server 2022.

Travaux à réaliser

- Installer et configurer un contrôleur de domaine Active Directory pour le domaine **stadiumcompany.com**.
- Déployer les services DNS et DHCP, intégrés à l'Active Directory. Configurer un serveur DNS secondaire (Linux ou Windows) pour la redondance.
- Créer la structure d'Unités d'Organisation (UO) par service, les groupes de sécurité et les comptes utilisateurs.
- Mettre en place des partages de fichiers avec des permissions basées sur les groupes AD.
- Définir et appliquer des GPO pour la politique de mot de passe et la sécurité des postes de travail.

Livrables attendus

- Schéma logique de l'Active Directory.
- Captures d'écran des configurations (AD, DNS, DHCP, GPO).
- Procédure de création d'un nouvel utilisateur.

Mission 3 : Sécurisation des Accès et des Interconnexions

Contexte

Les administrateurs doivent pouvoir gérer l'infrastructure à distance. De plus, les communications entre le stade et les sites distants (billetterie, magasin) doivent être chiffrées et sécurisées.

Travaux à réaliser

- Configurer l'accès distant sécurisé aux équipements réseau via le protocole **SSH**.
- Mettre en place un réseau privé virtuel (**VPN IPsec**) entre le site du stade et les deux sites distants.
- Mettre en œuvre des règles de pare-feu pour restreindre les accès d'administration aux seules adresses IP autorisées.
- Créer des comptes dédiés pour l'administration avec des droits restreints.

Livrables attendus

- Schéma des interconnexions VPN.
- Captures de configuration du VPN et des règles de sécurité SSH.
- Rapport de tests de connexion distante.

Mission 4 : Haute Disponibilité et Continuité de Service

Contexte

Une interruption de service pendant un événement est inacceptable. L'infrastructure doit être résiliente aux pannes matérielles.

Travaux à réaliser

- Mettre en place l'agrégation de liens (**EtherChannel**) entre les commutateurs principaux pour augmenter la bande passante et assurer la redondance.
- Configurer un protocole de redondance de passerelle (**HSRP/VRRP**) pour les VLANs critiques.
- Mettre en place la redondance des services critiques (ex: DHCP failover, DNS secondaire).
- Simuler des pannes (coupure de lien, arrêt d'un équipement) et valider le basculement automatique.

Livrables attendus

- Schéma d'architecture redondante.
- Captures des configurations d'agrégation et de redondance.
- Rapport de tests de panne et de basculement.

Mission 5 : Sécurisation de l'Accès à Internet et DMZ

Contexte

L'entreprise doit se connecter à Internet tout en protégeant son réseau interne. Les services exposés sur Internet (serveur web) doivent être isolés dans une zone démilitarisée (DMZ).

Travaux à réaliser

- Concevoir une architecture avec une **DMZ** pour héberger les serveurs publics.
- Installer et configurer un pare-feu pour filtrer les flux entre Internet, la DMZ et le réseau interne.

- Définir des politiques de filtrage strictes : autoriser le trafic web entrant uniquement vers la DMZ, autoriser la navigation web sortante pour les employés, et bloquer tout accès direct d'Internet vers le réseau interne.

Livrables attendus

- Schéma de l'architecture avec pare-feu et DMZ.
- Tableau des règles de filtrage du pare-feu.
- Rapport de tests de sécurité validant l'isolation des zones.

Mission 6 : Déploiement d'un Réseau Wi-Fi Sécurisé

Contexte

Le stade doit offrir un accès sans fil sécurisé et différencié pour ses employés et ses visiteurs, en conformité avec la législation.

Travaux à réaliser

- Déployer des points d'accès Wi-Fi compatibles PoE.
- Créer deux SSID : un pour les employés ("Stade-Employes") et un pour les visiteurs ("Stade-Visiteurs").
- Configurer la sécurité **WPA2/WPA3-Enterprise** avec authentification **RADIUS** (NPS sur Windows Server) pour le SSID des employés, en l'intégrant à l'Active Directory.
- Isoler le réseau visiteurs dans un VLAN dédié avec un accès limité à Internet, via un portail captif.

Livrables attendus

- Schéma de l'architecture Wi-Fi.
- Captures de configuration des points d'accès et du serveur RADIUS.
- Procédure de connexion pour les employés et les visiteurs.

Mission 7 : Gestion de Parc et Helpdesk

Contexte

La gestion des incidents et l'inventaire du parc informatique sont actuellement informels. Un outil centralisé est nécessaire pour professionnaliser le support utilisateur.

Travaux à réaliser

- Installer et configurer une solution de gestion de parc et de helpdesk open source (ex: **GLPI**).
- Déployer des agents d'inventaire sur les postes de travail pour automatiser la collecte d'informations.
- Synchroniser GLPI avec l'annuaire Active Directory pour l'authentification des utilisateurs.
- Configurer le système de ticketing, les notifications par e-mail et un collecteur pour créer des tickets depuis l'adresse support@stadiumcompany.com.

Livrables attendus

- Accès fonctionnel à l'interface GLPI.
- Guide utilisateur pour la création d'un ticket.
- Rapport de tests de la création de ticket (manuelle et par e-mail).

Mission 8 : Supervision de l'Infrastructure avec Nagios XI

Contexte

Pour garantir la disponibilité des services, la DSI a besoin d'un système de supervision proactif capable de détecter les pannes et de l'alerter en temps réel. Cet outil doit s'intégrer à l'annuaire d'entreprise pour la gestion des accès.

Travaux à réaliser

- Installer et configurer une solution de supervision (**Nagios XI**).
- Configurer la supervision des éléments critiques : serveurs (CPU, RAM, disque), équipements réseau (disponibilité, bande passante via SNMP), et services applicatifs (HTTP, DNS, DHCP).
- Mettre en place un système d'alertes par e-mail en cas de dépassement de seuil ou de panne.
- Créer des tableaux de bord (dashboards) et une cartographie du réseau.
- Intégrer Nagios XI à l'Active Directory/LDAP pour l'authentification des administrateurs et techniciens.

Livrables attendus

- Accès à la plateforme de supervision Nagios XI.
- Captures d'écran des tableaux de bord et des alertes.
- Documentation de l'intégration avec Active Directory.

Mission 9: Mise en Place d'un SIEM

Contexte

Face à la multiplication des cybermenaces, la simple supervision ne suffit plus. L'entreprise a besoin d'un outil de gestion des informations et des événements de sécurité (SIEM) pour corréler les journaux, détecter les comportements anormaux et faciliter la réponse aux incidents.

Travaux à réaliser

- Déployer une solution SIEM open source (ex: **Wazuh, ELK Stack**).
- Configurer la collecte centralisée des journaux (logs) depuis les serveurs, le pare-feu et les équipements réseau.
- Mettre en place des règles de corrélation pour détecter des activités suspectes (ex: tentatives de connexion échouées multiples, scan de ports).
- Configurer des alertes de sécurité en temps réel.
- Simuler une attaque simple et analyser l'alerte générée dans le SIEM.

Livrables attendus

- Accès fonctionnel au SIEM.
- Exemple d'une alerte de sécurité générée et analysée.
- Procédure simple de réponse à incident.

4. Schéma d'Infrastructure Cible

Le schéma ci-dessous représente l'architecture réseau cible à mettre en place sur le site principal du stade. Il détaille l'organisation des VLANs, les équipements clés et l'hébergement des services virtualisés.

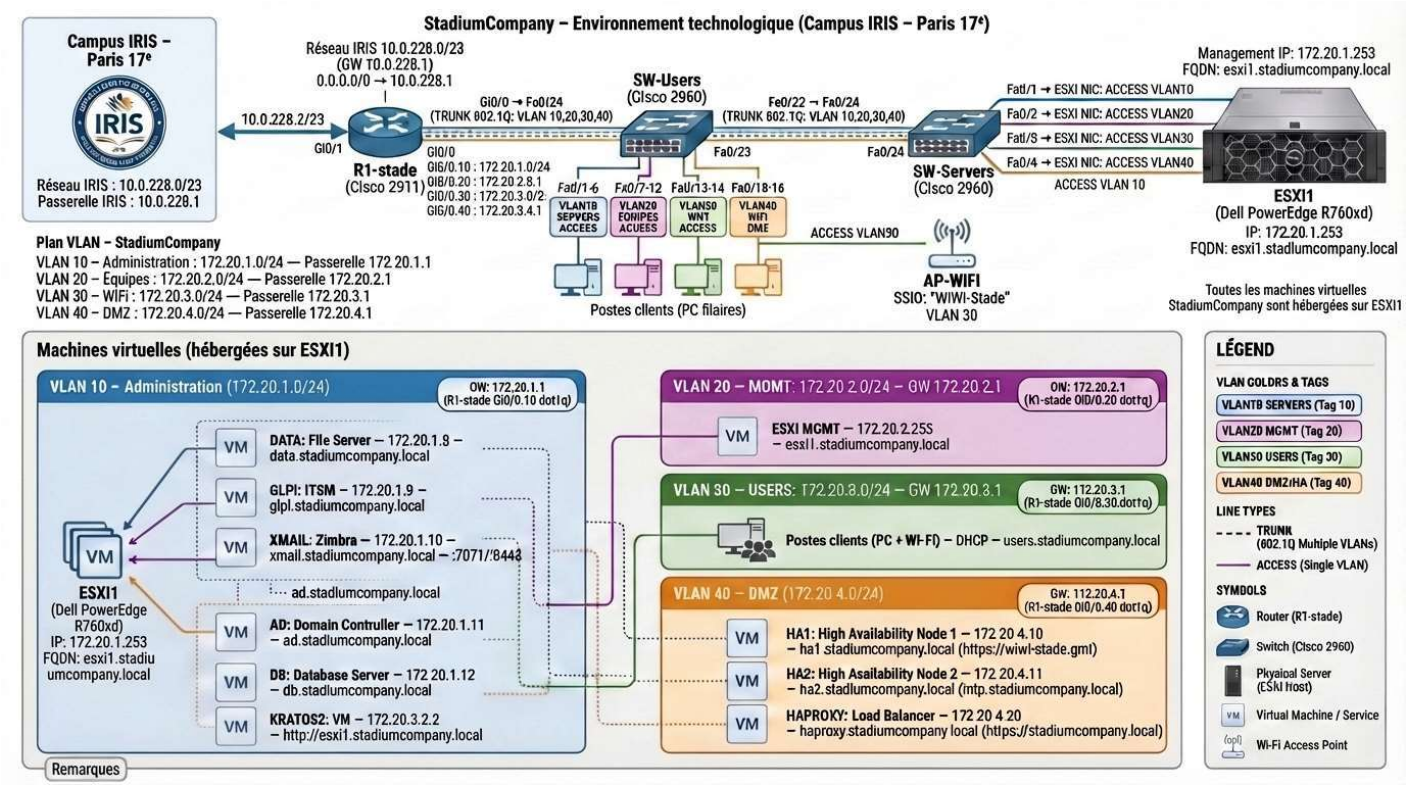

Figure 1 : Schéma de l'architecture réseau cible pour le site du Stade.

Ce schéma illustre:

- Le **routeur Cisco 4331 (R1-stade)** servant de passerelle et assurant le routage inter-VLAN.
- Les **commutateurs Cisco 2960 (SW-Users et SW-Servers)** connectant les utilisateurs et les serveurs.
- Le **serveur de virtualisation Dell PowerEdge (ESXI)** hébergeant les machines virtuelles des différents services.
- La segmentation du réseau en plusieurs **VLANs** :
  - **VLAN 10 (Administration) :** Héberge les contrôleurs de domaine (HERMES, NEPTUNE), le serveur de fichiers (DATA), le serveur DHCP (KRATOS2), le serveur DNS secondaire (ARES) et l'autorité de certification (ACR-PKI).
  - **VLAN 20 (Utilisateurs) :** Destiné aux postes de travail filaires des employés.

- **VLAN 30 (Wi-Fi) :** Gère les connexions sans fil via le point d'accès AP-WIFI (SSID "WIWI-Stade").
- **VLAN 40 (DMZ) :** Zone isolée pour les serveurs exposés à Internet, avec une solution de répartition de charge (HAPROXY).

- Les outils de gestion et de supervision tels que **GLPI, OCS, et NAGIOSXI**, intégrés au réseau.