MINISTÈRE
DE L'ÉDUCATION
NATIONALE,
DE LA JEUNESSE
ET DES SPORTS

Liberté
Égalité
Fraternité

Concours externe du Capet et Cafep-Capet

Section économie et gestion option informatique et systèmes d'information

Exemple de sujet pour l'épreuve écrite disciplinaire appliquée

À compter de la session 2022, les épreuves du concours externe du Capet et du Cafep-Capet sont modifiées. L'arrêté du 25 janvier 2021, publié au journal officiel du 29 janvier 2021, fixe les modalités d'organisation du concours et décrit le nouveau schéma des épreuves.

Rappel de la définition de l'épreuve

L'épreuve porte sur l'enseignement de sciences de gestion. Elle a pour but d'évaluer l'aptitude du candidat à concevoir et à organiser une séquence pédagogique sur la thématique proposée en exploitant de façon critique et argumentée un dossier documentaire fourni.

Le sujet de l'épreuve est spécifique à l'option choisie.

Durée : cinq heures. Coefficient 2.

L'épreuve est notée sur 20. Une note globale égale ou inférieure à 5 est éliminatoire.

Avertissement

Ce sujet « zéro » est plus long que le sujet qui sera proposé dans le cadre du concours afin d'offrir un large éventail des travaux qui pourraient être demandés aux candidats

La prise de connaissance des sujets exemples des autres options du Capet économie et gestion permet d'avoir une représentation de la variété de présentation de sujets pour cette épreuve.

Dans le sujet qui suit, la personne candidate traite la partie 1 puis choisit de traiter soit la partie 2A soit la partie 2B. Les ressources documentaires à exploiter selon le choix de la personne candidate sont identifiées.

Pour ce sujet exemple, des éléments ont été repris du cas ODBY traité dans le sujet du CAPET externe Informatique et systèmes d'information de la session 2018.

ODBY – Le projet de « *corpoworking* »

Vous enseignez en section de techniciens supérieurs Services informatiques aux organisations (SIO).

L'équipe pédagogique a choisi un contexte organisationnel qui sera utilisé dans l'enseignements des blocs professionnels et les ateliers de professionnalisation. Ce contexte permet de mettre les étudiantes et les étudiants en situation de participer, au sein de l'entreprise ODBY, à la mise en place d'un projet de *« corpoworking »* en faisant évoluer l'infrastructure système et réseau et les solutions applicatives.

À partir de vos connaissances et des ressources documentaires fournies, vous concevez une séquence pédagogique décomposée en deux parties :

– la première partie doit permettre de formuler une proposition permettant la découverte du contexte organisationnel dans le cadre des ateliers de professionnalisation afin de travailler des compétences de différents blocs de compétences dans les deux options du BTS ;

– la seconde partie doit permettre de formuler une proposition exploitant le contexte afin d'approfondir les compétences de l'option à votre choix,

soit pour l'option « Solutions d'infrastructure, systèmes et réseaux » SISR (partie 2A) ;

soit pour l'option « Solutions logicielles et applications métiers » SLAM (partie 2B).

Partie 1 - Découverte du contexte organisationnel

<u>Dossiers documentaires à exploiter :</u> dossier n° 1 commun et dossier n°2 spécifique à la partie 1

Dans le cadre des ateliers de professionnalisation permettant d'intégrer différentes compétences du BTS SIO, et afin de permettre la découverte du projet de *« corpoworking » au sein de l'entreprise ODBY*, vous avez à concevoir un scénario de découverte permettant de travailler les compétences :

B1.2 Répondre aux incidents et aux demandes d'assistance et d'évolution
Collecter, suivre et orienter des demandes
B2.3B- Gérer les données
Exploiter des données à l'aide d'un langage de requêtes
Concevoir ou adapter une base de données
B3.3 Sécuriser les équipements et les usages des utilisateurs
Identifier les menaces et mettre en œuvre les défenses appropriées
Gérer les accès et les privilèges appropriés
B3.5A Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service
Mettre en œuvre et vérifier la conformité d'une infrastructure à un référentiel, une norme ou un standard de sécurité

La situation et l'environnement d'apprentissage des étudiantes et étudiants, ainsi que le contexte ODBY, décrivant le projet de *« corpoworking »* sont présentés dans le dossier documentaire commun. Le dossier documentaire spécifique à cette partie complète différents aspects du contexte.

Le ***document 2.1*** du dossier documentaire fournit des exemples d'exploitation pédagogique.

Travail à faire

Proposer une première partie de séquence pédagogique réalisée dans le cadre des ateliers de professionnalisation, en précisant les points suivants :

- les objectifs d'apprentissage ;
- son déroulement : prérequis mobilisés, découpage en différentes phases, équipements et technologies mobilisés ;
- les travaux demandés aux étudiantes et étudiants en indiquant, pour chacune des phases,
- les consignes fournies (questions ou encore éléments d'évaluation à traiter) ;
- la ou les ressources choisie(s) dans le dossier joint en explicitant les raisons de votre choix. Pour les documents retenus, vous préciserez la transposition didactique nécessaire pour satisfaire les objectifs fixés (extraction d'une partie du document, suppression de certains termes ou informations, adjonction d'indications, etc.) ;
- les attendus de chaque travail demandé aux étudiantes et aux étudiants.

En particulier votre proposition intégrera :

- les règles de filtrage pour permettre l'accès aux DMZ
- l'intérêt et l'utilisation des options avancées de détection des vulnérabilités ou de prévention d'intrusion du pare-feu
- les bonnes pratiques pour sensibiliser les usagers à la confidentialité des données
- l'exploitation du langage d'interrogation des données
- la gestion des habilitations
- l'adaptation d'un schéma de base de données pour répondre à un nouveau besoin.

- - -

Partie 2A - Approfondissement du contexte organisationnel
Option « Solutions d'infrastructure, systèmes et réseaux » - SISR

Vous choisissez de traiter cette partie ou la partie 2B.

<u>Dossiers documentaires à exploiter :</u> dossier n° 1 commun et dossier n°3 spécifique à la partie 2A

Vous assurez plus particulièrement l'enseignement du bloc 2 de compétences **Administration des systèmes et des réseaux** pour les étudiantes et étudiants de l'option A « Solutions d'infrastructure, systèmes et réseaux » (SISR).
Dans le cadre de votre enseignement, vous décidez de poursuivre l'exploitation du contexte dans le cadre de la séquence pédagogique permettant de travailler les compétences :

B2.1A - Concevoir une solution d'infrastructure réseau

Analyser un besoin exprimé et son contexte juridique
Étudier l'impact d'une évolution d'un élément d'infrastructure sur le système informatique
Maquetter et prototyper une solution d'infrastructure permettant d'atteindre la qualité de service attendue

B2.2A - Installer, tester et déployer une solution d'infrastructure réseau

Installer et configurer des éléments d'infrastructure
Rédiger ou mettre à jour la documentation technique et utilisateur d'une solution d'infrastructure

B2.3A - Exploiter, dépanner et superviser une solution d'infrastructure réseau

Automatiser des tâches d'administration
Gérer des indicateurs et des fichiers d'activité des éléments d'une infrastructure

Il s'agit de mettre les étudiantes et étudiants en situation de faire évoluer l'infrastructure réseau et système induite par le projet de « *corpoworking »* et l'accueil des utilisateurs au sein d'espaces dédiés.

Le ***document 3.1*** du dossier documentaire spécifique à cette partie vous propose deux approches, l'une d'entre-elles est à choisir.

Travail à faire

Proposer une deuxième partie de séquence pédagogique, basée sur l'une des approches proposées, en précisant les points suivants :

- les objectifs d'apprentissage ;
- son déroulement : prérequis mobilisés, découpage en différentes phases, équipements et technologies mobilisés ;
- les travaux demandés aux étudiantes et étudiants en indiquant, pour chacune des phases,
- les consignes fournies (questions ou encore éléments d'évaluation à traiter) ;
- la ou les ressources choisie(s) dans le dossier joint en explicitant les raisons de votre choix. Pour les documents retenus, vous préciserez la transposition didactique nécessaire pour satisfaire les objectifs fixés (extraction d'une partie du document, suppression de certains termes ou informations, adjoction d'indications, etc.) ;
- les attendus de chaque travail demandé aux étudiantes et aux étudiants.

En particulier votre proposition intégrera selon l'approche choisie :

- approche n°1. Les éléments nécessaires à la mise en place de l'espace de « *corpoworking»* : modifications éventuelles du plan d'adressage, configuration des équipements filaires et sans fils répondant aux besoins exprimés par la par la direction des systèmes d'information (DSI) en

particulier concernant la limitation des accès aux seules ressources autorisées ;

- approche n°2. Les éléments nécessaires à l'automatisation de la gestion des journaux (*logs*) systèmes des accès internet des utilisateurs et à l'implémentation de la centralisation des journaux (*logs*). D'autres exemples de scripts pourront être proposés pour développer les compétences des étudiants dans le domaine de programmation à l'aide d'un langage de *script*.

- - -

Partie 2B - Approfondissement du contexte organisationnel Option « Solutions logicielles et applications métiers » - SLAM

Vous choisissez de traiter cette partie ou la partie 2A.

<u>Dossiers documentaires à exploiter :</u> dossier n° 1 commun et dossier n° 4 spécifique à la partie 2B

Vous assurez plus particulièrement l'enseignement du bloc 2 de compétences **Conception et développement d'applications** pour les étudiantes et étudiants de l'option B - Solutions logicielles et applications métiers (SLAM).

Dans le cadre de votre enseignement, vous décidez de poursuivre l'exploitation du contexte dans le cadre d'une séquence pédagogique permettant de travailler les compétences :

B2.1B -Concevoir et développer une solution applicative

Modéliser une solution applicative

Identifier, développer, utiliser ou adapter des composants logiciels

Utiliser des composants d'accès aux données

Intégrer en continu les versions d'une solution applicative

B2.3B - Gérer les données

Exploiter des données à l'aide d'un langage de requêtes

Administrer et déployer une base de données

Il agit de mettre les étudiantes et étudiants en situation de développer l'application de suivi de projet. Les espaces de « *corpoworking »* auront pour vocation de tester de nouveaux modes de collaboration plus agiles en accueillant des équipes provenant de différents services, voire en intégrant des partenaires ou encore des personnes extérieures à l'entreprise qui travailleront sur un même projet pour plusieurs semaines.

Le ***document 4.1*** du dossier documentaire spécifique à cette partie vous propose deux approches, l'une d'entre-elles est à choisir.

Travail à faire

Proposer une deuxième partie de séquence pédagogique, basée sur l'une des approches proposées, en précisant les points suivants :

- les objectifs d'apprentissage ;
- son déroulement : prérequis mobilisés, découpage en différentes phases, équipements mobilisés ;
- les travaux demandés aux étudiantes et étudiants en indiquant, pour chacune des phases,
- les consignes fournies (questions ou encore éléments d'évaluation à traiter) ;
- la ou les ressources choisie(s) dans le dossier joint en explicitant les raisons de votre choix. Pour les documents retenus, vous préciserez la transposition didactique nécessaire pour satisfaire les objectifs fixés (extraction d'une partie du document, suppression de certains termes ou informations, adjonction d'indications, etc.) ;
- les attendus de chaque travail demandé aux étudiantes et aux étudiants.

En particulier votre proposition intégrera selon l'approche choisie :

- approche n°1. L'exploitation d'un diagramme de classes et son implémentation, la modélisation et l'implémentation de l'héritage, le parcours de collections, l'exploitation d'un cas d'utilisation ;
- approche n°2. La mise en place d'une organisation agile de production logicielle, la démarche d'intégration continue, particulièrement l'implémentation des tests.

Index des dossiers documentaires

Dossier documentaire n° 1 commun

Document 1.1 : acquis des étudiants liés à la première année de BTS SIO

Ce document rassemble les acquis des étudiantes et étudiants lors de leur première année en sections de techniciens supérieurs SIO, en termes de savoirs et de savoirs technologiques. Ces acquis sont mobilisables dans les scénarios pédagogiques des parties 1 et 2 (A et B).

Orientation "réseau"

Les compétences travaillées ont permis d'aborder les notions suivantes :

- Bases sur la résolution des incidents : ITIL, cycle de vie d'un incident.
- Modèle OSI et TCP/IP, adressage IPv4, routage, segmentation, VLAN, réseaux sans fil (Wi-Fi).
- Notions d'annuaire : LDAP/Domaine Active Directory.
- Notions de base en programmation, langage de script.
- Principaux protocoles et ports et services associés : services d'architecture (DNS/DHCP, NTP), services de communication (fichiers, messagerie, annuaire LDAP...)

Les étudiantes et étudiants ont une pratique courante des technologies suivantes :

- Bases de l'administration système sous Linux : commandes de base, consultation de fichiers, filtres, pipe, installation de paquets...
- Bases de l'administration réseau : Mise à disposition d'un accès à un réseau commuté et segmenté
- Installer et configurer un commutateur (VLAN, 802.1q), un point d'accès Wi-Fi (WPA2 PSK)
- Installer et configurer un équipement assurant le routage des paquets (routage statique et dynamique : RIP)
- Utilisation de l'outil de simulation Cisco Packet Tracer et d'équipements physiques (routeurs, commutateurs, points d'accès Wi-Fi...)

Orientation "développement "

Les compétences travaillées ont permis d'aborder les notions suivantes :

- Programmation procédurale, bases de la programmation orientée objet.
- Modélisation et maquettage d'une solution applicative.
- Adaptation d'une base de données en réponse à de nouveaux besoins.
- Accès aux données à travers des requêtes du langage de la base depuis une application.
- Architectures applicatives n-tiers.

Les étudiantes et étudiants ont une pratique courante des technologies suivantes :

- Java, PHP.
- HTML CSS Javascript et/ou infrastructure logicielle (*framework*) Javascript.
- Étude et modification de *template* (modèle) de site web.
- Techniques de mise à disposition de site web (local, cloud privé, cloud public).
- Étude et modification de site PHP MySQL //procédural, accès aux données avec PDO.
- Interprétation et modification des formats de données structurées (JSON, XML).
- Génération et exploitation de script de création de base de données.
- Manipulation des données à l'aide du langage SQL.
- Étude et modification de site PHP MySQL //CMS WordPress.

– Étude et modification de site PHP MySQL //Framework Symfony.

– Gestion de versions de code source.

– Pratique d'un outil de gestion de projet (tâches, planification, ressources, etc.).

Document 1.2 : environnement technologique mobilisable dans les laboratoires

Les différents laboratoires SISR et SLAM au sein desquels les enseignements se déroulent sont équipés d'environnements conformes à l'Annexe 2E du référentiel du BTS SIO et décrits ci-après.

Environnement technologique mobilisable pour l'ensemble des blocs de compétences

- un service d'authentification pour les utilisateurs internes et externes à l'organisation ;
- un SGBD ;
- un accès sécurisé à internet ;
- un environnement de travail collaboratif ;
- deux serveurs, éventuellement virtualisés, basés sur des systèmes d'exploitation différents, dont l'un est un logiciel open source ;
- une solution de sauvegarde ;
- des ressources dont l'accès est sécurisé et soumis à habilitation ;
- deux types de terminaux dont un mobile (type smartphone ou encore tablette) ;
- un outil de gestion des incidents ;
- des services exploitant des techniques de chiffrements.

Environnement technologique mobilisable pour l'option A « Solutions d'infrastructure, systèmes et réseaux »

- un réseau comportant plusieurs périmètres de sécurité ;
- un service rendu à l'utilisateur final respectant un contrat de service comportant des contraintes en termes de sécurité et de haute disponibilité ;
- un logiciel d'analyse de trames ;
- un logiciel de gestion des configurations ;
- une solution permettant l'administration à distance sécurisée de serveurs et de solutions techniques d'accès ;
- une solution permettant la supervision de la qualité, de la sécurité et de la disponibilité des équipements d'interconnexion, serveurs, systèmes et services avec remontées d'alertes ;
- une solution garantissant des accès sécurisés à un service, internes au périmètre de sécurité de l'organisation (type intranet) ou externes (type internet ou extranet) ;
- une solution garantissant la continuité d'un service ;
- une solution garantissant la tolérance de panne de systèmes serveurs ou d'éléments d'interconnexion ;
- une solution permettant la répartition de charges entre services, serveurs ou éléments d'interconnexion ;
- une solution permettant le déploiement d'un réseau filaire *ethernet* commuté et Wi-Fi ;
- une solution permettant la connexion sécurisée entre deux sites distants ;
- une solution permettant le déploiement des solutions techniques d'accès ;
- une solution gérée à l'aide de procédures automatisées écrites avec un langage de *scripting* ;
- une solution permettant la détection d'intrusions ou de comportements anormaux sur le réseau.

Environnement technologique mobilisable pour l'option B « Solutions logicielles et applications métiers »

- un ou deux environnements de développement disposant d'outils de gestion de tests et supportant un cadre applicatif (*framework*) et au moins deux langages ;
- une bibliothèque de composants logiciels ;
- un SGBD avec langage de programmation associé ;
- un logiciel de gestion de versions et de suivi de problèmes d'ordre logiciel ;
- une solution permettant de tester les comportements anormaux d'une application ;

- Au sein des architectures de ces solutions applicatives se retrouvent ;
  - du code exécuté sur le système d'exploitation d'une solution technique d'accès fixe (type client lourd) ;
  - du code exécuté dans un navigateur Web (type client léger ou riche) ;
  - du code exécuté sur le système d'exploitation d'une solution technique d'accès mobile ;
  - du code exécuté sur le système d'exploitation d'un serveur.
- Une solution applicative issue d'un développement spécifique ou de la modification du code d'un logiciel notamment *open source*.

Document 1.3 : extraits du référentiel du BTS SIO

Bloc de compétences n°1 - Support et mise à disposition de services informatiques

Compétences	Indicateurs de performance	Savoirs associés
B1.2 Répondre aux incidents et aux demandes d'assistance et d'évolution ▪ Collecter, suivre et orienter des demandes	En utilisant les outils adaptés, les demandes d'assistance ont été prises en compte, correctement diagnostiquées et leur traitement correspond aux attentes.	Savoirs technologiques Outils et méthodes de gestion des incidents

Bloc de compétences 2 - Administration systèmes et réseaux options - Option A « Solutions d'infrastructure, systèmes et réseaux »

Compétences	Indicateurs de performances	Savoirs associés
B2.1A - Concevoir une solution d'infrastructure réseau • Analyser un besoin exprimé et son contexte juridique • Étudier l'impact d'une évolution d'un élément d'infrastructure sur le système informatique • Maquetter et prototyper une solution d'infrastructure permettant d'atteindre la qualité de service attendue	Les risques liés à une mauvaise utilisation ou à un dysfonctionnement de la solution d'infrastructure sont identifiés. Les composants de l'architecture technique sur lesquels la solution d'infrastructure à produire aura un impact sont recensés.	Savoirs technologiques Installation et configuration des éléments d'interconnexion et des services techniques réseau Déploiement d'éléments d'infrastructure : méthodes, technologies, techniques, normes et standards associés Supervision et métrologie des infrastructures réseaux : méthodes, technologies, techniques, normes et standards associés ; Techniques, outils et protocoles d'administration à distance Langage de commande d'un système d'exploitation : commandes et script d'administration d'une solution d'infrastructure
B2.2A - Installer, tester et déployer une solution d'infrastructure réseau • Installer et configurer des éléments	Des éléments d'infrastructure (élément d'interconnexion, service, serveur, équipement utilisateur) sont installés et configurés. L'intégration de la solution ne génère pas de dysfonctionnement du réseau ou dans le réseau.	

d'infrastructure • Rédiger ou mettre à jour la documentation technique et utilisateur d'une solution d'infrastructure **B2.3A - Exploiter, dépanner et superviser une solution d'infrastructure réseau** • Automatiser des tâches d'administration • Gérer des indicateurs et des fichiers d'activité des éléments d'une infrastructure	L'automatisation des tâches d'administration répond au besoin exprimé ; Les outils nécessaires à la production d'indicateurs d'activité et à l'exploitation de fichiers d'activité sont installés et configurés.	Techniques, outils et protocoles d'administration à distance

Bloc de compétences 2 - Solutions logicielles et applications métiers- Option B « Solutions logicielles et applications métiers »

Compétences	Indicateurs de performance	Savoirs associés
B2.1B - Concevoir et développer une solution applicative • Analyser un besoin exprimé et son contexte juridique • Modéliser une solution applicative • Identifier, développer, utiliser ou adapter des composants logiciels • Utiliser des composants d'accès aux données • Réaliser les tests nécessaires à la validation ou à la mise en production d'éléments adaptés ou développés • Intégrer en continu les versions d'une solution applicative	Le choix des composants logiciels à utiliser et/ou à développer est pertinent. Les composants logiciels sont validés par les procédures de tests unitaires et fonctionnels. Les données persistantes liées à la solution applicative sont exploitées à travers un langage de requête lié à la base de données qui peut être le langage de requête proposé par les échanges applicatifs des technologies Web, un langage de requête présent dans l'outil de correspondance objet-relationnel ou toute autre solution de persistance. L'application développée est opérationnelle conformément au cahier des charges et stable dans l'environnement de production. Les tests d'intégration sont réalisés.	<u>Savoirs technologiques</u> Méthodes, normes et standards associés au processus de conception et de développement d'une solution applicative Architectures applicatives : concepts de base et typologies Techniques et outils d'analyse et de rétro-conception Concepts de la programmation objet : classe, objet, abstraction, interface, héritage, polymorphisme, annotations, patrons de conception, interface de programmation d'applications Persistance et couche d'accès aux données Fonctionnalités d'un outil de gestion de

B2.3B - Gérer les données • Exploiter des données à l'aide d'un langage de requêtes • Concevoir ou adapter une base de données • Administrer et déployer une base de données	Un outil collaboratif de gestion des itérations de développement et de versions est utilisé. Une documentation des versions vient appuyer l'intégration continue. L'exploitation des données permet de construire l'information attendue. Les accès aux données sont contrôlés conformément aux habilitations définies par le cahier des charges. Les données sont modélisées conformément au besoin de la solution applicative.	projets. Concepts et techniques de développement agile

Bloc de compétences 3 - Cybersécurité des services informatiques

Compétences	Indicateurs de performance	Savoirs associés
B3.3 Sécuriser les équipements et les usages des utilisateurs ▪ Identifier les menaces et mettre en œuvre les défenses appropriées ▪ Gérer les accès et les privilèges appropriés	Les outils de défense mis en œuvre permettent de prévenir les menaces identifiées : - l'accès physique au terminal et à ses données est sécurisé ; - les applications installées sont vérifiées par des procédures automatisées et des logiciels de sécurité ; - les flux réseaux sont identifiés et sécurisés. Les accès et privilèges respectent les règles organisationnelles : - les utilisateurs sont authentifiés ; - les habilitations sont configurées ; - l'accès aux données est contrôlé ; - les privilèges sont restreints.	<u>Savoirs technologiques</u> Typologie des risques et leurs impacts. Principes de la sécurité : disponibilité, intégrité, confidentialité, preuve. Sécurité et sûreté : périmètre respectif. Sécurité des terminaux utilisateurs et de leurs données : principes et outils. Authentification, privilèges et habilitations des utilisateurs : principes et techniques. Gestion des droits d'accès aux données : principes et techniques. Sécurité des communications numériques : rôle des protocoles, segmentation, administration, restriction physique et logique. Protection et archivage des données : principes et techniques. Chiffrement, authentification et preuve : principes et techniques. Sécurité des applications *Web* : risques, menaces et protocoles.
B3.5A Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service ▪ Mettre en œuvre et vérifier la conformité d'une infrastructure à un référentiel, une	Les éléments de sécurité de l'architecture sont conformes et documentés.	<u>Savoirs technologiques</u> Technologies et équipements de la sécurité informatique des infrastructures réseau,

norme ou un standard de sécurité		systèmes et services. Outils de sécurité : prévention et détection des attaques, gestion d'incidents. <u>Savoir économique, juridique et managérial</u> Responsabilité civile et pénale de l'administrateur système et réseau.

Document 1.4 : contexte organisationnel de la société ODBY

ODBY, une entreprise de services du numérique (ESN) française

Le groupe ODBY est un grand acteur européen dans le domaine des services du numérique. Au niveau mondial, il est présent dans une vingtaine de pays avec un effectif total de près de 17 000 salariés dont environ 12 000 ingénieurs. ODBY est une société anonyme créée en 1985. Son siège social se situe à Paris. Sur le territoire national, ODBY dispose également de 14 agences (9 000 salariés) et d'une vingtaine d'autres dans le reste du monde. Les principaux métiers de ODBY sont :

- le conseil en stratégie ;
- l'ingénierie et le conseil en technologies ;
- le conseil en organisation ;
- le développement et la mise en œuvre de systèmes d'information ;
- l'infogérance.

ODBY a récemment décidé d'orienter ses choix organisationnels en intégrant de nouvelles modalités de travail notamment par le management des espaces de travail. ODBY souhaite repenser ces lieux pour y apporter davantage de flexibilité, favoriser la collaboration que ce soit en mode projet classique ou, de plus en plus fréquemment, en mode agile. Un premier volet de la mise en œuvre de la nouvelle organisation a amené les dirigeants à envisager de mettre en place un projet de cotravail (*coworking*) au sein de l'entreprise elle-même : on parle de cotravail en entreprise ou ***«corpoworking »*** (contraction de « *corporate* » et « *coworking* »).

Le projet de « corpoworking » chez ODBY

Avec la mise en place du « *corpoworking* », ODBY vise à proposer un mode d'organisation du travail basé sur des espaces partagés au sein de ses propres locaux dans le but de favoriser les échanges et la coordination entre les personnes. Ces lieux permettront d'accueillir des salariés pour leurs tâches quotidiennes mais aussi des équipes travaillant sur un même projet durant plusieurs semaines. Les « *corpoworkers* » formeront une communauté de partage nécessitant un travail d'animation et de coordination, par exemple pour l'organisation d'événements (conférences, interventions d'experts, réunions, déjeuners, etc.). L'aménagement de ces espaces de *« corpoworking »* sera particulièrement soigné : confort et bien-être y seront privilégiés (espaces modulables, mobilier de qualité, etc.), tout autant que la fiabilité et la sécurité de la connectique, de l'accès au réseau et de l'accès aux données de l'entreprise. Des outils adaptés au nomadisme permettront une utilisation fiable et simple de ces espaces.

Exemple de prestations que pourrait offrir un espace de *« corpoworking » d*e ODBY

Le « *corpoworking* » offrira, un espace de travail spécialement aménagé en plusieurs zones qui seront dédiées à un projet ou à un type de tâche et non plus à un collaborateur précis. Cet espace divisé en zones sera ouvert, sur réservation :

- aux employés de ODBY ;
- à ses partenaires (clients, prestataires, etc.) au sein de projets communs impliquant ODBY ;
- à des personnes totalement extérieures à la société qui louent à ODBY un espace connecté et équipé pour travailler.

Dans les deux premiers cas, le service est rendu pour le propre compte de ODBY, dans le troisième cas ODBY propose une prestation de location pour des clients extérieurs. D'un point de vue informatique, l'espace de *«corpoworking »* proposera systématiquement une connexion sans fil (Wi-Fi), des imprimantes, mais aussi, à la demande, des ordinateurs (clients et/ou serveurs), tablettes, du matériel de visioconférence permettant le travail en projet en semi-présentiel. L'entretien et la maintenance du lieu seront assurés par ODBY.

Au cours de la dernière séance de travail commune, la direction générale a demandé à la DSI de proposer des solutions logicielles pour faciliter le travail des équipes collaborant au sein des espaces de « *corpoworking* ». La DSI a déjà réfléchi à plusieurs outils parmi lesquels un espace numérique de travail collaboratif, une application de gestion des projets agiles et un outil de gestion de versions.

Le rôle de la direction des systèmes d'information (DSI)

La direction des systèmes d'information (DSI), composée d'une centaine de personnes, devra mettre en place et sécuriser l'ensemble des outils informatiques et des infrastructures des systèmes qui supporteront ces espaces de « *corpoworking* ». Elle a donc pour mission de proposer des solutions techniques d'intégration de ces espaces au système d'information existant. La DSI devra également en assurer l'entretien et la maintenance.

Document 1.5 : plan d'adressage du contexte de la société ODBY

Les informations qui suivent constituent la feuille de route de l'équipe « Réseaux & Systèmes » de la société ODBY afin de mettre en place les espaces de « *corpoworking* ».
Des sous-réseaux IP doivent être définis pour prendre en charge chaque catégorie d'usagers. Le plan d'adressage pour ces réseaux pour le site de Paris devra permettre de prendre en compte ces nouveaux réseaux IP sur la base des éléments suivants :

- l'adresse du réseau de l'entreprise est 10.0.0.0/8 ;
- chaque site a une adresse en 10.x.0.0/16 ou x est le numéro du site ;
- à l'intérieur de chaque site, pour les sous-réseaux locaux actuels, l'adressage est en 10.x.y.0/24 ou x correspond au site, et y correspond au numéro de VLAN (y est strictement inférieur à 128) ;
- on propose pour l'espace de *« corpoworking »* une adresse de type 10.x.y.0/24 avec y supérieur ou égal à 128 et correspondant au numéro de VLAN associé à chaque SSID ;
- le réseau des usagers internes aura la première adresse disponible, les partenaires la deuxième adresse et les externes la troisième adresse ;
- ce système permettra d'agréger d'un côté les sous-réseaux locaux existants et de l'autre les sous-réseaux de l'espace de « *corpoworking »* ;
- le routeur de distribution actuel associé au commutateur d'accès avec une adresse par VLAN sera utilisé pour router les nouveaux VLAN (il aura les adresses les plus hautes de l'espace d'adressage) ;
- les postes sans fil récupéreront une adresse dynamique (baux d'une journée) correspondant à leur espace d'adressage ;
- un serveur DHCP spécifique (placé dans la DMZ commune) sera configuré pour l'espace de *« corpoworking »* et accessible via le routeur de distribution ;
- le serveur DHCP renverra, entre autres, l'adresse d'un serveur DNS situé dans la zone démilitarisée (DMZ) commune.

Éléments du plan d'adressage

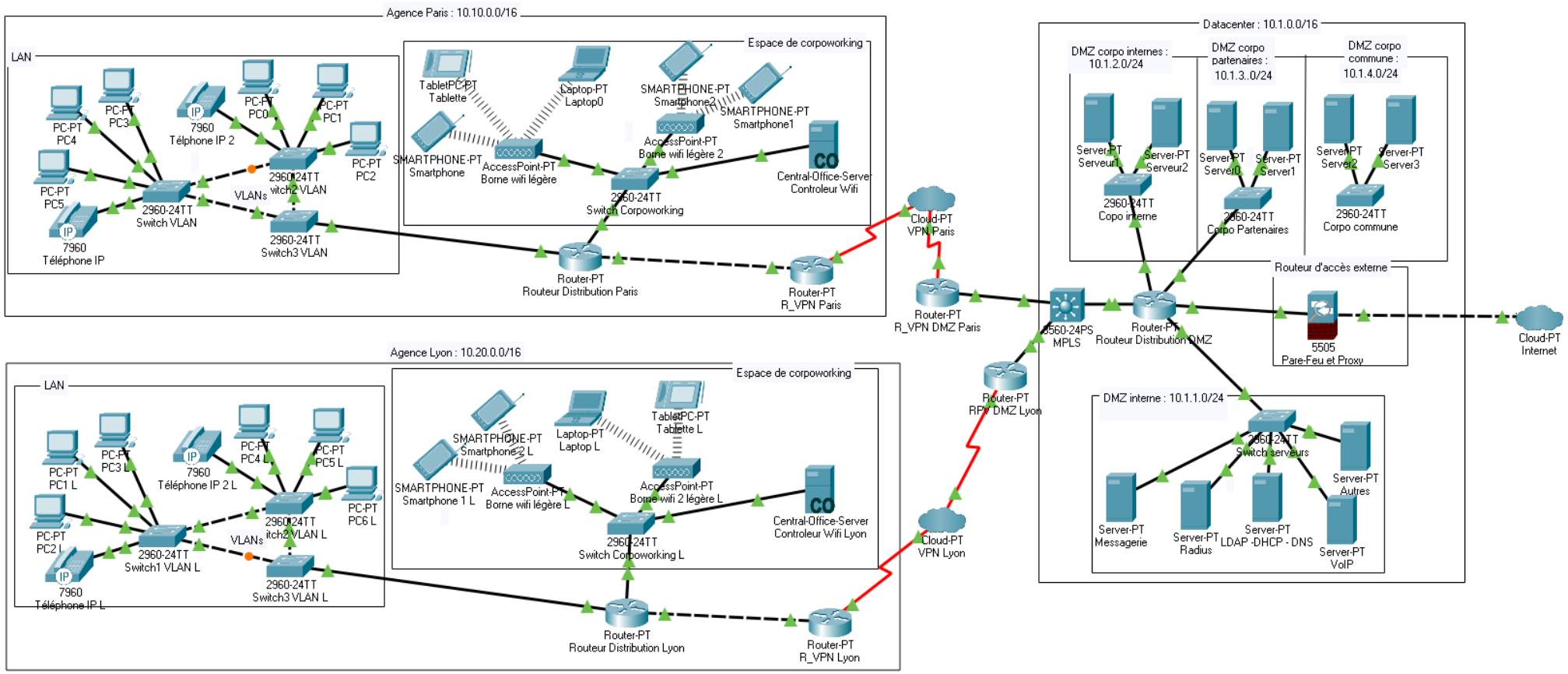
Adresse du siège social de Paris	10.10.0.0/16
Adresse du routeur de distribution de Paris, lien vers routeur d'accès	10.10.127.254
Adresse du routeur d'accès de Paris, lien vers routeur de distribution	10.10.127.253
Adresse du *datacenter*	10.1.0.0/16
Adresse DMZ interne	10.1.1.0/24
Adresse du serveur DHCP *corpoworking*	10.1.4.10

Extrait du tableau des serveurs

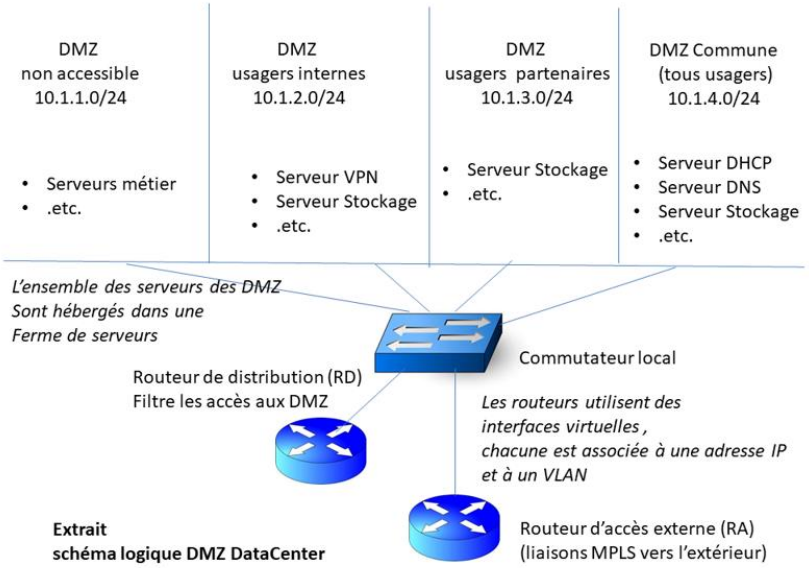
Nom des serveurs	**Fonction**	**Adresse IP**
serv-ladp1	Serveur d'authentification	10.1.0.1
serv-radius1	Serveur radius	10.1.0.11
serv-syslog	Serveur Syslog	10.1.0.21
serv-pub	Serveur Web public de Paris	10.10.0.31
serv-lyon	Serveur dédié au site de Lyon	10.20.0.1
serv-nice	Serveur dédié au site de Nice	10.30.0.1

Document 1.6 : schéma du réseau global de la société ODBY

Le schéma ci-dessous est un schéma logique, ainsi, entre autres, toutes les redondances associées à la tolérance de panne n'apparaissent pas.
Ce schéma présente une partie du réseau global et reprend les informations techniques présentées par ailleurs.



Document 1.7 : extrait du schéma logique du centre de données (*datacenter*) de la société ODBY



Document 1.8 : cahier des charges technique du projet d'espace de « *corpoworking* »

Les éléments ci-après ont été recueillis lors des réunions de l'équipe « Réseaux & Systèmes » et constituent les éléments du cahier des charges technique du projet d'espaces de « *corpoworking* ».
Attentes de la DSI : "Les usagers de l'espace de *« corpoworking »* vont utiliser des ressources mises à leur disposition à travers le réseau de ODBY. L'architecture proposée doit permettre de limiter les accès aux seules ressources autorisées par la DSI et de s'insérer dans l'architecture actuelle. Une architecture centralisée et une politique de sécurité doivent être définies par votre équipe."
Document de travail de l'équipe « Réseaux & Systèmes » :

- le mode exclusif d'accès à l'infrastructure réseau sera le mode sans fil quel que soit le matériel utilisé (portable, *smartphone*, tablette, etc.). Aucune connexion filaire ne sera mise à disposition ;
- dans cet espace, les utilisateurs seront autorisés à utiliser leur propre matériel (*BYOD* ou *BYOE*) qui ne sera pas contrôlé par le service « Réseaux et systèmes » ;
- trois catégories d'usagers seront admises dans ces espaces à savoir les usagers internes, les partenaires d'un projet, les clients extérieurs ;
- les données produites par les usagers pourront être hébergées sur les serveurs de l'entreprise dans des espaces sécurisés ;
- des applications métiers pourront être utilisées par les usagers internes et les partenaires ;
- trois niveaux de ressources seront accessibles à partir de l'espace de « *corpoworking»* correspondant à chacune des trois catégories d'utilisateurs ;
- en fonction de son niveau, une ressource est soit accessible par tous, soit accessible par les partenaires et les usagers internes, soit enfin accessible par les seuls usagers internes ;
- toutes les autres ressources seront inaccessibles à partir de l'espace de « *corpoworking » ;*
- la notion de ressource doit être comprise dans un sens très large, cela peut être aussi bien une imprimante, une application, un service numérique ou bien encore un espace de stockage ;
- la ressource « accès internet » doit respecter les obligations juridiques des entreprises ;
- il faudra procéder régulièrement à des tests de vulnérabilité du réseau Wi-Fi ;
- Il faudra mettre à disposition en libre-service un point diagnostic des terminaux mobiles avec notamment un antivirus à jour et d'autres outils logiciels d'analyse et de dépannage.

Dossier documentaire n° 2 spécifique à la partie 1

Document 2.1 : exemples d'exploitation du contexte ODBY

Le contexte organisationnel ODBY a déjà été mobilisé par l'équipe pédagogique l'année dernière. Ainsi deux missions avaient été définies. Elles exploitent le contexte et différentes ressources présentées dans le dossier documentaire spécifique à cette partie : description des services rendus aux utilisateurs, modélisation des données, configurations des différents matériels et systèmes, etc.

Mission 1 : exploitation et évolution de la base de données des incidents

ODBY assure en interne la maintenance de son parc informatique et la gestion des incidents. Chaque utilisateur rencontrant un problème avec son poste informatique s'adresse au service informatique. Une analyse rapide de cette gestion a conduit à la création d'une base de données relationnelle BDINCIDENTS dont un extrait se trouve en annexe du cas.

Plusieurs opérations sont nécessaires sur la base BDINCIDENTS.

Questionnement de la mission 1 :

1.a. La dernière intervention sur l'incident n° 2020086 a été enregistrée. Il reste à mettre à jour la table INCIDENT, où l'état de cet incident doit passer à la valeur "fermé".

1.b. L'application de gestion des incidents comporte la requête suivante :

```
Select NoIncident, NoPoste
from INCIDENT I
where NoIncident not in (select NoIncident from INTERVENTION)
```

Il faut faire évoluer la requête pour connaître le nom de la personne qui a déclaré l'incident.

1.c. L'administratrice de la base désigne M. SALEM comme unique gestionnaire des données de la base. Celui-ci doit avoir tous les droits sur les tables INCIDENT et INTERVENTION.

1d. Le tableau de bord doit permettre de connaître le nombre d'incidents mensuels survenus pour chaque service au cours de l'année 2020. Cette liste apparaît triée par ordre alphabétique des noms de service.

Il faut faire évoluer le schéma relationnel et le valider au moyen d'une requête répondant au besoin.

Mission 2 : limitation de l'accès aux ressources et sécurisation du BYOD dans l'espace de « *corpoworking »*

Vous participez en tant que technicien support à la mise en place du projet. Le chef du projet *« corpoworking »* vous confie la première tâche ci-après :

Questionnement de la mission 2 :

2.a. Le routeur de distribution du centre de données (*datacenter)* doit filtrer l'accès aux DMZ où sont placées les ressources. Vous devez compléter les règles de filtrage pour permettre l'accès aux DMZ pour les différents sous-réseaux associés au *« corpoworking »* du site de Paris.

L'accès internet pour l'entreprise est centralisé ; un pare-feu protège le réseau local. Le chef de projet s'interroge sur l'intérêt d'activer les options avancées de détection des vulnérabilités ou de prévention d'intrusion du pare-feu dans le contexte de l'utilisation par les usagers de matériels personnels (BYOD).

2.b. Proposer une réponse argumentée basée sur vos connaissances et sur la documentation technique du pare-feu d'ODBY.

Les comportements et les bonnes pratiques des usagers de l'espace sont la clé de la réussite du projet. La présence de personnes extérieures à ODBY doit être prise en compte par la politique de sécurité.

2.c. Le chef de projet vous demande de proposer une liste de bonnes pratiques destinées aux usagers pour les sensibiliser à la confidentialité des données.

Document 2.2 : réunion de projet à propos du déploiement de la solution « *corpoworking* »

Dans le cadre de la démarche de projet de déploiement de la solution « *corpoworking* », des réunions sont régulièrement organisées entre la direction générale, la direction des ressources humaines et la direction des systèmes d'information (DSI).

Voici les échanges de la dernière séance de travail commune :

Message du directeur général :

« [..] Une des principales conditions pour que le nouvel espace de *«corpoworking »* remporte l'adhésion des parties prenantes est d'assurer un parfait fonctionnement des installations matérielles et logicielles. Nous nous sommes engagés à garantir à l'ensemble des utilisateurs des espaces de *«corpoworking »* un délai de résolution des incidents matériels et logiciels d'au plus 30 minutes [..] »

Message du responsable des systèmes d'information :

« [..] Nous venons de mettre en place le nouvel outil de gestion du patrimoine informatique nous permettant de prioriser et de classifier les incidents (matériels, logiciels, données, personnels, procédures) et de gagner ainsi en visibilité sur notre parc informatique. [..] »

Message du responsable des ressources humaines :

« Merci pour ces éléments d'information, avez-vous pu avancer sur le projet de réplication et de sauvegarde ? »

Message du responsable des systèmes d'information :

« Concernant ce projet, nos équipes s'interrogent sur la réalisation de cette prestation en interne ou de passer par une offre cloud, nous permettant de :

- ne pas avoir à gérer la montée en charge
- ne pas avoir à gérer les sauvegardes et les modalités de stockage
- limiter les risques de dégradation des données de ODBY
- possibilité de moduler facilement les besoins (flexibilité, évolutivité, souplesse, …)

Nous allons terminer cette étude dans les prochains jours, nous permettant ainsi de poursuivre les projets de fond tels que :

- l’exploitation de machines virtuelles en mode dégradé pour remettre en place rapidement un environnement ;
- l’amélioration de la tolérance de pannes et la haute disponibilité sur tous les niveaux ;
- l’amélioration de la sécurité du système d’information ;
- poursuivre le plan de formation des utilisateurs ;
- la mise à disposition d’une documentation type FAQ.

[..]

Document 2.3 : base de données de maintenance du parc informatique

PERSONNEL(NoPersonnel, NomPersonnel)
NoPersonnel : clé primaire
NomPersonnel

POSTE(NoPoste, DescriptifPoste)
NoPoste : clé primaire

UTILISER(NoPersonnel, NoPoste)
NoPersonnel, NoPoste : clé primaire
NoPersonnel : clé étrangère faisant référence à NoPersonnel de la table PERSONNEL
NoPoste : clé étrangère faisant référence à NoPoste de la table POSTE

INCIDENT(NoIncident, DateIncident, HeureIncident, Symptôme, Etat, NoUtilisateur, NoPoste, NoIntervenant)
NoIncident : clé primaire
NoUtilisateur : clé étrangère faisant référence à NoPersonnel de la table PERSONNEL
NoPoste : clé étrangère faisant référence à NoPoste de la table POSTE
NoIntervenant : clé étrangère faisant référence à NoPersonnel de la table PERSONNEL

L'attribut État permet de connaître l'état actuel de l'incident : "ouvert" à la déclaration de l'incident, "en cours" après la première intervention et "fermé" après la dernière intervention.
L'attribut NoIntervenant indique le numéro de la personne chargée de la réparation.

INTERVENTION(NoIntervention, NoIncident, DateIntervention, Action, Commentaire)
NoIntervention : clé primaire
NoIncident : clé étrangère faisant référence à NoIncident de la table INCIDENT

Document 2.4 : extrait de la table de filtrage du routeur du centre de données

Le routeur de distribution du centre de données (*datacenter)* doit autoriser ou non l'accès aux zones démilitarisées (DMZ) où sont placées les ressources. Les règles de filtrage pour permettre l'accès aux zones démilitarisées depuis les différents sous-réseaux associés au *«corpoworking »* du site de Paris devront être définies sur la base du modèle ci-dessous.

No de règle	Interface	Entrée / Sortie	adresse IP source/masque	port source	adresse IP destination/masque	port destination	Accepte / Bloque
1	10.10.127.254	Entrée	10.10.0.0/17	*	10.1.1.0/24	*	Accepte
2	10.10.127.254	Entrée	10.10.128.0/24	*	10.1.2.0/24	*	Accepte
3	10.10.127.254	Entrée	*	*	*	*	Bloque

Remarque : Cette table ne préjuge pas de l'authentification des niveaux supérieurs

Document 2.5 : extrait de la documentation du pare-feu

Source : documentation de l'équipement

CONTRÔLE DES USAGES
Mode Firewall/IPS/IDS, Firewall basé sur l'identité des utilisateurs, Firewall applicatif, Microsoft Services Firewall, Détection et contrôle de l'usage des terminaux mobiles, Inventaire des applications (option), Détection des vulnérabilités (option), Filtrage par localisation (pays, continents), Filtrage d'URLs (base embarquée ou mode *Cloud*), Authentification transparente (Agent SSO Active Directory, SSL, SPNEGO), Authentification multi-user en mode cookie (Citrix- TSE), Authentification mode invité, programmation horaire par règle.

Dossier documentaire n° 3 spécifique à la partie 2A

Document 3.1 : exemples d'exploitation du contexte ODBY orientés « réseaux et systèmes »

Le contexte organisationnel ODBY a déjà été mobilisé par l'équipe pédagogique l'année dernière avec deux approches différentes :

– approche n°1. La mise à disposition d'un espace de « *corpoworking*» nécessite la mise en place de nouveaux sous-réseaux, de segmenter les flux en provenance des réseaux sans fil et filaire et de limiter les accès aux seules ressources autorisées par la direction des systèmes d'information (DSI). La sécurisation des accès au réseau nécessitera un éventuel marquage des trames entre les points d'accès et le contrôleur Wi-Fi ainsi que la mise en place d'un serveur d'authentification 802.1x (Radius).

Documents 3.2 à 3.8

– approche n°2. ODBY est dans l'obligation de conserver les journaux systèmes des accès internet des utilisateurs. L'administrateur réseau souhaite automatiser la gestion de ces journaux et disposer d'un système de notification par courriel du bon déroulement des opérations. De plus, la consultation de ces journaux doit être facilitée en cas de demande des autorités.

Documents 3.9 à 3.14

Document 3.2 : extrait des tables de routage des routeurs de Paris.

Extrait table de routage du routeur de distribution de Paris avant l'espace de « *corpoworking* »

Destination	Masque	Passerelle	Présence Agent relais DHCP sur interface
10.10.1.0	255.255.255.0	10.10.1.254	Oui → 10.1.1.10
10.10.126.0	255.255.255.0	10.10.126.254	Oui → 10.1.1.10
0.0.0.0	0.0.0.0	10.10.127.253	Non

Extrait table de routage du routeur d'accès de Paris le avant l'espace de « *corpoworking* »

Destination	Masque	Passerelle	Interface
10.10.0.0	255.255.128.0	10.10.127.254	10.10.127.253
0.0.0.0	0.0.0.0	Non communiqué	Non communiqué

Document 3.3 : notes d'étude pour le réseau sans fil

Document de travail de l'équipe « Réseaux & Systèmes »
La solution que nous proposons sera basée sur des contrôleurs Wi-Fi. En effet, avec des points d'accès autonomes, la configuration logique et physique doit être définie pour chacun d'eux. En cas d'incident il faut donc intervenir sur chaque borne. Avec le contrôleur, la configuration est définie à son niveau, les points d'accès ne sont plus alors que des "antennes".

Par exemple :

- en cas de problème d'émission, l'intervention au niveau du contrôleur permet de modifier dynamiquement les paramètres physiques d'émission (fréquence, canal, puissance .etc.) ;
- en cas d'attaque ou de dysfonctionnement, on peut souhaiter arrêter la diffusion d'un SSID au niveau du contrôleur.

Pour la DSI il y a donc un double avantage : facilité et souplesse de l'administration, sécurité et réactivité des configurations.

Nous avons choisi la solution WPA2-Entreprise qui s'appuie sur le serveur Radius et le serveur LDAP de l'entreprise pour les usagers internes. Cette contrainte de définir les utilisateurs dans l'annuaire de l'entreprise serait trop lourde pour les usagers extérieurs. Mais dans la mesure où les espaces accessibles sont séparés, on peut estimer que la sécurité par clé partagée (WPA2-PSK) est suffisante pour cette catégorie d'utilisateur.
Les flux en provenance du réseau sans fil et circulant dans le réseau filaire doivent impérativement être maîtrisés. Entre les points d'accès et le contrôleur Wi-Fi, le seul VLAN utilisé sera le VLAN de management il n'y a donc pas besoin de marquer les trames avec un identifiant 802.1q.

Voici les éléments d'implémentation que nous avons retenus :

- chaque point d'accès diffusera l'ensemble des SSID pilotés par un contrôleur Wi-Fi ;
- le nombre de points d'accès sans fil et leur implantation seront déterminés sur chaque site en fonction d'une étude de couverture ;
- chaque point diffusera trois SSID correspondant aux trois catégories d'utilisateur. Le chiffrage pour les SSID sera un chiffrage fort de type WPA2 (CCMP) ;
- pour les usagers internes, l'accès au SSID nécessitera une authentification de type WPA-Entreprise avec un serveur Radius qui consultera le serveur LDAP central ;
- pour les autres usagers une simple authentification de type WPA2-Personnel (PSK) sera requise.

Document 3.4 : propositions pour la segmentation du réseau filaire spécifique au « *corpoworking* »

Document de travail de l'équipe « Réseaux & Systèmes »

- chaque SSID sera associé à un VLAN dans le réseau filaire ;
- entre le contrôleur Wi-Fi et les points d'accès s'établira un tunnel CAPWAP (*Control And Provisioning of Wireless Access Point*) ;
- le tunnel CAPWAP permettra au contrôleur de contrôler et de configurer dynamiquement et en temps réel les points d'accès sans fil (tant physiquement : paramétrage des fréquences et puissance d'émission par exemple, que logiquement : diffusion ou non des SSID et chiffrage par exemple) ;
- les points d'accès transmettront les données en provenance de chaque SSID dans le tunnel CAPWAP ;
- le tunnel CAPWAP utilisera un VLAN de management ;
- en sortie du tunnel CAPWAP, le contrôleur Wi-Fi transmettra les données provenant de chaque SSID dans le VLAN correspondant ;
- les liens entre les points d'accès et le commutateur d'accès ne nécessiteront pas un marquage des trames par un identifiant 802.1q ;
- entre le contrôleur et commutateur d'accès il faudra par contre activer le marquage 802.1q pour identifier les différents VLAN.

Document 3.5 : sécuriser le BYOD dans l'espace de « *corpoworking* »

Extrait d'un échange entre le DSI et le responsable et l'équipe Réseaux et Systèmes :

« La DSI ne peut empêcher l'utilisation du matériel personnel dans l'espace de « *corpoworking* », ce serait contraire aux objectifs de la direction des ressources humaines. Les nouveaux usages tels que le BYOD (*Bring Your Own Device* : "Apportez votre équipement personnel de communication ») deviennent de toutes façons incontournables. Il appartient donc à votre équipe de trouver des solutions adaptées à ce nouveau défi pour la sécurité de notre système d'information". "L'accès internet pour l'entreprise est centralisé ; un pare-feu protège notre réseau local. Dans un environnement BYOD on n'est pas sûr que les machines soient à jour au niveau du système et des logiciels notamment en ce qui concerne les mises à jour de sécurité (vulnérabilités). La centralisation de l'accès internet et les options de notre pare-feu permettent de procéder de façon dynamique à

ce contrôle en alertant les utilisateurs sur les problèmes et en bloquant les machines trop vulnérables (exemple : Network Access Protection). »
« Les comportements et les bonnes pratiques des usagers de l'espace sont la clé de la réussite du projet. La présence de personnes extérieures à ODBY doit être prise en compte dans notre politique de sécurité. Vous devez nous aider à proposer une liste limitée de bonnes pratiques destinées à tous les usagers pour les sensibiliser à la confidentialité de leurs données. »

« Une des premières mesures à proposer à nos usagers est de les sensibiliser à ne pas laisser un ordinateur avec une session ouverte, ce qui permettrait à quelqu'un :

- d'introduire sans difficulté un logiciel malveillant sur le poste, sur le réseau, etc ;
- de voler/détruire/compromettre des données personnelles ou d'entreprise ;
- d'utiliser la messagerie électronique à l'insu de l'utilisateur connecté... ».

Document 3.6 : schéma logique du réseau Wi-Fi

Document de travail de l'équipe « Réseaux & Systèmes »

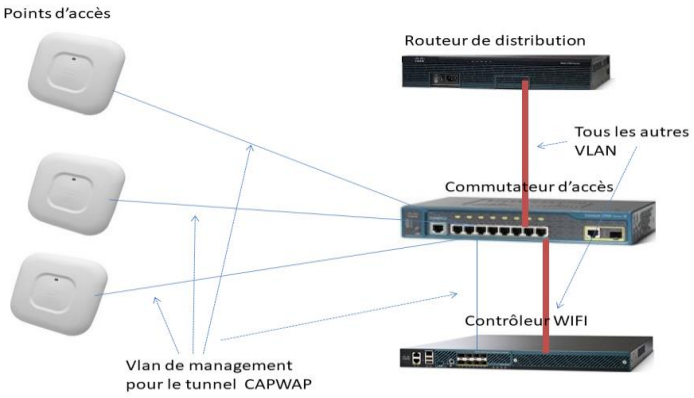
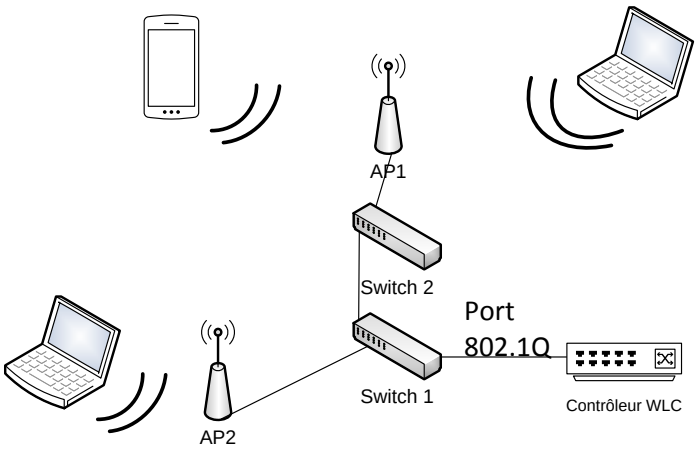


Schéma logique du WIFI

Document 3.7 : contrôleur Wi-Fi

Un point d'accès Wi-Fi (ou borne) est un dispositif qui permet aux périphériques sans fil de se connecter à un réseau câblé ou à un accès au réseau internet à l'aide d'une connexion par ondes radio. Pour que le point d'accès puisse fonctionner, il faut qu'il soit raccordé par un câble à un autre équipement, que ce soit un routeur ou un commutateur par exemple.
Un contrôleur Wi-Fi (WLC – Wireless LAN Controller) permet d'implémenter la gestion de réseaux sans fil complexes en centralisant la configuration de points d'accès sans fil. Le point d'accès émet un signal afin de faire le lien entre une communication sans-fil et le réseau filaire.
Le but du point d'accès est de faire le lien entre une communication sans-fil et le réseau filaire. Dans le cas de l'utilisation d'un contrôleur Wi-Fi, le fonctionnement est le suivant :

- d'un côté, il reçoit/envoie des trames dans les airs pour les clients Wi-Fi ;
- de l'autre côté (il est connecté à un commutateur), il reçoit/envoie des trames depuis/vers un boîtier intelligent dit WLC (*Wireless LAN Controller*).



Le contrôleur est branché sur un port tagué 802.1Q pour pouvoir envoyer les trames sur le VLAN adéquat.
Les bornes sont branchées sur des ports associés au vlan de management Wi-Fi pour pouvoir *discuter* avec le contrôleur.

Le boîtier WLC contrôle à distance toutes les bornes d'accès et c'est sur ce boîtier que l'administrateur va se connecter. Toute la configuration s'y trouve et c'est le WLC qui va commuter/router les trames vers les bonnes destinations et non plus les bornes elles-mêmes. Dans ce cas on parle de bornes dites "légères", car elles contiennent très peu de configuration et ne peuvent fonctionner qu'en présence d'un contrôleur.
Fonctionnement simplifié :

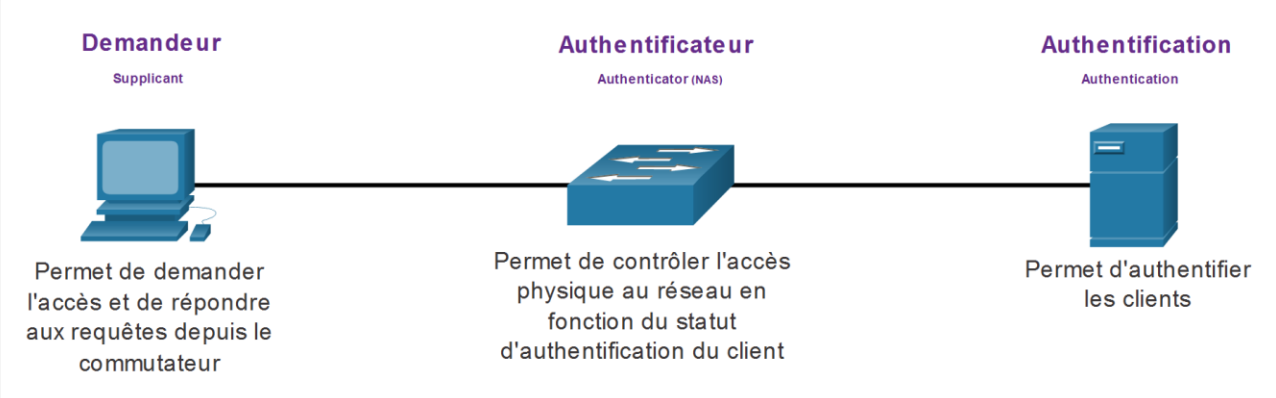
1. la borne démarre électriquement ;
2. son interface filaire va envoyer une requête DHCP pour récupérer une adresse IP ;
3. une fois reçue, elle va contacter son WLC ;
4. le WLC va lui envoyer sa configuration minimale avec tous les paramètres nécessaires au bon fonctionnement (SSID – un ou plusieurs -, puissance, canal, etc.) ;
5. une fois configurée, la borne envoie tout le trafic des clients Wi-Fi au contrôleur qui se chargera de les envoyer vers les bonnes destinations.

Document 3.8 : norme IEEE 802.1X

Source : *d'après Cisco NetAcad*

La norme IEEE 802.1X est un protocole de contrôle d'accès et d'authentification basé sur les ports. Ce protocole empêche les stations de travail non autorisées de se connecter à un réseau local via des ports de commutation accessibles au public. Avant de mettre à disposition les services offerts par le commutateur ou le LAN, le serveur d'authentification authentifie chaque station de travail connectée à un port de commutation.
Avec l'authentification basée sur le port 802.1X, les périphériques du réseau ont des rôles spécifiques, comme illustré sur la figure ci-après.

- **Client (Demandeur)** : il s'agit d'un périphérique équipé d'un logiciel client conforme à la norme 802.1X, disponible pour les périphériques avec ou sans fil.
- **Commutateur (Authentificateur – NAS-)** : le commutateur sert d'intermédiaire entre le client et le serveur d'authentification. Il demande les informations d'identification du client, vérifie ces informations auprès du serveur d'authentification, puis transmet une réponse au client. Un autre dispositif qui pourrait servir d'authentificateur est le point d'accès sans fil.
- **Serveur d'authentification** : le serveur valide l'identité du client et informe le commutateur ou le point d'accès sans fil que le client est ou n'est pas autorisé à accéder au LAN et aux services de commutateur.



Document 3.9 : exemple d'architecture RADIUS pour le réseau Wi-Fi

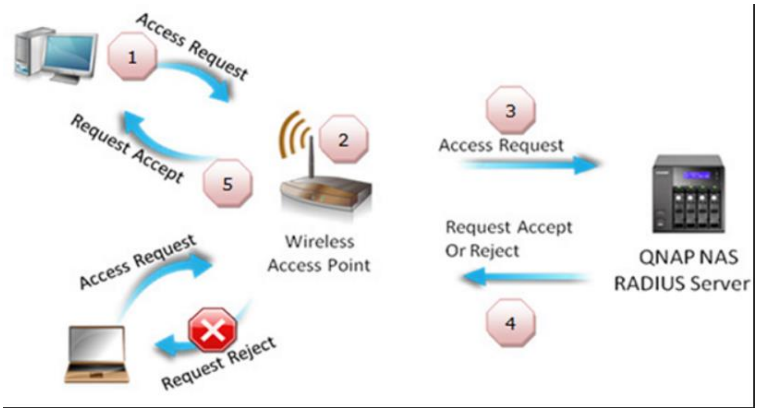
Source : d'après Cisco NetAcad et documentation QNAP

Dans les réseaux qui ont des exigences de sécurité strictes, une authentification ou une connexion supplémentaire est requise pour accorder l'accès aux clients sans fil. Le choix du mode de sécurité d'entreprise (WPA2 Entreprise par exemple) nécessite un serveur RADIUS (*Remote Authentication Dial In User Service*) d'authentification, d'autorisation et de comptes (AAA).
Les éléments ci-dessous doivent être configurés sur le point d'accès Wi-Fi (AP) :

- adresse IP du serveur RADIUS : Il s'agit de l'adresse accessible du serveur RADIUS ;
- numéros de port UDP : ports UDP officiellement attribués 1812 pour l'authentification RADIUS et 1813 pour la comptabilité RADIUS, ou à l'aide des ports UDP 1645 et 1646 ;
- clé partagée : utilisée pour authentifier l'AP (Access Point ou borne) avec le serveur RADIUS.

L'authentification et l'autorisation des utilisateurs sont gérées par la norme 802.1X, qui fournit une authentification centralisée sur le serveur des utilisateurs finaux.
La fonctionnalité de serveur RADIUS du NAS QNAP permet de gérer les authentifications et autorisations de manière centralisée, et donc, de se connecter à des services réseau et de les utiliser.
Les authentifications PAP, EAP-TLS/PAP et EAP-TTLS/PAP sont les seules à être prises en charge pour les comptes d'utilisateur système. Seules les bornes compatibles avec les normes WPA-enterprise et 802.1X sont prises en charge.

1. Les utilisateurs demandent des autorisations d'accès au réseau sans fil.
2. Le point d'accès sans fil reçoit la demande et la transfère au serveur RADIUS (NAS QNAP).
3. Le serveur RADIUS la reçoit et traite les informations.
4. Le serveur RADIUS renvoie le résultat au routeur sans fil.



Le point d'accès sans fil autorisera ou refusera l'utilisateur selon les résultats renvoyés par le serveur RADIUS.

Document 3.10 : implémentation de la centralisation des journaux (*logs*)

ODBY possède un serveur syslog qui permet de centraliser le journal (*log*) de l'ensemble des serveurs. ODBY a choisi de néanmoins conserver un fichier log en local sur chaque client du serveur syslog.
En cas de plantage d'un client du serveur syslog, il sera possible de récupérer les erreurs et actions menées sur le serveur avant que celui-ci soit indisponible, facilitant ainsi la recherche des causes du plantage.

Nous avons choisi de conserver un fichier log en local, car en cas de panne réseau ou d'indisponibilité du serveur de logs centralisé, on pourra toujours consulter les traces de chaque machine, équipements ou services.
Chaque serveur virtuel comporte les caractéristiques suivantes :

- un nom interne pleinement qualifié “nom_interne_du_serveur.odby .local” ;
- une réservation d’adresse IP ;
- une synchronisation avec le serveur de temps ntp ;
- un accès à distance SSH via une authentification clé privée / clé publique ;
- tous les logs de sévérité de 0 à 3 (emerg, alert, crit, err) sont redirigés vers le serveur syslog.

Chaque nouveau serveur ou nouvel équipement est paramétré comme client du serveur syslog.
Il suffit d’ajouter une ligne dans le fichier syslog.conf du serveur dédié au nouveau serveur mentionnant toutes les fonctionnalités (*) et les messages de sévérité inférieure ou égale à 3 (err, crit, alert et emerg) et son adresse IP précédée de @, comme ci-dessous :
*.err @10.10 .30.21:514

Document 3.11 : exploitation et conservation des journaux systèmes

Problème constaté
Des utilisateurs signalent des lenteurs lors des téléchargements sur internet. L’administrateur souhaite vérifier si de gros téléchargements ont eu lieu afin de pouvoir expliquer ces ralentissements. Pour cela, un script en bash interroge les journaux (*logs*) du proxy squid.

Exemple de script proposé
Par défaut le script recherche des chargements >= 10^8 octets soit 100 Mo dans les 9 derniers journaux de log. On peut surcharger cette valeur en paramètre : « ./gros-access 9 » par exemple affichera tous les téléchargement > 10^9 octets soit 1Go. Un filtre avec une expression régulière est utilisé.

```
#!/bin/bash
## Récupère l'ordre de grandeur recherché soit le paramètre passé soit par défaut 9 cad 10^8
if [ "$1" == "" ]; then
  og=9
else
  let og=$1+1
fi
## Affiche tous les chargements de taille > à l'ordre de grandeur depuis le plus ancien log archivé vers le plus récent
for i in `seq 9 -1 2`; do
  cat /var/log/squid/access.log.$i | egrep "TUNNEL" | expand | tr -s " " " " | cut -d " " -f 1,3,5,7,8| egrep "\ .*\ [0-9]{$og,}"
done
## Fini avec le log en cours
cat /var/log/squid/access.log | egrep "TUNNEL" | expand | tr -s " " " " | cut -d " " -f 1,3,5,7,8| egrep "\ .*\ [0-9]{$og,}"
```

Document 3.12: exemples d’extraits de fiches de savoirs

Fiche de savoir n°1 : traçabilité des évènements

Adapté de l’ouvrage Cybersécurité des services informatiques, BTS SIO 1ère année, édition DELAGRAVE, page 173

La traçabilité permet de suivre les actions réalisées au sein d’un système informatique. Elles sont enregistrées dans des journaux (*logs*) qui peuvent servir de preuves numériques.
L’ANSSI recommande d’enregistrer les événements suivants :

Évènements	Exemples
Authentification	Réussites et échecs d’authentification, utilisation des différents mécanismes d’authentification, élévation de privilèges.
Gestion des comptes et des droits	Ajouts, suppressions de comptes ou de groupes, affectations ou suppressions de droits aux comptes ou aux groupes,

	modifications des données d'authentification.
Accès ou modification des ressources et des configurations	Accès ou tentatives d'accès en lecture, écriture ou exécution aux ressources et aux applications. Réinitialisation de configurations.
Activité des processus (programmes) et des systèmes (matériels et systèmes d'exploitation)	Démarrages ou arrêts, dysfonctionnements, surcharges du système, chargement ou déchargement de modules, activité matérielle (défaillance, connexions, déconnexions).

Afin que l'exploitation juridique des preuves numériques soit garantie, l'ANSSI recommande également d'appliquer les procédures ci-dessous :

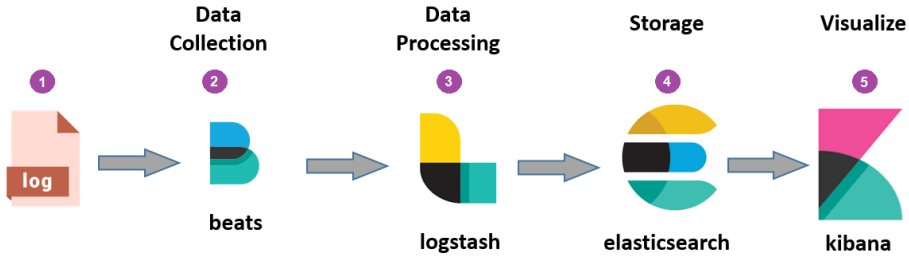
- enregistrement des journaux systèmes dans un format lisible et facilement consultable ;
- centralisation des journaux systèmes afin d'éviter l'utilisation de plusieurs sources incohérentes ;
- horodatage correct via un serveur de temps qui met à l'heure exacte les serveurs et les machines (protocole NTP) ;
- transfert en temps réel des évènements enregistrés sur le serveur de journaux (*logs*) afin de disposer d'une photographie exacte des faits enregistrés au moment de la consultation des traces ;
- transit des journaux systèmes via un réseau dédié avec une bande passante minimale garantie.

Fiche de savoir n°2: outils de filtrage des journaux systèmes

L'utilisation d'expressions régulières permet d'effectuer des filtres de recherche d'informations sur des journaux systèmes volumineux. Ces filtres peuvent s'utiliser nativement via des commandes systèmes (*grep, sed, less, tail* sous Linux par exemple). Certains filtres nécessitent une construction plus élaborée via des motifs (*patterns*) sur des métacaractères ($ pour une position de fin de chaîne, ^83 pour toute chaîne commençant par 83, [A-Z]{2,4} pour toute chaîne qui contient 2 à 4 lettres consécutives en majuscules...).

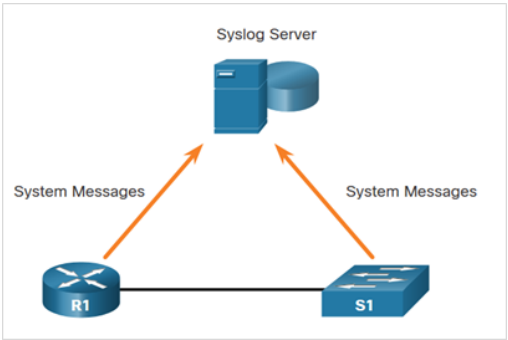
Fiche de savoir n°3: description de la suite Elastic Stack

Lorsque le volume des journaux systèmes est très important et que les sources de collecte sont multiples, des outils comme ELK peuvent être utilisés pour automatiser la recherche d'informations pertinentes. ELK est un acronyme pour une suite libre (*open source*) réunissant 3 produits intégrés : Elasticsearch, Logstash et Kibana qui permettent de collecter n'importe quel format de données depuis n'importe quelle source, puis d'interroger, d'analyser et de visualiser les données afin de pouvoir réagir aux évènements en temps réel. Ces outils permettent de travailler avec une interface graphique permettant une visualisation plus aisée des informations.



Source : d'après elastic.co

Document 3.13 : serveur Syslog



Syslog est un protocole implémenté sur des systèmes comme Windows ou Linux et des périphériques réseaux définissant un service de journaux d'événements d'un système informatique. C'est aussi le nom du format qui permet ces échanges.
Ce protocole permet donc de transporter les messages de journalisation générés par les applications ou le système vers une machine hébergeant un serveur Syslog.
Syslog se compose d'une partie cliente et d'une partie serveur. La partie cliente émet les informations sur le réseau, via le port UDP 514. Les serveurs collectent l'information et se chargent de créer les journaux.

La priorité du message est un indice qui permet, lors de son exploitation, de le traiter suivant un ordre de criticité. Elle est calculée en fonction de sa catégorie et de sa sévérité : *(8 * catégorie) + sévérité*.

La sévérité (ou niveau de gravité) d'un message correspond au degré d'urgence du message. Les huit sévérités existantes sont définies par les demandes de commentaires (RFC) :

Code	Gravité	Mot-clé	Description
0	Emergency	emerg (panic)	Système inutilisable.
1	Alert	alert	Une intervention immédiate est nécessaire.
2	Critical	crit	Erreur critique pour le système.
3	Error	err (error)	Erreur de fonctionnement.
4	Warning	warn (warning)	Avertissement (une erreur peut intervenir si aucune action n'est prise).
5	Notice	notice	Événement normal méritant d'être signalé.
6	Informational	info	Pour information.
7	Debugging	debug	Message de mise au point.

La catégorie d'un message correspond au type d'application générant le message. 24 fonctionnalités existantes sont définies par la demande de commentaires RFC 3164.

Configuration du serveur Syslog et des clients

Sur un serveur Linux, la configuration se réalise dans le fichier **/etc/rsyslog.conf** qu'il faut paramétrer comme suit pour qu'il accepte les logs venant de l'extérieur en écoutant sur le port UDP 514 :

```
#provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514
```

Sur un client Linux, la configuration se réalise dans le fichier /etc/rsyslog.conf en ajoutant une ou plusieurs lignes de la forme suivante :

```
Catégorie.Sévérité @adresseIPDestination:port
```

Par exemple :

. @192.168.1.100:514	envoie tous les logs au serveur syslog dont l'adresse IP est 192.168.1.100
mail.info @192.168.100:514	envoie uniquement les messages dont la catégorie est liée au service mail et la sévérité est inférieure ou égale à « information » (0<=sévérité<=6)
"<19>sept 12 14:46:18 172.16.201.27 Message d'erreur du Service Mail"	correspond à un message envoyé par un client dont l'adresse IP est 172.16.201.27

Dossier documentaire n° 4 spécifique à la partie 2B

Document 4.1 : exemples d'exploitation du contexte ODBY orientés « développement »

Le contexte organisationnel ODBY a déjà été mobilisé par l'équipe pédagogique l'année dernière avec deux approches différentes.

Approche n°1 : une problématique de codage et de modélisation (documents 4.2 à 4.7).

Il faut développer et documenter les fonctionnalités de l'application en cours de développement.
Les modèles fournis sont à s'approprier par les étudiants : compréhension du diagramme de classes, accesseurs, mutateurs, classes techniques, compréhension du cas d'utilisation.
Leur capacité à les exploiter, s'en inspirer, les faire évoluer, s'exprime avec les fonctionnalités à développer :
-affectation de tâches à un lot (méthode *donneTachesAAffecter* de la classe Lot) ;
-adaptation du diagramme de classes pour distinguer projets internes et externes et implémentation de l'héritage ;
-modélisation du cas d'utilisation de création des lots d'un projet et maquettage de l'interface.

– Approche n°2 : une problématique de suivi et déploiement de l'application (documents 4.8 à 4.11).
Il faut sensibiliser les étudiants à la mise en place, dès le début du projet, d'une organisation agile : de la gestion de version du code source produit par l'équipe des développeurs à la mise en production des versions de l'application.
Cette organisation s'inscrit dans une démarche d'intégration continue, systématique, automatique, avec la nécessité de tester le code et de disposer d'indicateurs sur le déroulement des opérations.
Faire pratiquer aux étudiants le découpage en lots-tâches, affecter des priorités aux tâches et les regrouper en itérations (*sprints*), poser des jalons, proposer la mise en place d'une plateforme d'intégration continue : celle-ci doit permettre d'enchaîner les tests, à illustrer par le test unitaire de la méthode *pourcentageAvancement*() de la classe Projet. La plateforme doit également permettre la création dynamique de l'infrastructure nécessaire à l'application, comme une base de données et superviser les composants nécessaires à son fonctionnement.
Enfin, il faut préparer les étudiants à rendre compte de l'avancement d'un projet, au moyen d'un langage d'interrogation des données : quels sont les développeurs qui ont collaboré à un projet, quel est le nombre de commit par branche d'un projet, etc.

Document 4.2 : application de gestion des projets agiles

Avec la mise en place des espaces de « *corpoworking* », ODBY souhaite favoriser le travail en projet. Ainsi, des équipes vont s'y retrouver pendant quelques semaines ou quelques mois pour collaborer. La société, qui veut tendre vers plus d'agilité, va accompagner les « *corpoworkers* » en leur proposant une application spécifique de suivi de projet inspirée de la méthode agile Scrum. Même si l'approche reste itérative et collaborative, elle a été simplifiée afin d'assurer une transition douce des modes de travail.
Chaque projet est ainsi découpé en lots de tâches. Ces lots sont constitués au fur et à mesure de l'avancement du projet car les priorités peuvent être revues par le.la responsable du projet en cas de nécessité. Les tâches sont ensuite confiées aux collaborateurs qui en assureront la réalisation et les tests. Donc, chaque projet géré via cette application contient une liste de tâches qui restent à réaliser, triée par ordre décroissant des priorités. Les tâches les plus urgentes se trouvent ainsi au début de cette liste triée. Un projet passera, au fil du temps, par trois états :

- en attente : tant qu'il n'a pas réellement démarré ;
- en cours : lorsqu'il est en cours de réalisation ;
- terminé : lorsque l'ensemble de ses lots est terminé.

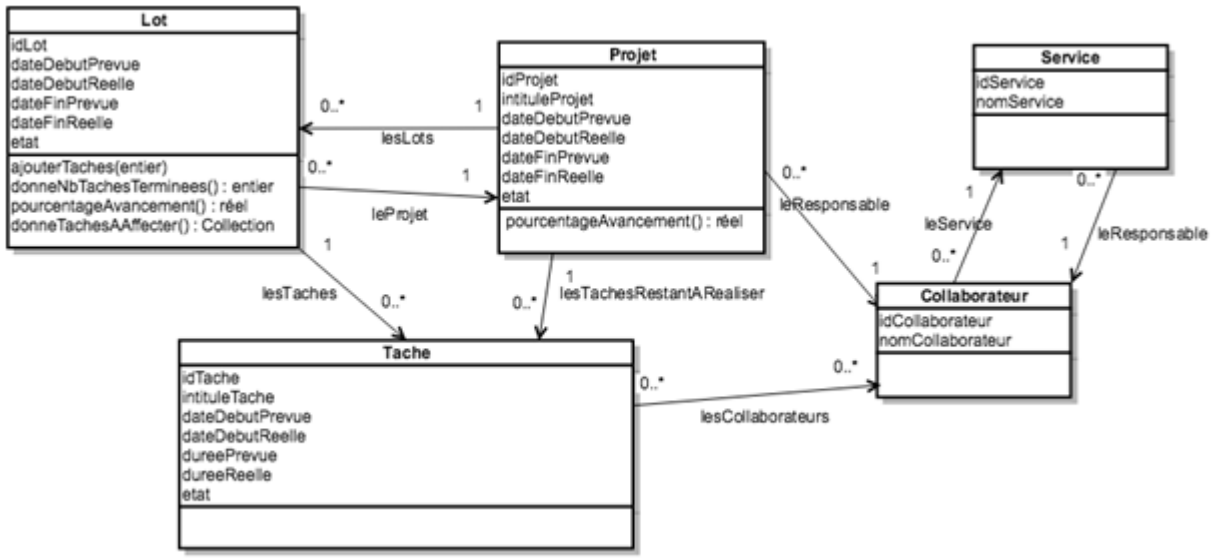
Le principe est le même pour un lot qui pourra prendre trois états : « en attente », « en cours » et « terminé » lorsque l'ensemble de ses tâches est terminé.

À chaque réunion d'avancement, au moins un nouveau lot de tâches est constitué en prélevant, par ordre d'importance de priorité, un nombre de tâches donné à la liste triée des tâches restant à réaliser pour le projet ; les tâches prélevées disparaissent donc de cette liste. Une tâche passera, au cours de son cycle de vie, par plusieurs états :

- en attente de lot : tant qu'elle se trouve dans liste des tâches restant à réaliser du projet. Dès que la tâche intègre un lot, elle passe à l'état "à affecter" à un ou plusieurs collaborateurs ;
- à affecter : lorsqu'elle fait partie d'un lot mais attend qu'un ou plusieurs collaborateurs lui soient affectés ;
- en cours : lorsqu'elle a été affectée à un ou plusieurs collaborateurs ;
- à tester : lorsque la réalisation de la tâche est terminée et qu'elle attend un testeur ;
- en test : lorsque la tâche est testée ;
- terminée : lorsque le test est validé et que la tâche est terminée.

Lorsque toutes les tâches d'un lot sont terminées, celui-ci est considéré comme terminé. Il en va de même pour le projet qui est considéré comme terminé lorsque ses lots le sont.

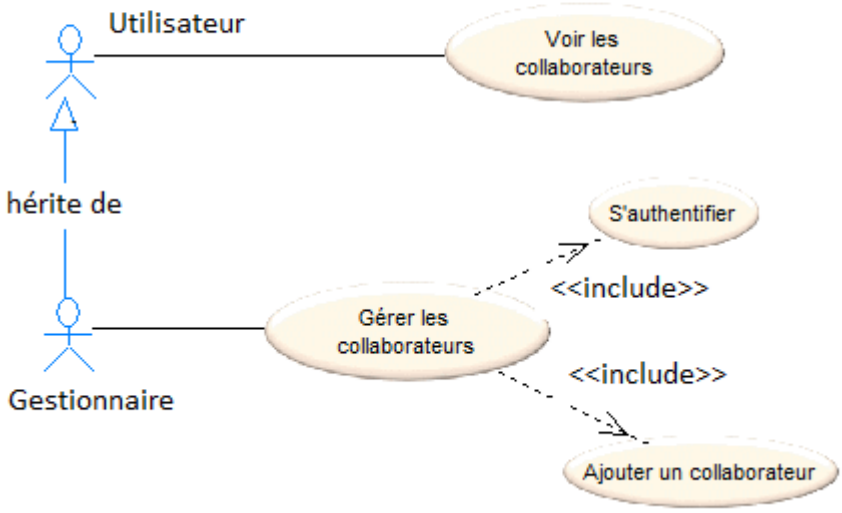
Document 4.3 : diagramme de classes de l'application de gestion des projets agiles



Les constructeurs, accesseurs et mutateurs des attributs des classes ne figurent pas sur le diagramme.
Le système utilise les classes techniques Date et Collection qui ne sont pas représentées

Document 4.4 : extrait du cas d'utilisation de l'application de gestion de projet

Gérer les collaborateurs		
Diagramme de cas d'utilisation		
Version : 1	Créé le : 24/3/2021	Modifié le : 24/3/2021



PROJET : Gestion des projets agile	Description cas d'utilisation
Nom cas d'utilisation : Gérer les collaborateurs	
Acteur déclencheur : Le gestionnaire	
Pré condition : être authentifié Post conditions : Néant	
Scénario nominal : 1. Le gestionnaire demande à ajouter un nouveau collaborateur 2 Le système retourne un formulaire de saisie 3 Le gestionnaire sélectionne le service, saisit le nom du collaborateur et valide 4 Le système enregistre le nouveau collaborateur en générant l'identifiant aléatoire Extension : 3.1 Le service n'existe pas. Le gestionnaire demande à créer un nouveau service 3.1.1 Le système retourne un formulaire de création d'un service 3.1.2 Le gestionnaire sélectionne le responsable, saisit le nom du service puis valide 3.1.3 Le système enregistre ce nouveau service Exceptions : 3.1 Le nom du collaborateur n'est pas renseigné 3.1.a Le système en informe le gestionnaire, retour à 2	

Document 4.5 : environnement de base de données relationnelle

Pour permettre un développement efficace et une meilleure évolutivité du code, la persistance des données est fournie par l'outil Hibernate, qui gère la persistance des objets dans une base de données relationnelle (ORM *object-relational mapping*). L'outil Hibernate apporte une solution aux problèmes d'adaptation entre le paradigme objet et les SGBD en remplaçant les accès à la base de données par des appels à des méthodes objet de haut niveau.Ainsi son utilisation permet d'établir et maintenir la correspondance entre une table de la base de données et une classe du modèle objet métier.

La base de données contient les tables correspondant aux classes du modèle objet métier et leurs liaisons. De plus, la vue "vSuiviProjet" contenant les données liées Projet-Lots-Taches-Collaborateurs facilite la production d'indicateurs de suivi des projets.

Parmi les projets en cours, "resaplanning" est un développement logiciel de l'application de réservations des espaces partagés.

Ainsi la requête

```
Select distinct nomCollaborateur
From vSuiviProjet
Where idProjet = (select idProjet from projet where intituleProjet='resaplanning')
```

Retourne les noms des collaborateurs du projet intitulé "resaplanning"

Document 4.6 : implémentation de la classe Projet

```
//description textuelle des propriétés et méthodes de la classe
Classe Projet
- idProjet: entier
- intituleProjet: Chaine de caractères//intitulé du projet
- dateDebutPrevue: Date //date de début prévue du projet
- dateDebutReelle: Date //date de début réelle du projet
- dateFinPrevue: Date //date de fin prévue du projet
- dateFinReelle: Date //date de fin réelle du projet
- etat : Chaine de caractères// état du projet : en attente, en cours, terminé
- leResponsable: Collaborateur // responsable du projet
- lesTachesRestantARealiser: ListeTriee de Tache //contient l'ensemble des tâches restant à réaliser dans le projet. Ces tâches sont triées par ordre décroissant de priorité grâce à la classe technique ListeTriee
- lesLots: ListeTriee de Lot //contient l'ensemble des lots déjà réalisés ou en cours de réalisation du projet
+ pourcentageAvancement(): réel //retourne un pourcentage correspondant au nombre de tâches terminées au regard du nombre de tâches total du projet

//implémentation Java de la méthode pourcentageAvancement
public double pourcentageAvancement () {

//on récupère le nombre de tâches terminées des lots existants
int totalTerminees = 0 ;
int totalTaches = 0 ;

// parcourir les lots du projet
for (Lot unLot : lesLots) {
        totalTerminees = totalTerminees + unLot.donneNbTachesTerminees() ;
        totalTaches = totalTaches + unLot.getLesTaches().size() ;
  //ajouter les tâches en attente de lot du projet
  totalTaches = totalTaches +   this.lesTachesRestantARealiser.size() ;
```

```
  double pourcentage = totalTerminees / totalTaches * 100
   if ( pourcentage == 100) { this.setEtat(« terminé ») ; }
  }
  return (pourcentage);
}
```

La méthode size() retourne le nombre d'éléments d'une collection.

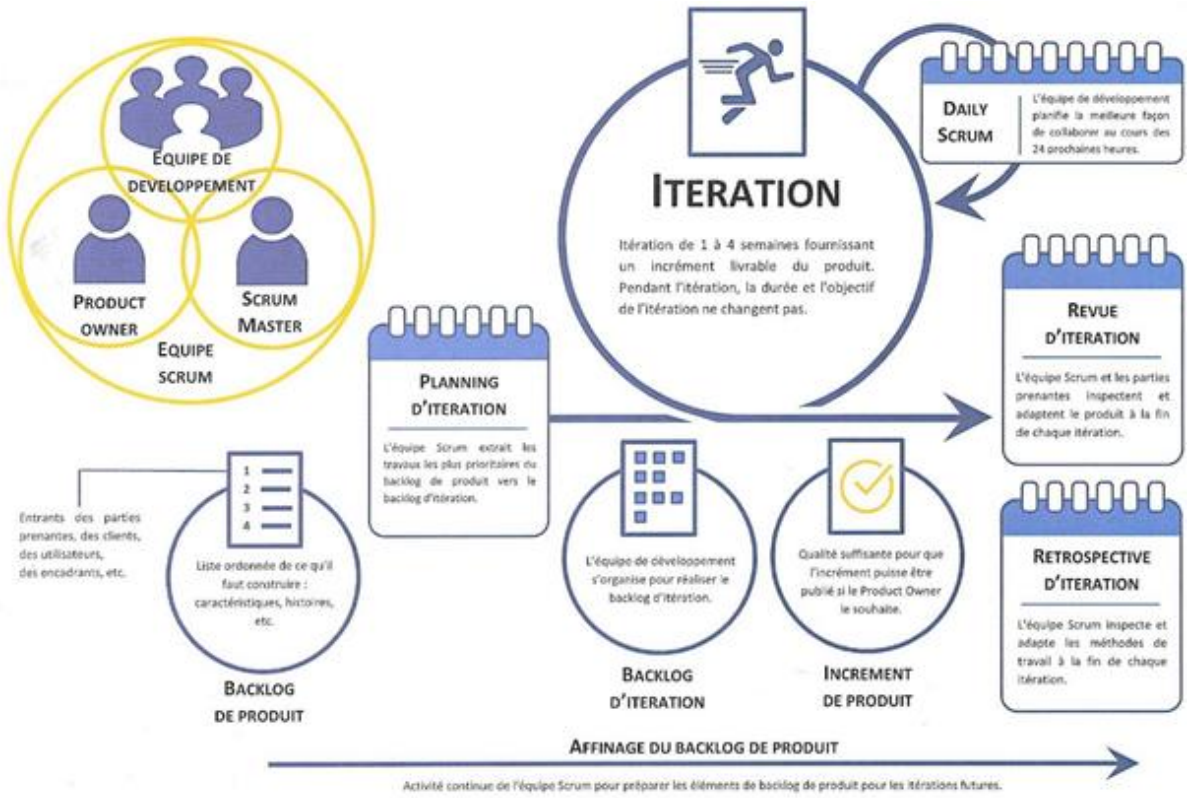
Document 4.7 : projets internes et projets des clients

La responsable de la DSI regrette que l'application actuelle de gestion des projets agiles n'intègre pas la distinction entre les projets destinés au groupe ODBY et les projets réalisés pour ses clients. En effet, dans le premier cas, il est nécessaire de connaître le ou les services de ODBY maîtres d'ouvrage du projet; dans le second, il faut impérativement identifier le client à qui le projet est destiné, notamment pour en connaître l'interlocuteur privilégié, ses coordonnées (adresse de messagerie et téléphone) et le budget associé.

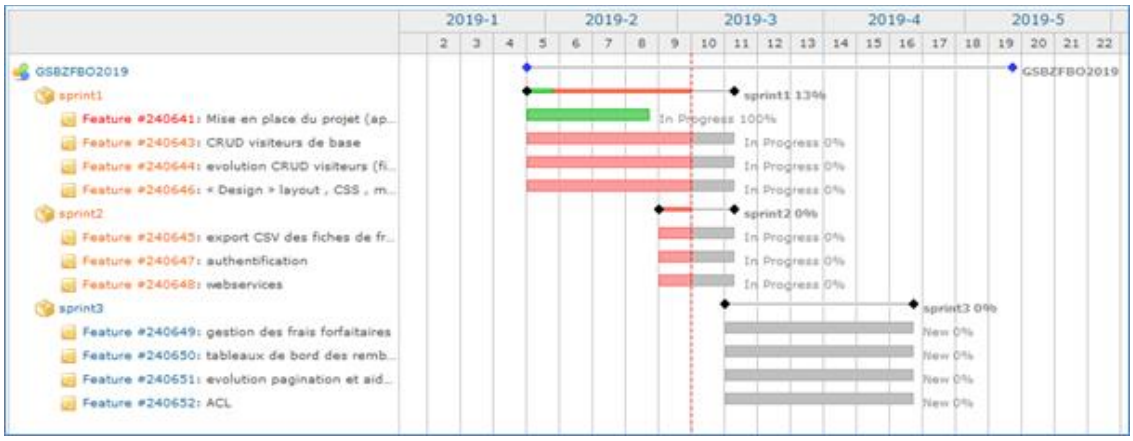
Une évolution du diagramme de classes actuel est nécessaire pour prendre en compte les besoins exprimés par la responsable de la DSI.

Document 4.8 : méthode SCRUM

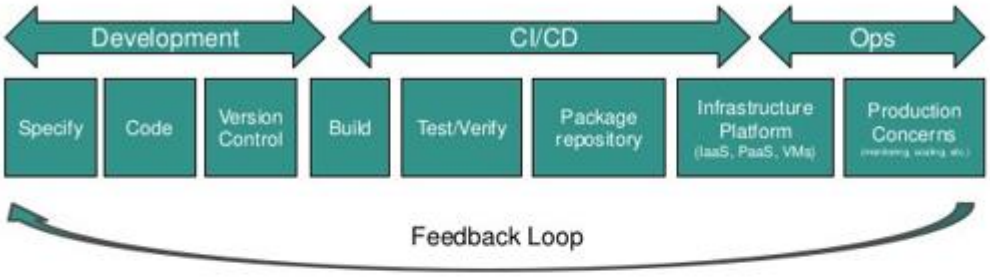
La méthode Scrum s'appuie sur le découpage d'un projet en « boîtes de temps », nommées sprints (« pointes de vitesse »). Les « *sprints* » peuvent durer entre quelques heures et un mois (avec un « *sprint* » médian à deux semaines). Chaque « *sprint* » commence par une estimation suivie d'une planification opérationnelle.
Le « *sprint* » se termine par une démonstration de ce qui a été achevé. Avant de démarrer un nouveau « *sprint* », 'équipe réalise une rétrospective. Cette technique analyse le déroulement du sprint achevé, afin d'améliorer ses pratiques. Le flux de travail de l'équipe de développement est facilité par son auto-organisation, il n'y aura donc pas de gestionnaire de projet.



Document 4.9 : itérations (*sprints*) de projet



Document 4.10 : intégration et déploiement continu



Source http://www.slideshare.net/cote/cicd-from-a-donkey-perspective

Une chaîne (pipeline) d'actions automatisées
Des scripts assurent l'enchainement des actions, y compris le déploiement d'une infrastructure à la volée (environnements de développement, de test, de production).
Déclencheur de la chaine : commit et fusion de code sur le dépôt
La chaine s'arrête si une étape échoue.

Document 4.11 : test unitaire

```
public void testAjouterCollaborateur()
{
   // création de deux  instances de collaborateur
    Collaborateur C1 = new Collaborateur(1;"Renaud");
    Collaborateur C2 = new Collaborateur(2;"Delattre");

  // création d'une instance de Tache
    Tache TacheTest = new Tache(1, "Réaliser les tests", new DateTime(2021, 02, 15), new DateTime(2021, 02,
15),3,3,"terminée");

   // Ajout de deux collaborateurs
    TacheTest.AjouterCollaborateur(C1);
  TacheTest.AjouterCollaborateur(C2);


    nbCollaborateurs = TacheTest.getLesCollaborateurs().size();
  Assert.AreEqual(nbCollaborateurs,2, "erreur");

}
```

La classe technique **Assert** contient différentes méthodes statiques permettant de savoir si le test unitaire a réussi ou non. Elle contient la méthode ***AreEqual*** dont voici la signature :

public **static** void AreEqual(double expected, double actual, string message)

expected : valeur de type double contenant la valeur attendue
actual : valeur de type double contenant la valeur obtenue
message : message à afficher si l'assertion échoue, c'est-à-dire lorsque la valeur attendue est différente de la valeur obtenue.