BTS SERVICES INFORMATIQUES AUX ORGANISATIONS	SESSION 2016

E5SR : PRODUCTION ET FOURNITURE DE SERVICES

Durée : 4 heures	Coefficient : 5

CAS RIOCA

Ce sujet comporte 16 pages dont un dossier documentaire de 11 pages.
La candidate ou le candidat est invité.e à vérifier qu'il est en possession d'un sujet complet.

Conformément aux recommandations du Haut Conseil à l'Égalité entre les femmes et les hommes dans son guide publié en novembre 2015, l'expression du féminin et du masculin s'effectue en utilisant le point, par exemple, client.e.

Aucune calculatrice n'est autorisée

Dossier documentaire

Barème

Dossier A	**Conception et maintenance de services**	60 points
Dossier B	**Production de services et gestion du patrimoine**	40 points
	Total	100 points

Présentation du contexte

La société RIOCA implantée à Ainsa (province de Huesca, Espagne) est spécialisée dans la fabrication de cycles tout terrain (VTT).

Proche des Pyrénées, la société RIOCA a d'abord révolutionné le monde du ski en développant des bâtons de ski en aluminium. Puis dans les années 1980, RIOCA a introduit son premier VTT sur le marché du cycle. Depuis, l'entreprise accumule les prouesses techniques en présentant en 1998 le VTT tout suspendu le plus léger au monde, puis en 2001 le vélo de route Team RIOCA, dont le cadre pèse moins de 1 kilo, enfin, en 2008 le vélo de triathlète Plasma RIOCA dont le cadre ne pèse que 980 grammes.

Aujourd'hui, l'entreprise se lance sur le marché des cycles électriques en collaboration avec la marque Bosch.

Ce développement historique de l'entreprise, s'est accompagné de différentes restructurations. Aujourd'hui, l'entreprise compte une centaine de salariés répartis dans cinq unités :

- un atelier de fabrication ;
- un service recherche et développement ;
- un garage de tests et validation de la production et des prototypes ;
- un service informatique ;
- un service de direction générale chargé de toute la gestion administrative et commerciale.

L'entrée de RIOCA sur le marché du cycle électrique s'accompagne d'un programme de restructuration et d'amélioration de ses prestations. La société RIOCA souhaite réaliser un certain nombre d'audits dont un audit de son système d'information. Son service informatique étant limité à 2 techniciens et à un administrateur système nouvellement embauché, elle fait appel à une entreprise extérieure.

L'entreprise de services du numérique (ESN) JMC est mandatée pour auditer le réseau informatique de la société et répondre à certaines préoccupations afin d'optimiser le système informatique. Vous intégrez cette société et le groupe de travail de 4 personnes chargé de réaliser les missions suivantes :

- Analyser les performances et maintenir l'architecture existante
- Préparer une solution d'infrastructure

L'architecture réseau et les équipements informatiques sont détaillés dans le dossier documentaire.

Dossier A Conception et maintenance de services

Documents nécessaires à la réalisation du dossier A : 1 à 8.

Mission 1 : Analyse et maintenance de l'infrastructure

Le nombre sans cesse croissant d'ordinateurs au sein de l'entreprise RIOCA, entraîne une quantité toujours plus importante d'informations à gérer pour les techniciens et l'administrateur système. Le groupe de travail de l'entreprise JMC a recensé plusieurs problèmes et a commencé à élaborer un rapport d'audit basé sur des feuilles de révélation et d'analyse des problèmes (FRAP).

Vous êtes en charge de la description du premier problème constaté concernant « l'organisation et la gestion de l'infrastructure informatique » et vous devez compléter la FRAP N°1.

A.1.1	Détailler, pour **chaque constat de la FRAP N°1**, les conséquences que cela peut avoir sur le fonctionnement du réseau.
A.1.2	Recommander les solutions techniques susceptibles de résoudre durablement l'ensemble des problèmes.

Mission 2 : Définition des éléments nécessaires à la continuité de service de l'infrastructure

Suite à cet audit, lors du deuxième semestre 2015, les solutions préconisées ont commencé à être implémentées.

Pour un meilleur suivi, il a été décidé d'intégrer également une gestion des SLA (*Service Level Agreement*, accord de niveau de service).

A.2.1	Donner le principe d'une gestion des SLA (*Service Level Agreement*) et les avantages apportés.
A.2.2	Identifier les points faibles de l'infrastructure réseau actuelle de cette organisation en termes de disponibilité des systèmes et des applications.

La rédaction de la FRAP N°4 portant sur les problèmes relatifs à la continuité d'exploitation a conduit à une proposition permettant de mettre en place un PCA (plan de continuité d'activité) qui doit être justifiée avant d'être présentée à la société RIOCA. Il vous est demandé, d'une part de trouver les arguments appuyant cette proposition et, d'autre part, d'élaborer les procédures de mise en œuvre.

A.2.3	Démontrer qu'en cas d'arrêt planifié d'un serveur ESXi, les modules de la solution de base permettent d'assurer la continuité de service.
A.2.4	Préciser en quoi la solution de base améliore également le plan de reprise d'activité (PRA) de l'entreprise RIOCA en cas de panne brutale d'un des serveurs ESXi.
A.2.5	Expliquer comment les modules optionnels pourraient améliorer le taux de disponibilité du serveur d'authentification une fois virtualisé.
A.2.6	Montrer que la virtualisation et la haute disponibilité peuvent avoir un impact positif sur le TCO (*Total Cost of Ownership* ou coût total de possession).

Mission 3 : Définition des éléments nécessaires à la sécurité de l'infrastructure

Suite aux recherches pour comprendre la cause de la panne du serveur LDAP, vous avez constaté un défaut sur le système de climatisation. Ce défaut a généré le déclenchement du système anti-incendie dans la salle des serveurs. Deux disques de la baie de disques ont été endommagés et sont hors service ainsi que l'alimentation électrique du serveur ayant généré la panne.

A.3.1	Citer deux éléments matériels indispensables permettant de sécuriser un serveur physique.
A.3.2	Indiquer trois autres dispositifs permettant de mieux sécuriser cette salle serveur.

Lors des compétitions internationales de VTT, la société RIOCA héberge le portail web de gestion des événements se déroulant à Ainsa en Espagne.

Afin d'améliorer la sécurité du service web, votre responsable préconise la mise en place d'un pare-feu applicatif (*WAF, Web Application Firewall*) nommé *mod_security* installé sur le serveur web pour sécuriser les applications web.

A.3.3	Donner deux arguments permettant de justifier la mise en place de ce pare-feu applicatif en complément du pare-feu actuel de l'entreprise.

Mission 4 : Amélioration du trafic réseau

La mise en place de l'outil de gestion intégré est récente ; il est nécessaire de surveiller le trafic généré par ce dernier.

Vous constatez des lenteurs sur le réseau. Votre analyse du trafic réseau montre un fort taux de trames SNMP (*Simple Network Message Protocol*) émises par le serveur de gestion des SLA. Suite à ce constat, le responsable informatique souhaite obtenir des informations sur la mise en place de notifications (*traps*) SNMP.

A.4.1	Expliquer en quoi la mise en place de *traps* SNMP pourrait résoudre ce problème de lenteur sur le réseau.

Mission 5 : Planification des sauvegardes

L'entreprise souhaite garder une trace des connexions internet de ses utilisateurs pendant au moins une année.

Le schéma fonctionnel et les caractéristiques du serveur de sauvegarde (*NAS – Network Attached Storage*) sont présentés dans le dossier documentaire.

Aucun dysfonctionnement n'a pour l'instant été constaté sur le proxy web, mais votre responsable préfère s'assurer qu'il n'y en aura aucun à l'avenir et vous demande de réaliser une étude.

A.5.1	Proposer une solution permettant la réplication quotidienne, sur le serveur NAS, des fichiers contenant les connexions internet.
A.5.2	Donner les caractéristiques techniques du serveur NAS permettant de répondre aux deux critères suivants : confidentialité des données et disponibilité des données.

Dossier B Production de services et gestion du patrimoine

Documents nécessaires à la réalisation du dossier B : 1, 9, 10, 11, 12, et 13.

Mission 1 : Préparation d'une solution d'infrastructure

Dans le cadre du dialogue social au sein de RIOCA, les salariés ont demandé à pouvoir utiliser dans l'entreprise leurs appareils personnels pour accéder à internet via le réseau de l'entreprise pendant leur pause. Vous êtes sollicité.e lors d'une réunion regroupant l'ensemble des personnels pour répondre à cette nouvelle problématique. Celle-ci nécessiterait de mettre en place une zone Wi-Fi au sein d'une unité pilote qui serait l'atelier. Un entretien entre le directeur des systèmes d'information (DSI) et la société prestataire JMC a permis d'identifier les conditions de mise en œuvre du réseau sans fil.

B.1.1	Justifier que la borne d'accès sans fil choisie respecte les conditions de mise en œuvre définies avec le DSI.

Pour la mise en place de cette nouvelle zone, votre responsable propose différents choix de configuration permettant de sécuriser ce nouvel accès sans fil.

a. Modifier le nom par défaut du réseau (*SSID Service Set IDentifier*)

b. Cacher le nom du réseau (*SSID Service Set IDentifier*)

c. Configurer les adresses IP statiques des clients avec une plage d'adresses limitée

d. Choisir un mot de passe fort d'accès à l'administration du point d'accès

e. Filtrer les équipements clients par adressage MAC

f. Choisir une méthode d'authentification (portail captif/serveur RADIUS).

B.1.2	Proposer des éléments de réponse permettant de valider ou d'invalider la mise en place de chacun de ces choix de configuration dans le cadre du déploiement de cette nouvelle zone.
B.1.3	Proposer la nouvelle configuration du commutateur de l'atelier afin d'intégrer cette nouvelle zone dans le VLAN Wi-Fi.

Mission 2 : Recyclage de solutions techniques d'accès

L'activité de l'entreprise connait des variations saisonnières. Pour absorber un pic de production, il est nécessaire d'ajouter 10 postes informatiques au sein de l'unité Garage. Pour répondre à ce besoin, dans le cadre d'une politique budgétaire stricte, le recyclage des postes est préconisé. Les 10 postes recyclés proviendront de l'unité de recherche et développement. Les deux postes restants dans cette unité seront conservés dans un local, prêts à remplacer un poste défaillant.

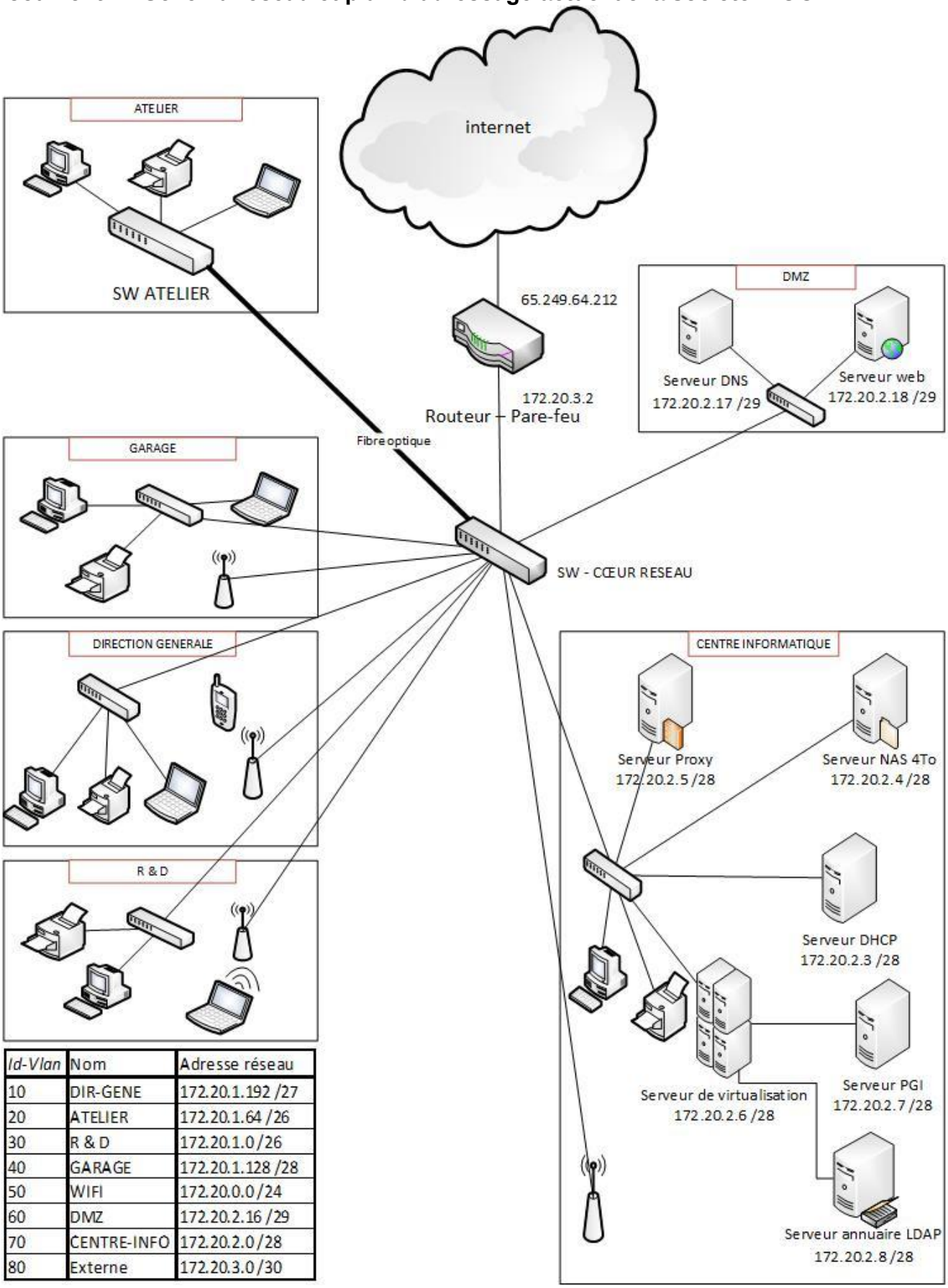
Un serveur LTSP (*Linux Terminal Server Project*) est recommandé ; il est présenté dans le dossier documentaire. Il sera hébergé au sein du *cluster* ESX.

B.2.1	Donner trois avantages apportés par ce type d'architecture.
B.2.2	Montrer en utilisant le critère du TCO que le recyclage est plus intéressant que l'achat de nouveaux postes.
B.2.3	Indiquer s'il est possible d'ajouter les 10 clients légers sans modification du réseau tant du point de vue physique que logique. *Justifier la réponse*.

Le parc des 10 postes supplémentaires est maintenant physiquement installé et le serveur a été mis en place au sein du centre informatique. Des tests sont effectués à partir d'un client léger. Vous disposez du fichier de configuration du serveur DHCP et des résultats des tests dans le dossier documentaire.

B.2.4	Identifier la raison pour laquelle le client léger ne récupère pas de session.
B.2.5	Proposer une solution afin de résoudre ce problème.

Document 1 : Schéma réseau et plan d'adressage actuel de la société RIOCA



Id-Vlan	Nom	Adresse réseau
10	DIR-GENE	172.20.1.192 /27
20	ATELIER	172.20.1.64 /26
30	R & D	172.20.1.0 /26
40	GARAGE	172.20.1.128 /28
50	WIFI	172.20.0.0 /24
60	DMZ	172.20.2.16 /29
70	CENTRE-INFO	172.20.2.0 /28
80	Externe	172.20.3.0 /30

Ce réseau est structuré de la manière suivante :

- l'atelier comporte 15 ordinateurs et 1 imprimante ;
- le service Recherche et Développement compte 12 ordinateurs et 2 imprimantes ;
- le garage comporte 10 ordinateurs et 1 imprimante ;
- le centre informatique compte un ensemble de serveurs (listés ci-dessous), 3 ordinateurs et 1 imprimante ;
- la direction générale comporte 6 ordinateurs et 6 imprimantes.

Actuellement le réseau informatique de la société est composé de 7 commutateurs Gigabit (dont 1 commutateur-routeur cœur de réseau, un commutateur administrable et 5 non administrables), 4 points d'accès Wi-Fi et un routeur pare-feu.

Chacun des 6 commutateurs présents dans chaque zone disposent d'au minimum 24 ports.
Le commutateur de l'atelier possède 4 ports POE supplémentaires Gi0/25 à Gi0/28.

RIOCA est connecté par ADSL au FAI fournissant une bande passante de 2 Mbits/s en débit montant et 12 Mbits/s en débit descendant.

Le centre informatique de RIOCA comporte 6 serveurs :

- serveur1 : service DHCP ;
- serveur2 : proxy web ;
- serveur3 : DNS ;
- serveur4 : service *web* ;
- serveur5 : sauvegarde (NAS) ;
- serveur6 : serveur physique sur lequel est installé un hyperviseur Vmware ESXI hébergeant deux serveurs virtuels, le premier contient un PGI (progiciel de gestion intégré), le deuxième contient un serveur annuaire LDAP (gestion des utilisateurs et ordinateurs).

Le service DHCP distribue des adresses aux VLAN suivants : DIR-GENE, ATELIER, R&D, WIFI. Toutes les imprimantes sur ces VLAN font l'objet de réservations d'adresse. L'agent relais DHCP est activé sur le cœur de réseau.

Toutes les connexions internet passent par le *proxy web*. Quotidiennement, le serveur crée localement un fichier journal qui contient toutes les connexions internet du jour.

RIOCA utilise les supports de transmission suivants :

- la fibre optique : la fibre optique est utilisée au sein du réseau intranet pour interconnecter les différents bâtiments, de la salle serveur située au centre informatique jusqu'au bâtiment atelier (distance supérieure à 300 mètres) ;
- les câbles torsadés : le câblage torsadé blindé et non blindé est utilisé à l'intérieur des bâtiments (blindé dans les faux plafonds et non blindé catégorie 6 pour connecter les ordinateurs et autres équipements réseaux) ;
- les supports sans fil : un VLAN dédié est utilisé pour les accès sans fil.

Document 2 : Rapport d'audit et feuilles de révélation et d'analyse des problèmes

Le rapport d'audit intègrera neuf feuilles de révélation et d'analyse des problèmes (FRAP).
Une FRAP est un document synthétique permettant d'analyser et de documenter un dysfonctionnement, il comprend ici 5 composants :

- l'énoncé du problème ;
- les constats ;
- les causes qui expliquent le problème ;
- les conséquences qui en découlent ;
- les recommandations pour solutionner le problème.

La FRAP est renseignée par l'auditeur à chaque fois qu'il observe un dysfonctionnement, une insuffisance, etc. Elle a pour objectif de conduire son raisonnement et de l'amener à formuler une recommandation.

La première feuille de révélation et d'analyse des problèmes (FRAP) a commencé à être rédigée ainsi :

FRAP N° 1 – Organisation et gestion de l'infrastructure informatique.

➔ Domaine d'application : entreprise – ensemble de l'architecture réseau.

➔ Problème : manque d'organisation et insuffisances dans la gestion de l'infrastructure réseau.

➔ Constats :
- Pas d'alerte en cas de problème (réel ou potentiel) sur un élément d'infrastructure.
- Pas de documentation écrite lors de la résolution d'un incident.
- En cas de problème aucune identification de la panne n'est possible avant l'arrivée des techniciens.
- L'administrateur système procède à un examen journalier des journaux systèmes.

➔ Causes : jusqu'à très récemment, le service informatique n'était constitué que de 2 techniciens qui avaient en charge les incidents quotidiens de niveau 1 et 2. L'infrastructure réseau s'est développée au coup par coup, sans visibilité à long terme.

Le rapport complet sera remis à la société RIOCA à l'issue de la mission d'audit de son système informatique et plus particulièrement de son réseau informatique et de la sécurité associée.

Document 3 : Interface de gestion des SLA (*Service Level Agreement*)

Seules les solutions préconisées suite aux problèmes constatés dans la FRAP N°1 ont pour l'instant été implémentées.

Les principaux indicateurs concernant les niveaux de service définis, entre les utilisateurs de RIOCA et le service informatique de RIOCA, à la suite de l'audit sont donnés via le nouvel outil de gestion intégré au système.

Tous les serveurs, et tous les matériels d'interconnexion qui le permettent, sont surveillés grâce à ce nouvel outil. Cette surveillance s'effectue de manière active en utilisant le protocole SNMP. C'est donc celui-ci qui interroge à intervalle régulier les différents serveurs et matériels pour connaitre leur état. Vous pouvez observer un extrait de ses restitutions :

Niveaux de Service (SLA)	Période	Niveau actuel	Niveau requis
SLA1 : Serveurs *web*	Décembre 2015	89,00 %	99,90 %
SLA2 : Réponse utilisateur final	Décembre 2015	87,87 %	85,00 %
SLA3 : Serveur d'authentification	Décembre 2015	71,40 %	99,90 %

Le niveau actuel du SLA3 est dû à une panne du serveur d'annuaire LDAP qui a empêché l'entreprise de fonctionner normalement durant deux journées.

Document 4 : Proposition d'infrastructure de virtualisation

La FRAP N°4 portant sur les problèmes relatifs à la continuité d'exploitation a conduit à une proposition basée sur une plate-forme de virtualisation qui fonctionnerait sur plusieurs serveurs physiques (ESXi) accueillant différentes machines virtuelles. Le serveur actuellement utilisé serait conservé, la solution existante serait enrichie d'un nouveau serveur ESXi.

À cette description générale de la solution proposée, s'ajoutent les propositions complémentaires présentées ci-dessous.

Solution de base

Les composants de la solution de base

VMware vCenter Server est le point central pour configurer, approvisionner et gérer des environnements informatiques virtualisés. Il va permettre d'administrer plusieurs serveurs ESXi (*cluster*) permettant ainsi de nombreuses solutions en matière de disponibilité.

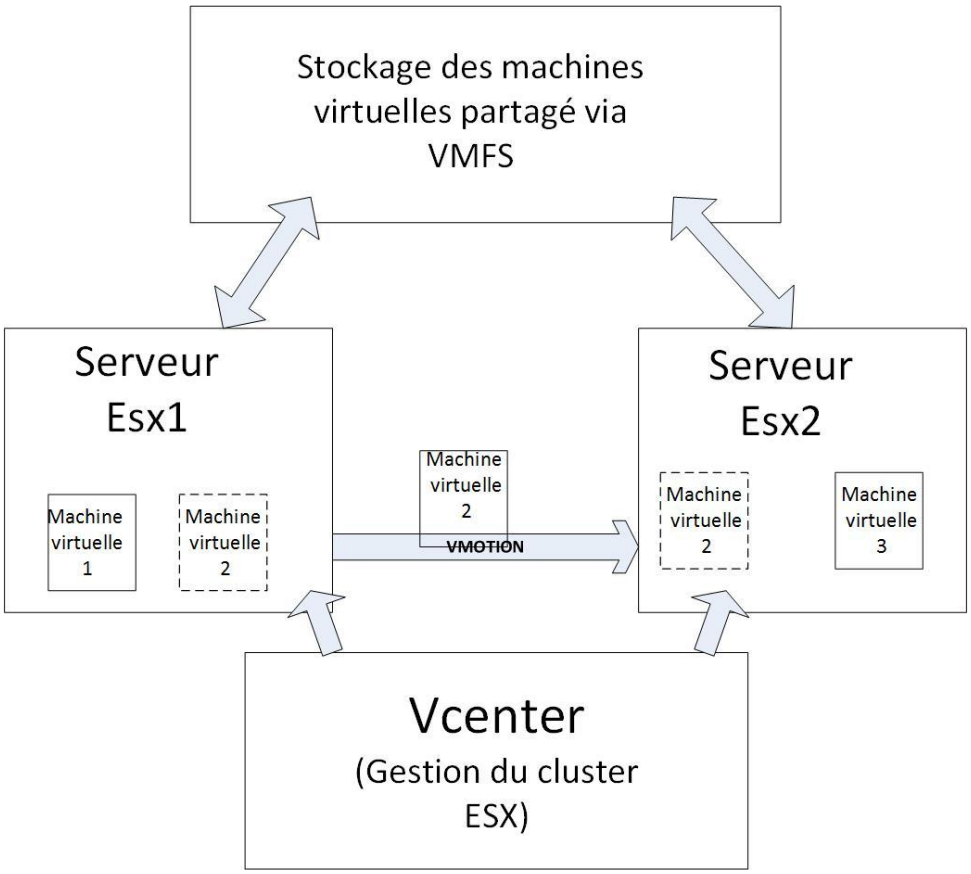
VMware vSphere Client est une interface permettant aux administrateurs de se connecter à distance au vCenter Server ou ESXi depuis n'importe quel PC.

VMware vSphere Web Access est une interface *web* permettant de gérer une machine virtuelle et d'accéder à des consoles distantes.

VMware vSphere VMFS est un système de fichiers en *cluster* hautement performant optimisé pour les machines virtuelles. Alors que les systèmes de fichiers classiques ne permettent qu'à un seul serveur d'accéder en écriture-lecture à un même système de fichiers à un moment donné, VMFS utilise le

stockage partagé afin d'autoriser simultanément plusieurs hôtes VMware vSphere à écrire et lire des données sur le même stockage.

VMware vMotion permet de migrer manuellement en direct des machines virtuelles en service depuis un serveur physique que l'on doit maintenir par exemple, vers un autre serveur sans période d'interruption avec une disponibilité de service permanente et une intégrité de transaction complète.



Composants optionnels permettant d'améliorer encore le service rendu

Source : extrait de la documentation VMware

VMware Haute disponibilité (HA)

Fonction qui offre une haute disponibilité aux machines virtuelles. En cas de panne du serveur, les machines virtuelles affectées sont redémarrées automatiquement sur d'autres serveurs de production disposant de surcroît de capacité.

VMware Distributed Resource Scheduler (DRS)

Fonction qui affecte et équilibre la capacité informatique dynamiquement dans les collections de ressources matérielles pour les machines virtuelles (équilibrage de charge entre différents serveurs ESXi). Cette fonction comporte des possibilités de gestion d'alimentation distribuée (DPM) permettant au centre de données de réduire significativement sa consommation d'énergie.

Tolérance aux pannes VMware Fault Tolerance (FT)

Quand la tolérance aux pannes est activée pour une machine virtuelle, une seconde copie de la machine originale (ou primaire) est créée. Toutes les actions réalisées sur la machine virtuelle primaire sont également effectuées sur la seconde machine virtuelle. Si la machine virtuelle primaire devient indisponible, la seconde machine devient active pour une disponibilité continue.

Document 5 : Module de sécurité mod_security

Les applications et les portails *web* sont les éléments les plus vulnérables et les plus vecteurs d'intrusion de nos jours. Il s'agit là de la porte d'entrée la plus commune pour les pirates informatiques.

Le module de sécurité tiers (mod_security) permet un filtrage applicatif *web*, c'est un outil très performant écrit à la base en tant que module Apache et ensuite exporté sur d'autres plates-formes comme Nginx ou Microsoft IIS (Internet Information Service).

La fonction principale de mod_security est le filtrage des requêtes et des réponses générées entre les clients (visiteurs) et une application ou un site *web*. Appelé pare-feu applicatif ou pare-feu *web* (*Web Application Firewall* – WAF) il agit au niveau des applications. La plupart des pare-feux agissent au niveau des ports (port 22 SSH, port 80 Web…). Les WAF comme mod_security vont beaucoup plus loin dans la lecture du contenu des paquets afin d'y voir et d'y filtrer plus d'informations.

Mod_security peut avoir une mission de journalisation, c'est à dire de tracer (*logger)* certaines réponses ou certaines requêtes ou alors de blocage sous certaines conditions que l'on appelle règle. Mod_security propose également des fonctionnalités avancées ou annexes comme la possibilité d'échange avec des pare-feux de plus bas niveau par l'exécution de scripts. Par exemple, à la détection consécutive de plusieurs transgressions à des règles venant d'une même adresse IP, mod_security peut exécuter un script qui va demander au pare-feu de bas niveau de bloquer cette adresse IP.

D'après: http://www.it-connect.fr

Document 6 : Les traps SNMP (Simple Network Management Protocol)

Le protocole SNMP prévoit la possibilité pour l'agent client installé sur l'équipement, lorsqu'il rencontre un événement prédéfini, d'envoyer une notification (appelée *trap*) au serveur de supervision pour l'en avertir. Exemples d'évènements prédéfinis : un disque qui a moins de 10 % d'espace libre, le trafic de diffusion qui dépasse 40 % sur un port de commutateur.

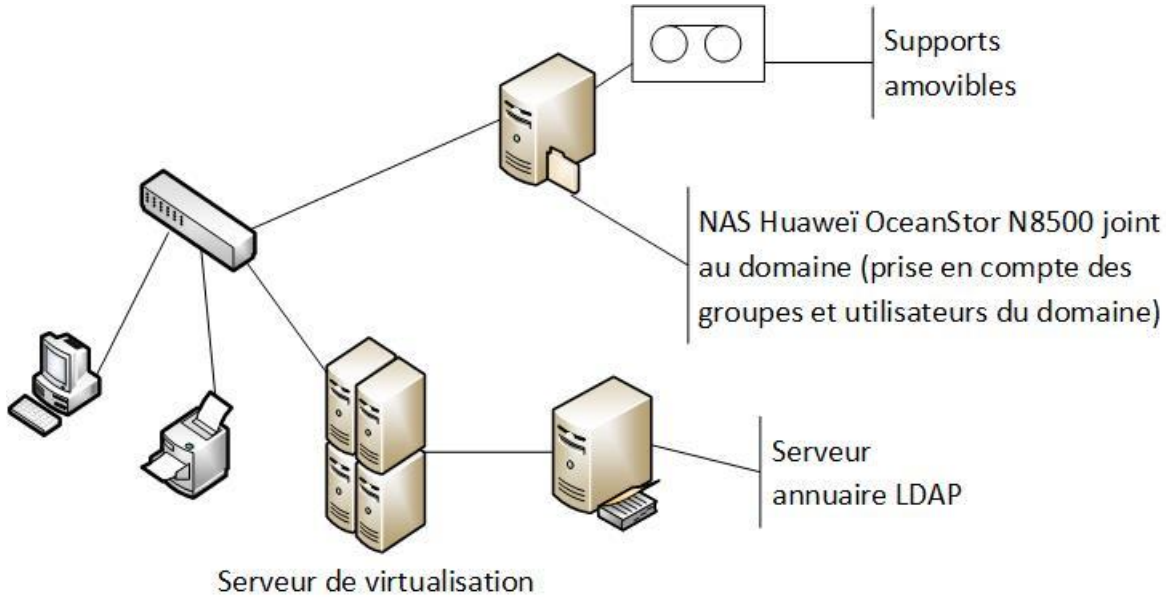
Le signal envoyé au serveur de supervision contient plusieurs attributs dont :

- L'adresse de l'équipement qui a envoyé l'information.
- L'OID racine (Object Identifier) correspond à l'identifiant du message reçu.
- Le message envoyé au travers du *trap* SNMP qui correspond à un ensemble de paramètres.

Afin de pouvoir interpréter l'évènement reçu, le serveur de supervision doit posséder dans sa configuration les éléments nécessaires pour traduire l'évènement. Pour cela, il doit disposer d'une base de données contenant les OID ainsi que leurs descriptions, appelée MIB (*Management Information Base*). Il existe deux types de MIB :

- Les MIB standards qui utilisent des OID standardisés et qui sont implémentés par de nombreux constructeurs sur leurs équipements.
- Les MIB constructeurs qui sont propres à chacun et souvent à chaque modèle d'équipement.

Document 7 : Schéma fonctionnel du serveur NAS Huaweï OceanStor N8500



Document 8 : Spécifications du NAS Huaweï OceanStor N8500 (Extrait)

Modèle	N8500
Architecture	Architecture de cluster actif-actif multi-nœud
Nombre de nœuds	2
Cache/nœud	48 Go
Ports GE/nœud	4 ports Gigabit Ethernet
Types de disque	SSD, SAS et NL-SAS
Capacité de stockage physique	Dynamiquement extensible jusqu'à 15 Po
Niveaux de RAID	0, 1, 3, 5, 6, 10, et 50
Protocoles de stockage en réseau	FC, FCoE, iSCSI, NFS, CIFS, FTP et HTTP
Logiciels à valeur ajoutée pour les fichiers	Niveaux de stockage dynamique (DST) Équilibrage de charge Instantané Mise en miroir Quota Réplication
Logiciels à valeur ajoutée pour les blocs	HyperSnap (instantané) HyperCopy (copie de volume) HyperClone (clone) HyperReplication (réplication à distance prenant en charge la perte de données maximale admissible - Recovery Point Objective) SmartQoS (contrôle de la qualité de service) SmartPartition (partitionnement intelligent)

Document 9 : Discussion issue de la réunion du 3 juin 2015 – Ainsa – Société RIOCA

Voici l'entretien entre le directeur des systèmes d'information (DSI) et le représentant de la société JMC :

DSI : Pensez-vous qu'il soit envisageable d'utiliser les smartphones personnels des employés ?

JMC : Dans quel but ?

DSI : À leur demande, c'est une mesure négociée dans le cadre du dialogue social.

JMC : Bien sûr, ce concept est nommé BYOD, Bring Your Own Device, qui signifie apportez vos appareils personnels, mais cela nécessitera d'intégrer les smartphones des employés dans l'architecture réseau de votre société.

DSI : Quelle technologie préconisez-vous ?

JMC : Il sera nécessaire d'ajouter des équipements permettant la mise en place d'une zone Wi-Fi couvrant la totalité de l'entreprise. Mais je vous propose de commencer par une zone pilote au sein de l'atelier.

DSI : Un nouvel accès sans fil, d'accord mais le principal problème des réseaux Wi-Fi est leur fragilité vis-à-vis des attaques externes, le cryptage et l'authentification devront être simples pour les personnes connectées et très difficiles à pirater, de plus la mise en place des bornes doit être rapide et nécessiter le minimum de travaux, les bornes devront être protégées contre le vol et les incidents divers, et physiquement inaccessibles.

JMC : Il faut évaluer le nombre de bornes nécessaires à la couverture spatiale de l'atelier. Quelle est la surface de l'atelier ?

DSI : L'atelier a une largeur de 20 m environ et une longueur de 80 m environ, soit une surface approximative de 1 600 m^2.

JMC : Deux bornes devraient donc suffire, compte-tenu de ces informations. Toutes ces contraintes doivent pouvoir être respectées, nous permettrons aux personnels d'utiliser tous types de solutions techniques d'accès dans l'atelier en toute sécurité pour l'entreprise. Pour l'alimentation électrique des bornes, le câblage électrique est-il facile d'accès ?

DSI : Non, l'installation électrique est complexe dans l'atelier, le déploiement de nouveaux câbles risque d'être compliqué. Une dernière remarque, n'oubliez pas le débit, nous avons fait en sorte de concevoir un réseau en Gigabit.

JMC : Ne vous inquiétez pas nous ferons le nécessaire dans la limite des spécificités techniques des liaisons sans fil.

DSI : Très bien, merci.

Document 10 : Fiche technique borne d'accès Wi-Fi Cisco WAP371

INFORMATIONS GENERALES	
Désignation	Cisco Small Business WAP371
Marque	Cisco Small Business
Modèle	WAP371-E-K9
SPECIFICATIONS TECHNIQUES	
Normes réseau	Wi-Fi AC, Wi-Fi AC 1300 Mbps (IEEE 802.11ac) Wi-Fi AC 1733 Mbps (IEEE 802.11ac) Wi-Fi N 450 Mbps (IEEE 802.11n) Wi-Fi G 54 Mbps (IEEE 802.11g) Wi-Fi B 11 Mbps (IEEE 802.11b)
Dual-Band	Oui
Connecteur(s)	Ethernet – RJ45 Femelle
Cryptage	WPA, WPA2
Antenne(s) Amovible(s)	Non
Puissance antenne(s)	2dBi
Hauteur	43mm
Largeur	230mm
Profondeur	230mm
Poids	740g
Couleur	Blanc
Compatible IPv6	Oui
Interface	Gigabit Ethernet (10/100/1000Mbps)
Alimentation	PoE
Protocole(s)	QoS, segmentation VLAN, Load Balancing, RADIUS
Prix	275 €

NB : La borne présentée a une portée minimale de 100 m (test effectué dans l'environnement de l'unité atelier).

Document 11 : Configuration VLAN commutateur administrable Atelier (Cisco 2950)

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi0/17, Gi0/18, Gi0/19, Gi0/20
                                                Gi0/21, Gi0/22, Gi0/23, Gi0/24
                                                Gi0/26, Gi0/27, Gi0/28

20   VLAN_ATELIER                     active    Gi0/1, Gi0/2, Gi0/3, Gi0/4
                                                Gi0/5, Gi0/6, Gi0/7, Gi0/8
                                                Gi0/9, Gi0/10, Gi0/11, Gi0/12
                                                Gi0/13, Gi0/14, Gi0/15, Gi0/16
                                                Gi0/25
```

Nota : Le port Gi0/25 est le port de cascade connecté au cœur de réseau.

Document 12 : Extrait du fichier de configuration du serveur DHCP / Tests

```
subnet 172.20.1.128 netmask 255.255.255.240 {
    range 172.20.1.130 172.20.1.141;                    #étendue
    option broadcast-address 172.20.1.143;
    option routers 172.20.1.142;                        #passerelle

group {                                                 #description clients légers
       option root-path "/opt/ltsp/lightclient";        #chemin de l'environnement
       next-server 172.20.2.12;                         #IP du serveur LTSP
       filename "/ltsp/lightclient/pxelinux.0";         #chemin du chargeur d'amorçage

                                                        #définition clients légers
                                                        #client léger N°1
              host leger1 {                             #nom d'hôte ou dns du client
               hardware ethernet 00:0c:b9:15:12:00;     #adresse MAC du client 1
                fixed-address 172.20.1.130;             #adresse IP du client
              }

                                                        #client léger N°2
              host leger2 {
              …
              }
      }
```

Résultat de la commande ***ifconfig eth0*** lancée depuis le serveur LTSP (extrait)

```
eth0    Link encap:Ethernet  HWaddr 14:d6:4d:09:1d:c3
        inet addr:172.20.2.13  Bcast:172.20.2.15  Mask:255.255.255.240
```

Test de communication : Ping vers le serveur LTSP depuis un poste atelier

```
Réponse de 172.20.2.13 octets=32 temps<1ms TTL=128
Réponse de 172.20.2.13 octets=32 temps<1ms TTL=128
Réponse de 172.20.2.13 octets=32 temps<1ms TTL=128
```

Message d'erreur client léger :

```
MAC :00:0c:b9:15:12:00 UUID :56424f59-0000-0000-0000-08002787837b
Searching for server (DHCP). . . . .
Me: 172.20.1.130, DHCP: 172.20.2.3, Gateway: 172.20.1.142
Loading 172.20.2.12:/ltsp/lightclient/pxelinux.0 . . . . . .
No server found
```

Document 13 : Présentation LTSP (Linux Terminal Server Project)

Le projet *Linux Terminal Server* (LTSP) est un paquet additionnel pour GNU/Linux qui permet de connecter de nombreuses stations clientes légères sur un serveur GNU/Linux. Les applications s'exécutent sur le serveur, les stations clientes envoient les signaux d'entrée de périphérique vers le serveur et affichent en retour le résultat donné par les applications.

Le concept de base veut que toute machine ayant une carte réseau puisse être utilisée comme client léger.

LTSP est une solution flexible et rentable qui permet l'informatisation des écoles, des entreprises et des organisations du monde entier en déployant des clients légers.

Nouveaux clients légers et PC existants peuvent être utilisés pour naviguer sur le *web*, envoyer des courriels, créer des documents, et exécuter d'autres applications bureautiques.

LTSP est une collection de logiciels qui transforme une installation de GNU / Linux en serveur de clients légers. Cela permet à faible coût d'utiliser des clients légers comme terminaux sur le serveur de client léger.

LTSP ne nécessite pas de logiciel côté client. Cette architecture exige seulement une interface réseau PXE que beaucoup de clients légers et ordinateurs possèdent déjà. Cela signifie qu'aucun support de stockage physique (disque dur, compact-flash, etc.) n'est nécessaire sur le client léger afin de démarrer LTSP. Cela réduit considérablement la maintenance du réseau.

De là, toutes les opérations telles que l'authentification (nom d'utilisateur et mot de passe), le lancement d'applications, et affichage des sites *web* sont traités sur le serveur LTSP. Le serveur LTSP transfère toutes les informations graphiques au client sur le réseau. Cela permet à des configurations minimales d'utiliser la puissance du serveur pour toutes les opérations.

D'après la documentation LTSP
http://www.ltsp.org/