

E5SR : PRODUCTION ET FOURNITURE DE SERVICES

Durée : 4 heures

Coefficient : 5

CAS HTS

Ce sujet comporte 17 pages dont 10 pages de documentation.
Il est constitué de deux parties qui peuvent être traitées de façon indépendante.
Le candidat est invité à vérifier qu'il est en possession d'un sujet complet.

Aucun matériel ni document autorisé

Liste de la documentation jointe

Dossier documentaire : cahier des charges de la société Bloom
Fiche d'incident

p 8
p 17

Barème

Partie A	Conseil avant-vente au client <i>Bloom</i>	50 points
Partie B	Mise en place et maintenance du nouveau réseau <i>Bloom</i>	50 points
	Total	100 points

CODE ÉPREUVE : SIE5SR		EXAMEN : BREVET DE TECHNICIEN SUPÉRIEUR	SPÉCIALITÉ : SERVICES INFORMATIQUES AUX ORGANISATIONS Parcours SISR
Session 2013	SUJET	ÉPREUVE : E5-PRODUCTION ET FOURNITURES DE SERVICES INFORMATIQUES	
Durée : 4 h	Coefficient : 5	Code sujet : 13SI06	Page : 1/17

Le prestataire de services : la société HTS

HTS est une société de services en informatique qui s'est diversifiée depuis une dizaine d'années en créant différentes filiales spécialisées :

- *Daixone*, opérateur télécom et fournisseur d'accès internet professionnels qui fait appel à quatre FAI professionnels : *Oleane*, *SFR*, *BT* et *Nordnet* ;
- *Hebertek*, société spécialisée d'abord dans l'hébergement de sites *web* puis, plus récemment, dans l'hébergement de systèmes informatiques ;
- *IT-Compétences*, société spécialisée dans la formation et dans la mise à disposition de personnes ressources.

Hebertek propose différentes formes d'hébergement sur mesure à ses clients :

- Du *hosting*, c'est-à-dire de l'hébergement d'équipements appartenant aux clients auxquels la société loue des « U » sécurisées (c'est-à-dire des emplacements dans des armoires à serveurs). Ces équipements peuvent être des serveurs, des pare-feux, des robots de sauvegarde, etc. *Hebertek* propose des services complémentaires comme l'exposition de serveurs à l'Internet, l'accès en administration à distance aux équipements, les sauvegardes, etc.
- Au-delà du simple hébergement de serveurs, *Hebertek* propose des contrats d'infogérance. Dans ce type de contrat, un périmètre d'infogérance est défini en fonction duquel les techniciens d'*Hebertek* administrent et supervisent tout ou partie des matériels, des systèmes d'exploitation ou encore des applicatifs "métiers" des clients.
- Enfin, *Hebertek* propose les mêmes niveaux de prestations, mais sur ses propres équipements qui sont alors loués aux clients. On parle alors de *location de puissance machine*. Depuis 2010, la grande majorité des locations de puissance machine portent sur des systèmes virtualisés. Les services proposés aux clients hébergés sont décrits dans la brochure commerciale de la société.

Hebertek dispose, sur ses deux sites technologiques de la ville de Tarckange, de deux fermes de serveurs proposant différents « *box de puissance* », c'est-à-dire des salles spécialisées, climatisées et respectant des normes strictes en terme d'accès sécurisé et de protection anti-incendie.

Chaque « *box de puissance* » est doté de plusieurs armoires à serveurs contenant chacune des grappes de CPU ou d'unités de stockage. Les systèmes informatiques y sont tous virtualisés.

Le client : la société *Bloom*

Depuis une dizaine d'année, *HTS* est le fournisseur de la cristallerie de luxe française *Bloom*, pour les matériels (serveurs, systèmes d'impression ou postes client) et pour l'accès Internet, SDSL, via sa filiale *Daixone*.

La société *Bloom* est implantée sur plusieurs sites. Le siège de *Bloom* est situé à Pannes-en-Argonne. On y trouve l'usine principale du groupe, où sont produits la plupart des objets en catalogue, et une boutique. Le site abrite également le « centre des maîtres verriers » qui est

tout à la fois un lieu de démonstration du savoir-faire des ouvriers, un laboratoire de recherche et une « pépinière » de jeunes créateurs, dont la production est vendue au sein de la boutique locale.

L'usine historique de Sciaux produit essentiellement des pâtes de verre et les plus beaux objets du catalogue.

Le site de Paris abrite les bureaux du service *marketing* et du webmestre du site de la société. Le site *web* de la société, qui n'est pas un site marchand mais seulement un site « vitrine », est pour l'instant situé chez un prestataire.

Le groupe dispose d'un réseau de 12 boutiques (bientôt 30) réparties sur tout le territoire français et d'un réseau de boutiques situées dans de grandes villes d'une trentaine de pays. Seules les boutiques françaises sont reliées en réseau avec le siège.

À l'occasion du rachat d'une autre cristallerie de luxe et de son réseau de boutiques, le responsable informatique de *Bloom* s'est rapproché du service avant-vente de *HTS* pour envisager une réponse technique satisfaisante à trois projets d'évolution de son système d'informatique.

- Le premier problème auquel est confrontée la société *Bloom* tient à la fragilité des liaisons informatiques entre ses différents sites. Le siège de la société, situé en pleine campagne, à Pannes-en-Argonne, a récemment été coupé pendant 24 heures des autres sites et de l'Internet suite au sectionnement par un engin de travaux publics du fourreau qui abritait à la fois le câble de sa liaison SDSL principale et celui de sa liaison de secours.
- Le second projet est lié à l'extension du nombre de ses points de vente. Les boutiques *Bloom* ont été dernièrement équipées de postes de type client léger, associés à un serveur d'application *Terminal Server* dimensionné en conséquence. Les responsables de chez *Bloom* souhaitent étendre cette solution au réseau de boutiques rachetées. Se pose alors le problème du sous-dimensionnement du serveur d'applications. Les responsables de *Bloom* souhaitent qu'on leur propose une solution souple et évolutive pour intégrer de nouveaux terminaux « client léger ».
- Le troisième projet consiste à mettre en place un réseau de caméras IP de surveillance, de déposer les clichés pris par ces caméras sur un serveur FTP central et de permettre des alertes de diverses natures (SMS, *mail*) à destination du service de sécurité ou des autorités de police locales.

Vous faites partie de l'équipe technique d'*Hebertek* chargée de répondre à ces différents besoins et vous allez avoir l'occasion d'intervenir à différentes phases de ces projets.

Éléments du dossier documentaire nécessaires pour la partie A

Dossier documentaire : cahier des charges de la société <i>Bloom</i>	8
1.1 Catalogue des services proposés par <i>Hebertek</i>	8
1.2 L'infrastructure <i>Hebertek</i>	9
2.1 La gestion des commutateurs avec le protocole VTP (<i>VLAN Trunking Protocol</i>).....	11
2.2 L'outil de supervision	12
3.1 Plan du réseau <i>Bloom</i> avant la mise en place de l'hébergement chez <i>Hebertek</i>	12
3.2 Liste des serveurs et services associés de la société <i>Bloom</i>	13
4.1 Plan du réseau <i>Bloom</i> après la mise en place de l'hébergement	14

Avant de signer un contrat d'hébergement et de transférer leurs serveurs depuis le siège de Pannes-en-Argonne au sein de la ferme d'hébergement d'*Hebertek*, les responsables de la société *Bloom* souhaitent qu'une réunion soit organisée pour leur permettre d'approfondir ce que va leur apporter cette solution.

Mission 1 : préparation de la présentation d'une solution d'infrastructure

Le responsable du service « avant vente » vous a fixé pour première mission de préparer cette réunion. Elle sera centrée sur la proposition d'hébergement basée sur le nouveau schéma d'infrastructure qui a été communiqué dans le cahier des charges joint. Les responsables de *Bloom* ont transmis par avance une liste de questions.

Question A.1.1

Préparer des éléments de réponse convaincants aux questions techniques posées par les responsables de *Bloom* et en particulier par ceux qui travaillent au siège de Pannes-en-Argonne.

- a. « Si le coup de pelleteuse se reproduit, comme la dernière fois, au même endroit je ne vois pas ce qui va changer. »
- b. « Chaque fois qu'on recevra de nouvelles versions de l'ERP, va-t-il falloir se déplacer pour les installer ? »
- c. « Expliquez-moi comment vous garantissez que notre trafic réseau sera séparé de celui des autres clients ? »
- d. « Quel dispositif mettez-vous en place pour la sauvegarde de nos données métier ? »
- e. « Quel est l'intérêt du serveur *proxy* que vous voulez nous louer ? Pourquoi centraliser la sortie de nos postes sur Internet ? »
- f. « Pourquoi répartir nos serveurs de *mail* et *web* dans une DMZ publique, notre serveur ERP dans une autre DMZ privée, et nos autres serveurs dans notre VLAN dédié ? »

La société *Hebertek* propose à ses clients un ensemble de services d'hébergement facturables. De manière générale, elle entend convaincre les clients potentiels et en particulier la société *Bloom* d'opter pour une ou plusieurs de ces solutions en s'appuyant sur la mise en ligne d'une FAQ (foire aux questions).

Question A.1.2

Rédiger les réponses suivantes de la FAQ présentant les avantages, pour un client, de faire héberger ses serveurs au sein de la ferme *Hebertek* quelle que soit la solution d'hébergement retenue :

- a. Sur le plan de la disponibilité des communications vers les serveurs hébergés ;
- b. Sur le plan de la sécurité physique des serveurs ;
- c. Sur le plan financier ;
- d. Sur le plan de l'évolutivité de l'infrastructure du système informatique du client ;
- e. Sur le plan humain et des différentes responsabilités entre le client et *Hebertek*.

Lors de la présentation des solutions *Hebertek* aux responsables informatiques de la société *Bloom*, un responsable de *Bloom* a demandé des éclaircissements sur la création des VLAN prévus pour sa société (le VLAN n°195) au sein des très nombreux commutateurs de la ferme. L'ingénieur réseau d'*Hebertek* a expliqué que le paramétrage de tous les VLAN (il y en a près de 1 000) était simplifié par l'utilisation du protocole VTP.

Votre responsable a promis de transmettre au client une courte note d'information sur l'intérêt de ce protocole. À l'issue de la séance, il vous demande de rédiger le corps de cette note et de lui soumettre.

Question A.1.3

Justifier l'utilisation du protocole VTP dans le cadre de l'architecture proposée par *Hebertek*.

Mission 2 : évaluation d'un risque lié à la fourniture d'un service

Alors que la société *Bloom* hésite encore sur le niveau d'hébergement à contractualiser, son site vitrine vient de subir une attaque par déni de service : lorsque les clients tentaient de se connecter au site, celui-ci affichait le message suivant : « impossible de se connecter au serveur distant ».

Souhaitant profiter de cette opportunité, votre responsable vous demande de fournir des explications techniques qui aideront la société *Bloom* à prendre la décision d'opter pour une solution de supervision en vous appuyant sur l'attaque de leur site *web*.

Question A.2.1

Expliquer en quoi consiste une attaque par déni de services (DOS).

Question A.2.2

Citer les commandes de l'outil de supervision qui permettront d'alerter au plus tôt en cas de nouvelle attaque sur le site *web* et justifier leur usage dans le cas d'une attaque par déni de service (DOS).

La proposition d'hébergement situe les serveurs réels appartenant à la société *Bloom* dans le *box* n°4 (celui qui est dédié aux équipements propres des clients), les machines virtuelles en « location de puissance » dans le *box* n°3 et les machines en DMZ exposées à l'internet dans le *box* Telecom.

Éléments du dossier documentaire nécessaires pour la partie B

3.1 Plan du réseau Bloom avant la mise en place de l'hébergement chez <i>Hebertek</i>	12
3.2 Liste des serveurs et services associés de la société Bloom.....	13
3.3 Configuration du réseau de la société Bloom sur le site de Paris.....	13
4.1 Plan du réseau Bloom après la mise en place de l'hébergement	14
4.2 Notes sur le nouveau plan de réseau Bloom.....	14
4.3 Configuration du réseau de la société Bloom sur le site de Paris.....	15
5.1 Fonctionnement du protocole RIP.....	15
5.2 Répartition de charge réseau / équilibrage de sessions <i>Terminal Server</i>	15
Fiche d'incident	17

La société *Bloom* a décidé de faire héberger ses serveurs chez *Hebertek* et de louer de nouveaux serveurs conformément au nouveau schéma d'infrastructure. Elle veut connaître l'impact de la mise en place de cet hébergement centralisé sur le paramétrage des équipements existants sur ses sites.

Mission 1 : mise à jour des réseaux des sites de la société *Bloom*

La nouvelle configuration de réseau doit être implantée sur l'ensemble des sites de la société *Bloom*. Chaque site sera relié aux serveurs hébergés chez *Hebertek* par une liaison VPN sur un réseau internet privé opéré par *Daixone*. Dans le contrat qui lie la société *Bloom* à *Hebertek*, ce dernier prend en charge l'hébergement des serveurs et la gestion des télécommunications entre les sites et les serveurs. Les routeurs de terminaison et leur configuration sont donc intégralement gérés par *Hebertek*.

Il est également prévu d'intégrer dans la nouvelle infrastructure un réseau de caméras IP de surveillance et de centraliser les vidéos sur un serveur FTP hébergé chez *Hebertek*. Sur les sites, les caméras IP viennent d'être installées, connectées physiquement et configurées.

Le déploiement de la nouvelle infrastructure doit se faire rapidement en conformité avec le cahier des charges. Il a été décidé que les techniciens réseaux locaux des sites de *Bloom* doivent préparer la migration et procéder à l'installation des routeurs configurés par *Hebertek*.

Le responsable du projet *Bloom* chez *Hebertek* doit assister les techniciens de *Bloom* pour faciliter la mise en place de la nouvelle infrastructure. Vous êtes chargé-e d'assister et de conseiller le technicien *Bloom* du site de Paris.

L'essentiel des étapes préparatoires à la mise en place du lien avec les serveurs hébergés concerne le routeur-commutateur à services intégrés (ISR), nommé *RBL*.

Votre responsable vous charge de baliser les étapes nécessaires à la migration du réseau en donnant le détail des opérations à réaliser sur l'équipement *RBL*.

Question B.1.1

Justifier le bien fondé de la proposition de l'administrateur réseau d'*Hebertek* de supprimer la ligne 4 de la table de routage de l'équipement *RBL*.

Question B.1.2

Donner toutes les modifications de configuration à réaliser sur le commutateur-routeur RBL pour obtenir le fonctionnement attendu dans la nouvelle configuration du réseau de la société *Bloom*.

Question B.1.3

Expliquer si le basculement de l'ancienne configuration de ce matériel vers la nouvelle provoquera une interruption de service.

Mission 2 : configuration du serveur d'application

Jusqu'à maintenant, un seul serveur d'application *Terminal Server* (TS) gérait les postes de type client léger. La généralisation de ce type de postes à toutes les boutiques pose le problème de son sous dimensionnement. Il a donc été remplacé par une grappe (*cluster*) de serveurs TS pour répondre aux besoins actuels et faciliter une évolution future si nécessaire.

Cette grappe est composée de trois serveurs aux caractéristiques physiques identiques avec une implémentation du service de répartition de charge réseau dit "RCR" afin de solliciter les trois serveurs de manière équilibrée.

Question B.2.1

Justifier le fait que le mode de répartition choisi par *Hebertek* pour le client *Bloom* soit le mode de répartition de charge «Répartition égale » du service RCR.

Mission 3 : maintenance du serveur d'application

Un mois après la mise en service de la grappe de serveurs TS, des utilisateurs ont fait remonter l'incident suivant : l'ouverture de session leur est parfois refusée. Après avoir lu les fichiers de trace des serveurs au moment d'un dysfonctionnement, vous constatez qu'un des serveurs possède 16 sessions *Terminal Server* ouvertes (le maximum autorisé) alors que les autres possèdent respectivement 7 et 3 sessions ouvertes. Une piste possible de ce dysfonctionnement semble être la durée des sessions sur chaque serveur.

Question B.3.1

Rechercher les causes du dysfonctionnement et alimenter la base de connaissances en expliquant dans une courte note l'origine de cet incident et la solution à mettre en œuvre pour y remédier.

Les utilisateurs des boutiques vous font remonter un dysfonctionnement récurrent. Vous disposez d'une des fiches d'incident avec le message d'erreur affiché par leurs navigateurs lorsque leur demande de connexion est dirigée pour la première fois vers le serveur physique **H-TSE-1** du *cluster*. Le même problème apparaît la première fois que leur tentative de connexion est dirigée vers le serveur physique **H-TSE-2** ou **H-TSE-3**.

Question B.3.2

- Expliquer les causes de l'apparition de ce message.
- Écrire les procédures pour résoudre cet incident.

Dossier documentaire : cahier des charges de la société *Bloom*

1. Les services, l'infrastructure et les outils *Hebertek*

1.1 Catalogue des services proposés par *Hebertek*

Offre	Type d'hébergement	Détail de la solution	Périmètre d'intervention	Éléments de coût
N°1	Hébergement de serveurs non administrés (<i>Hosting</i>)	Hébergement des serveurs du client dans notre ferme d'hébergement	Gestion et administration des serveurs aux soins du client.	Hébergement forfait /mois Débit x/Gb Nombre de VPN Nombre de VLAN
N°2	Hébergement de serveurs	Hébergement des serveurs du client dans notre ferme d'hébergement	Gestion et administration des serveurs définies par un périmètre d'infogérance. L'administration, la supervision et la maintenance peuvent être partagées entre <i>Hebertek</i> et le client en fonction de ce périmètre.	Hébergement forfait /mois Location matérielle / forfait mois Débit x/Gb Nombre de VPN Nombre de VLAN Infogérance forfait/mois
N°3	Hébergement de serveurs administrés en « location de puissance machine »	Administration et exploitation des serveurs	Gestion et administration de serveurs dédiés par nos soins : <ul style="list-style-type: none">- supervision et administration ;- maintenance matérielle.	Administration des serveurs Hébergement forfait /mois Location matérielle / forfait mois Débit Nombre de VPN et VLAN

Pour tous les types d'hébergement

- Protection physique : contrôle par badge personnalisé sur tous les accès. Traçabilité de tous les accès. Contrôle vidéo et audio des personnels présents dans les *box*.
- Surveillance 24h/24, 7j/7 des équipements et serveurs avec alerte SMS. Intervention en moins de deux heures. Les équipements sont supervisés au plan matériel et l'équipe d'exploitation gère les alertes rigoureusement au fur et à mesure de leur signalement.
- Hotline : en fonction du contrat. À cet effet, un numéro d'astreinte est mis à votre disposition.

Option assistance technique à distance

- Intervention en moins d'une heure ou sous 24h
- Helpdesk de niveau 1 ou de niveau 2 et 3

Options applications

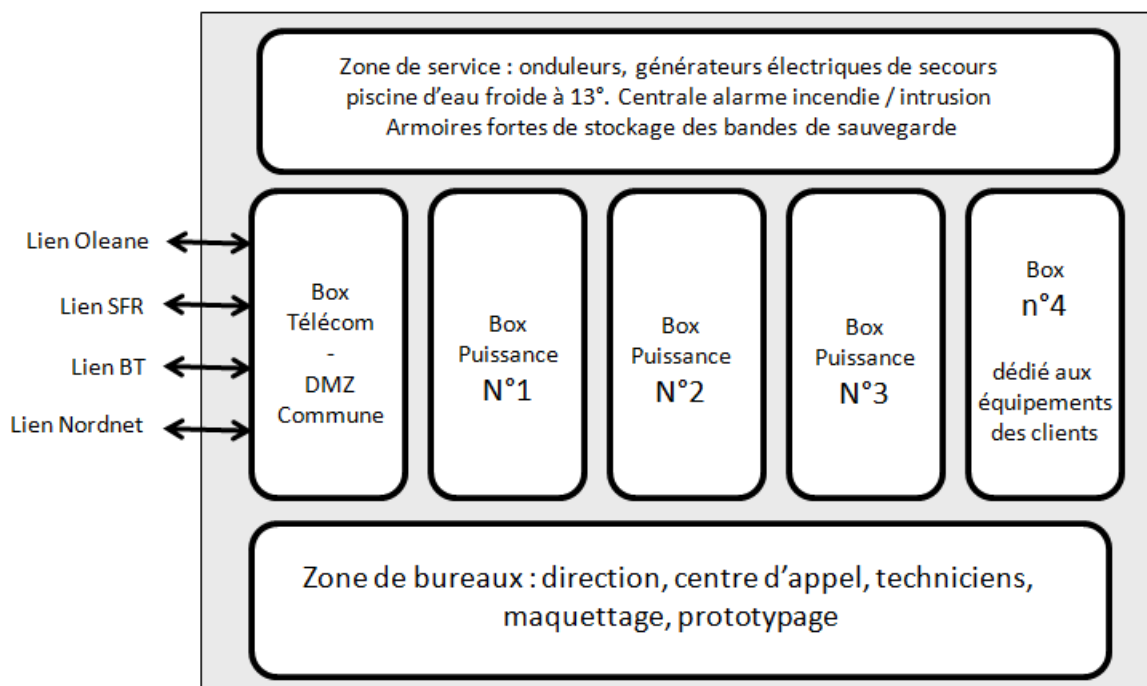
- Mise à disposition d'une messagerie et/ou d'un outil de travail collaboratif
- Service d'impression
- Service de streaming
- VOIP

Options sécurité

- Sauvegarde sur équipement centralisé avec une politique de sauvegarde complète et sauvegarde incrémentale. Stratégie de sauvegarde en 7j/7. Contrôle journalier des sauvegardes
- Stockage redondant à la demande
- Proxy, pare-feu
- Supervision
- Protection anti-virus
- Détection d'intrusion
- Test d'intrusion
- Plan de reprise d'activité (PRA)

1.2 L'infrastructure *Hebertek*

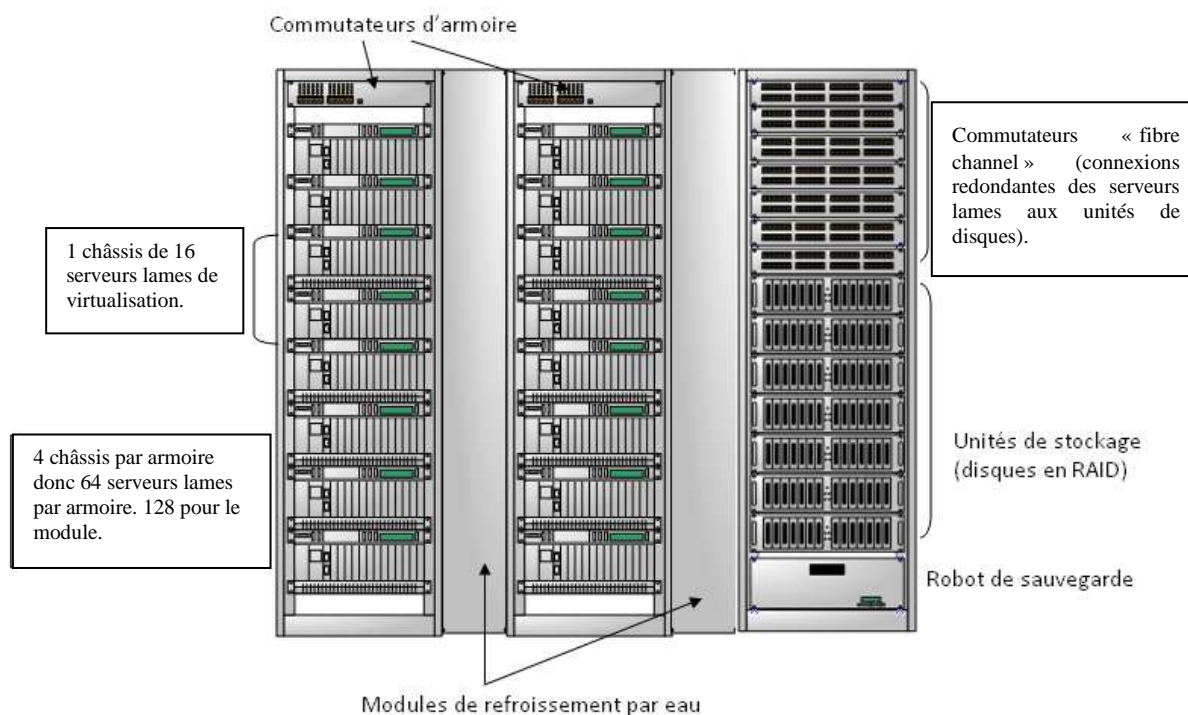
Plan d'une des deux fermes d'hébergement de la société *Hebertek*



Rôle du *Box Télécom*

- centralisation des 4 arrivées « télécom » des quatre FAI professionnels (« FAI de FAI ») : *Oleane*, *SFR*, *BT* et *Nordnet*. La redondance des liens vers les FAI permet de réduire les risques d'indisponibilité de l'accès Internet.
- pare-feux virtuels isolant les réseaux des clients ;
- zone de DMZ commune à tous les clients, exposée sur l'Internet.

Composition d'un « module armoire » dans les « *box de puissance* » *Hebertek*



Chaque « *box* de puissance » contient quatre « modules armoires », soit 512 serveurs lames exécutant chacun jusqu'à 16 instances de systèmes virtuels dotés en moyenne de 4 Go de mémoire réelle chacun. Un *box* de puissance peut donc abriter jusqu'à 8 192 systèmes virtualisés. La capacité de la ferme est donc de plus de 24 000 systèmes.

Chaque armoire est reliée à un commutateur de *box*. Chaque *box* est relié à un équipement centralisateur dans le *box* « *Télécom* ».

Chacune des machines physiques (et donc des systèmes virtuels qu'elles abritent) est dotée d'au moins trois accès physiques :

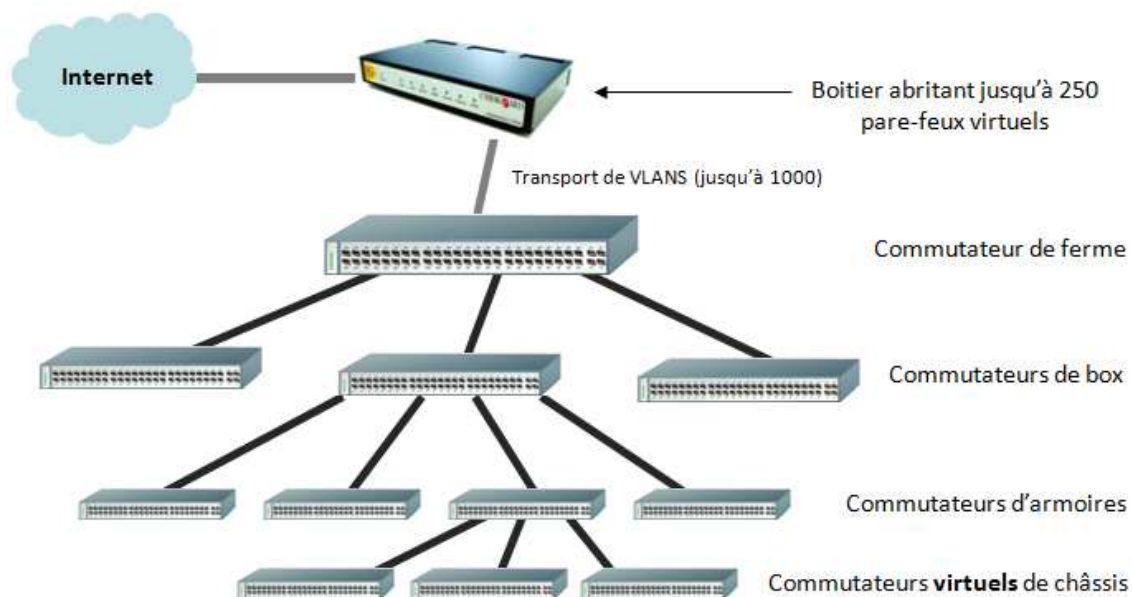
- une prise à la norme propriétaire *ILO* permettant un accès distant de bas niveau pour allumage et extinction distants, accès au *BIOS*, installation de système d'exploitation, administration ;
- une prise Ethernet dédiée à un VLAN de sauvegarde et d'administration ;
- une (quelquefois plusieurs) prise(s) Ethernet dite(s) « DATA », associée(s) au VLAN du système informatique du client.

Un routeur sépare tous les VLAN des clients de la zone d'administration (le plateau technique) depuis laquelle des logiciels et des techniciens supervisent et administrent les machines en contrat d'infogérance, louées ou non.

Les sauvegardes sont réalisées de jour par copie de disque à disque, puis les données sont stockées la nuit sur bandes, via un robot de sauvegarde.

Les systèmes informatiques des clients sont tous séparés dans des VLAN propres à chaque client et chaque *box* peut comporter jusqu'à 1 000 VLAN.

Hiérarchie des commutateurs au sein d'une ferme *Hebertek*



Les liens redondants entre les commutateurs de *box* sont en 10 Gigabits/seconde. Les autres liens sont en 1 Gigabit/s. Les commutateurs virtuels de chacun des châssis de virtualisation

sont gérés par l'hyperviseur *Microsoft Hyper-V* qui équipe tous les *box* de puissance. Certains systèmes appartenant aux clients sont équipés en *Vmware ESX*.

Chaque lien peut transporter jusqu'à 1 000 *VLAN*. Certains clients ont des systèmes informatiques (et donc un *VLAN*) regroupant des machines de plusieurs *box*, réelles ou virtuelles, certaines louées, d'autres non.

L'accès dans le *VLAN* du client se fait depuis l'extérieur par un pare-feu virtuel géré par un équipement spécialisé.

Un protocole dynamique (*VTP*) assure la connaissance de tous les *VLAN* par tous les commutateurs.

2. Les outils *Hebertek*

2.1 La gestion des commutateurs avec le protocole *VTP (VLAN Trunking Protocol)*

Le protocole *VTP* (de niveau 2) développé par *Cisco* permet de centraliser la gestion de la base des données des équipements *Cisco* d'un réseau et d'en faciliter le paramétrage en évitant de devoir déclarer tous les *VLAN* sur tous les commutateurs traversés par ceux-ci.

Il est constitué de trois modes :

- Serveur : Il s'agit d'un équipement sur lequel il est possible de créer, modifier, ou supprimer des *VLAN* et de les transmettre au "domaine *VTP*" (ensemble de *N* commutateurs utilisant *VTP* et connecté à un certain nom de domaine) via les liens 802.1Q.
- Client : Il s'agit d'un équipement qui va recevoir les informations du serveur *VTP* qui se situe dans le même domaine *VTP*, les prendre en compte, et les retransmettre aux commutateurs qui lui sont interconnectés.
- Transparent : le commutateur va recevoir les informations du serveur *VTP* du même domaine et les retransmettre **sans les prendre en compte**. Il est possible de créer, modifier ou supprimer des *VLAN* en local sur ce commutateur sans que ceux-ci soient répercutés sur les autres équipements du même domaine.

Séquence de paramétrage des commutateurs

Dans le commutateur "server"

- choix de la version du protocole *VTP*
- lancement de *VTP* en mode serveur
- nommage du domaine *VTP* XXXXX
- indication d'un mot de passe pour le domaine *VTP* XXXXX
- activation du mode *pruning* (permettant une limitation de la bande passante utilisée par le protocole)
- création des *VLAN*

Dans les commutateurs "client"

- choix de la version du protocole *VTP*
- lancement de *VTP* en mode client (ou en mode transparent)
- connexion au domaine *VTP* XXXXX
- indication du mot de passe du domaine *VTP*

En mode client, tous les *VLAN* connus du serveur sont créés dans le commutateur client.

En mode transparent, les informations reçues du serveur sont simplement transmises aux commutateurs connectés. (source : www.telecom-reseaux.net)

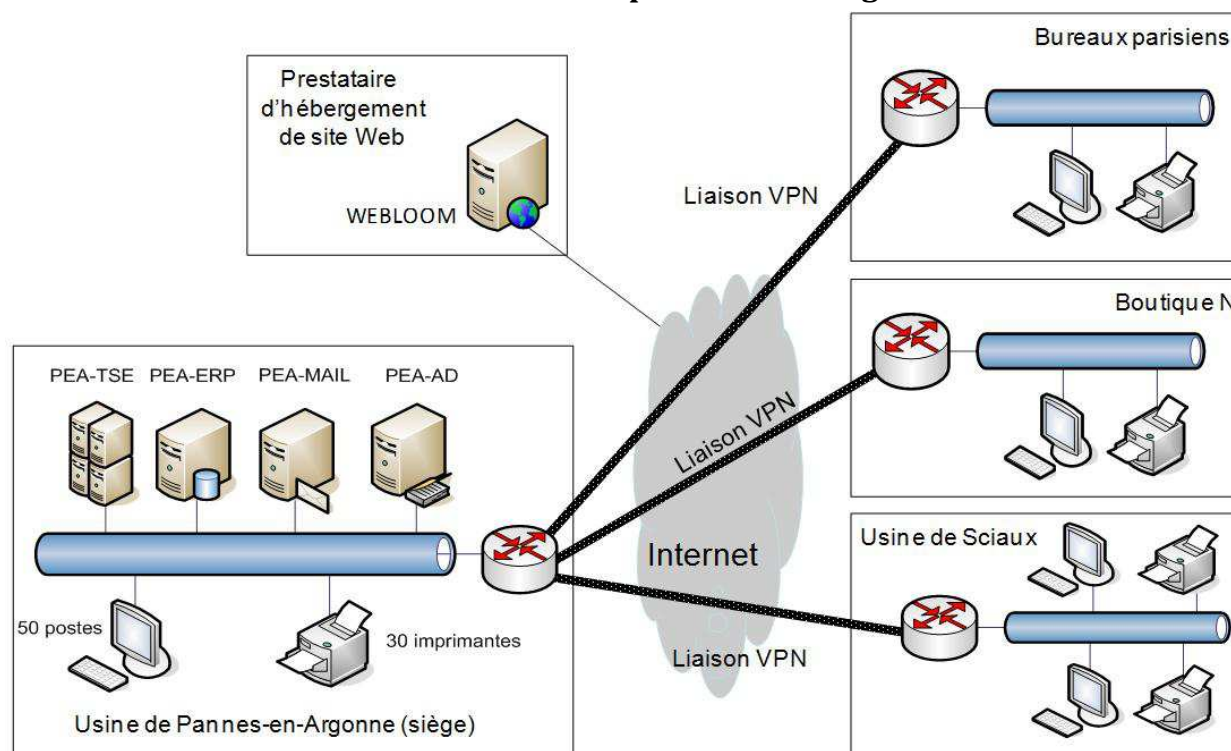
2.2 L'outil de supervision

Extrait d'une liste de commandes de l'outil de supervision

<i>check_traffic</i>	Permet de contrôler le débit en entrée et en sortie d'une interface réseau en retournant des données de performance.
<i>check_nt</i>	Permet de superviser des PC dont le système d'exploitation est Windows.
<i>check_procs</i>	Permet de surveiller le nombre de processus.
<i>check_snmp_cpu</i>	Permet de contrôler la charge CPU d'un serveur.
<i>check_https</i>	Permet de tester si un service HTTPS est bien lancé sur la machine à superviser.
<i>check_ping</i>	Permet de vérifier qu'un hôte est bien joignable.
<i>check_dns</i>	Permet d'interroger un service DNS et de résoudre une adresse.
<i>check_host_alive</i>	Permet de vérifier si un hôte est joignable.
<i>check_http</i>	Permet de tester si un service HTTP est bien lancé sur la machine à superviser.
<i>check_dhcp</i>	Permet de vérifier que le service est bien disponible.
<i>check_ftp</i>	Permet de vérifier la disponibilité d'un service FTP.
<i>check_disk</i>	Permet de vérifier l'espace disponible.
<i>check_users</i>	Permet de vérifier le nombre d'utilisateurs connectés.
<i>check_uptime</i>	Permet de vérifier depuis combien de temps une machine est démarrée.
<i>check_dir_size</i>	Permet de vérifier la taille occupée par un répertoire sur un disque/partition Windows

3. Analyse de l'existant de la société Bloom

3.1 Plan du réseau Bloom avant la mise en place de l'hébergement chez Hebertek

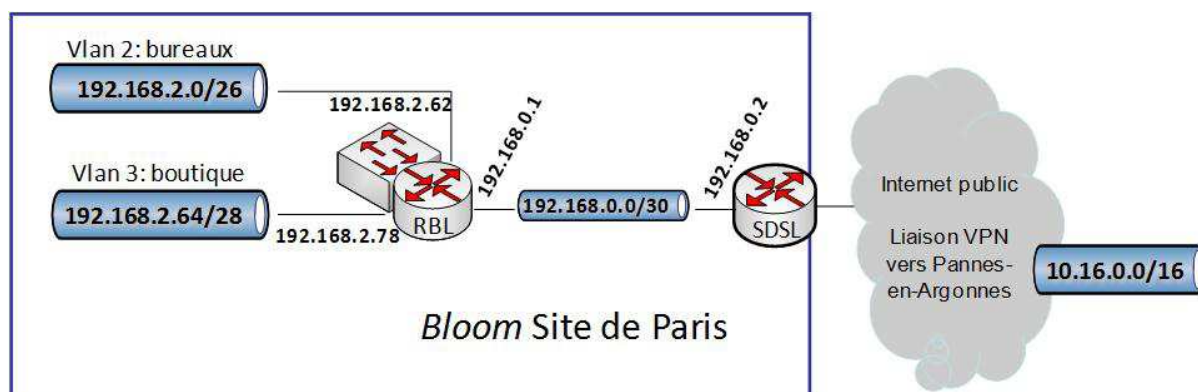


3.2 Liste des serveurs et services associés de la société *Bloom*

Nom du serveur	Emplacement	Services	Système
PEA-AD	Pannes-en-Argonne	Annuaire central - Serveur de données - Serveur d'impression	Windows 2003 server
PEA-MAIL	Pannes-en-Argonne	Serveur de courrier - Exchange	Windows 2003 server
PEA-ERP	Pannes-en-Argonne	Serveur ERP - Adonix	Windows 2003 server
PEA-TSE	Pannes-en-Argonne	Serveur d'applications - Terminal Server	Windows 2003 server
WEBloom	Hébergeur de site web	Site web vitrine	Linux - Apache

3.3 Configuration du réseau de la société *Bloom* sur le site de Paris

Schéma logique du réseau



Le réseau local est séparé en deux VLAN : le réseau des bureaux et le réseau de la boutique. Un équipement à services intégrés (routeur + commutateur), RBL, permet à ces réseaux d'accéder à internet d'une part, aux serveurs du siège de Pannes-en-Argonne via une liaison SDSL d'autre part.

Configuration du routeur « cœur du réseau » : RBL

RBL est un équipement intégrant les services d'un commutateur et d'un routeur, équipé de huit ports. Son paramétrage actuel est le suivant :

■ VLAN

N° de VLAN	Réseau	Adresse de l'interface
2	Postes des bureaux parisiens	192.168.2.62/26
3	Postes de la boutique	192.168.2.78/28

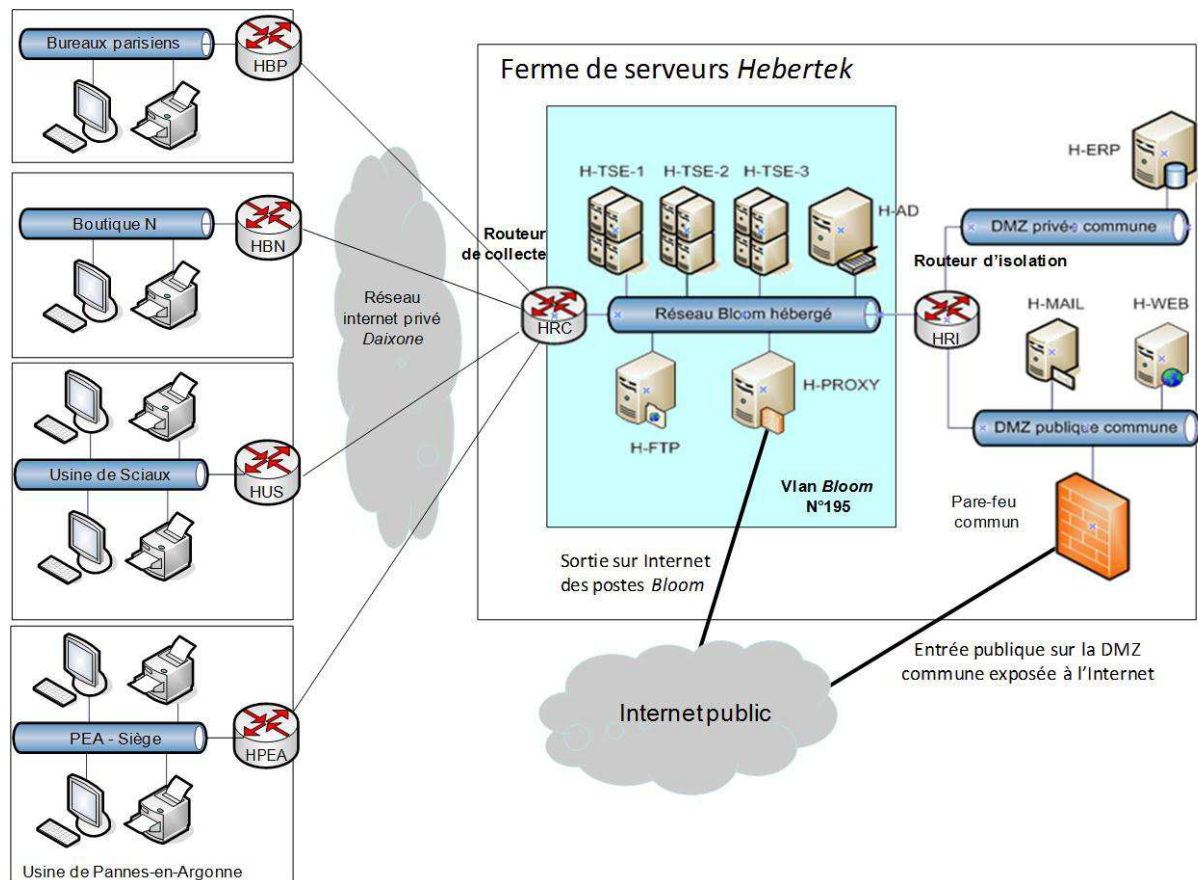
Note : Les adresses de passerelle correspondent au dernier hôte de la plage de l'adresse réseau.

■ Table de routage

	Protocole de routage	Adresse du réseau de destination	Masque du réseau de destination	Adresse de passerelle	Adresse de l'interface
1	Route connectée	192.168.0.0	255.255.255.252	192.168.0.1	192.168.0.1
2	Route connectée	192.168.2.0	255.255.255.192	192.168.2.62	192.168.2.62
3	Route connectée	192.168.2.64	255.255.255.240	192.168.2.78	192.168.2.78
4	Route statique	10.16.0.0	255.255.0.0	192.168.0.2	192.168.0.1
5	Route statique	0.0.0.0	0.0.0.0	192.168.0.2	192.168.0.1

4. Notre proposition pour le client *Bloom*

4.1 Plan du réseau *Bloom* après la mise en place de l'hébergement



4.2 Notes sur le nouveau plan de réseau *Bloom*

Les DMZ publique et privée sont communes à l'ensemble des clients hébergés par *Hebertek* et leur exposition à l'internet public se fait via un pare-feu commun. Dans la DMZ publique sera installé le serveur *web* (H-WEB) interfacé avec l'ERP de la société (H-ERP) qui sera installé dans la DMZ privée.

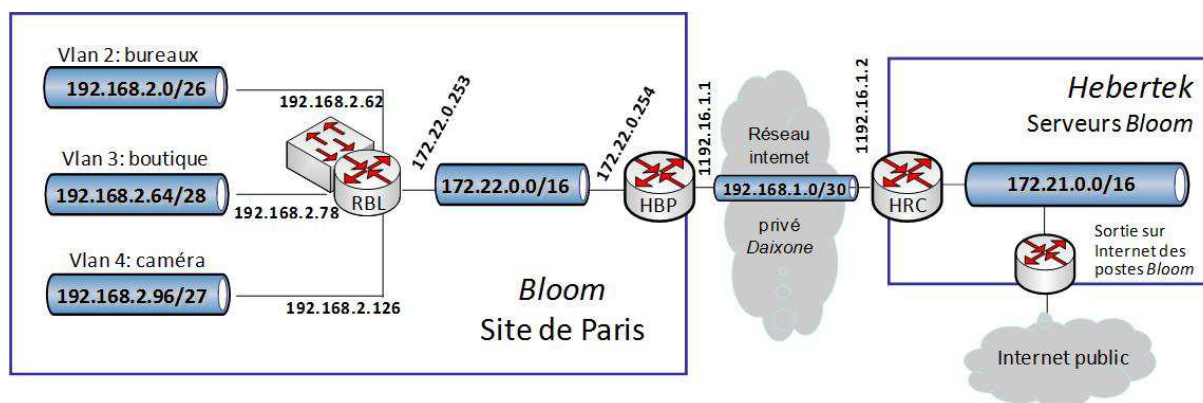
La sortie sur Internet de l'ensemble des postes des usines, des bureaux parisiens et des boutiques se fera via un serveur *proxy* hébergé, au sein du VLAN Client n°195, loué et dédié à la société *Bloom*.

Après absorption d'une seconde cristallerie, le nombre de boutiques sera triplé. En conséquence, pour garantir les meilleurs temps de réponse, on proposera la mise en place de deux serveurs d'application *Terminal Server* supplémentaires.

Les caméras IP de surveillance des sites déposeront leurs clichés sur un serveur FTP (H-FTP) hébergé également dans le VLAN n°195.

4.3 Configuration du réseau de la société *Bloom* sur le site de Paris

Schéma logique



Cahier des charges de la migration

La société *Bloom* conserve l'équipement RBL et les adresses de réseau des VLAN existants du site parisien. On prévoit de mettre en place un VLAN supplémentaire (VLAN 4) destiné à relier les caméras de surveillance IP. Les clichés de ces caméras seront transférés sur un serveur FTP hébergé chez *Hebertek*. Le VLAN 4 utilise l'adresse réseau 192.168.2.96/27.

L'ensemble des postes du site parisien passe par le réseau Internet privé *Daixone* pour accéder aux serveurs hébergés et à l'internet public. Le réseau des serveurs hébergés utilise l'adresse 172.21.0.0/16. Le routeur de terminaison HBP est configuré par *Hebertek* avec l'IP 172.22.0.254 comme adresse de passerelle pour le réseau local parisien 172.22.0.0/16.

Tous les routeurs de terminaison dédiés à la société *Bloom* sont configurés exclusivement en routage dynamique basé sur le protocole RIP. On rappelle que les techniciens de la société *Bloom* n'ont pas accès au paramétrage de ces équipements.

5. Les outils nécessaires à la nouvelle infrastructure *Bloom*

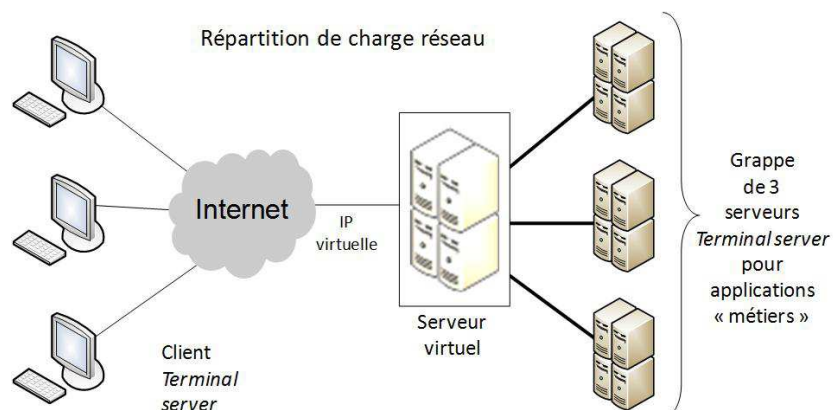
5.1 Fonctionnement du protocole RIP (*routing information protocol*)

Le routage dynamique *RIP* consiste à demander à chaque routeur de « publier » la liste des réseaux qui lui sont connectés directement. Le protocole dynamique permet ensuite à chacun des routeurs d'apprendre les routes publiées par ses voisins et donc d'échanger l'information permettant le routage.

5.2 Répartition de charge réseau / équilibrage de sessions *Terminal Server*

A. La répartition de charge réseau (nommée ici service « RCR »)

En plus d'une répartition de charge réseau, le service RCR permet d'assurer une tolérance de panne sur les membres de la grappe.



Le RCR utilise pour cela une adresse IP virtuelle unique ainsi qu'une adresse MAC virtuelle unique qui va permettre d'envoyer les données à destination du service mis en grappe (le serveur virtuel) à l'ensemble des membres de la grappe.

Les clients se connecteront donc à l'aide de l'adresse IP virtuelle. Le serveur virtuel est en fait hébergé sur **chaque machine physique de la grappe** (*cluster*) ce qui permet une tolérance de panne. Il faut donc implémenter le service RCR sur chaque serveur.

Les caractéristiques du service RCR

- **Support du TCP/IP** : les règles de configurations du RCR permettent d'agir sur des ports ou des protocoles particuliers.
- **Répartition de charge** : les requêtes envoyées par les clients sont automatiquement réparties sur les membres de la ferme de serveurs qui compose la grappe.
- **Haute disponibilité** : le service RCR permet de détecter automatiquement les serveurs défaillants afin de redistribuer leurs clients sur les autres serveurs.
- **Possibilité d'évolution** : avec le service RCR, il est possible d'ajouter jusqu'à 32 hôtes dans la ferme de serveurs pour prendre en charge les clients.
- **Administration** : Le service RCR est administré via un outil en ligne de commande.

Les trois modes de répartitions de charges possibles

- **Répartition manuelle** : elle permet de définir un poids de charge pour chaque nœud du *cluster*. Si trois serveurs sont configurés respectivement avec les poids 50, 30, 20, le premier va recevoir la moitié des requêtes, le second 30% et le dernier 20%.
- **Répartition égale** : elle permet de répartir de façon égale les requêtes sur l'ensemble des serveurs composant le *cluster*.
- **Répartition prioritaire** : après avoir défini des priorités pour chaque serveur, l'ensemble du trafic sera tout d'abord acheminé sur le serveur ayant la priorité 1. Si celui-ci tombe en panne, l'ensemble du trafic sera envoyé au serveur de priorité 2 et ainsi de suite.

Le service RCR ne prend pas en charge le taux d'occupation des ressources serveurs (RAM, CPU ou autres limitations imposées par les logiciels).

B. L'équilibrage des sessions (nommé ici service ES)

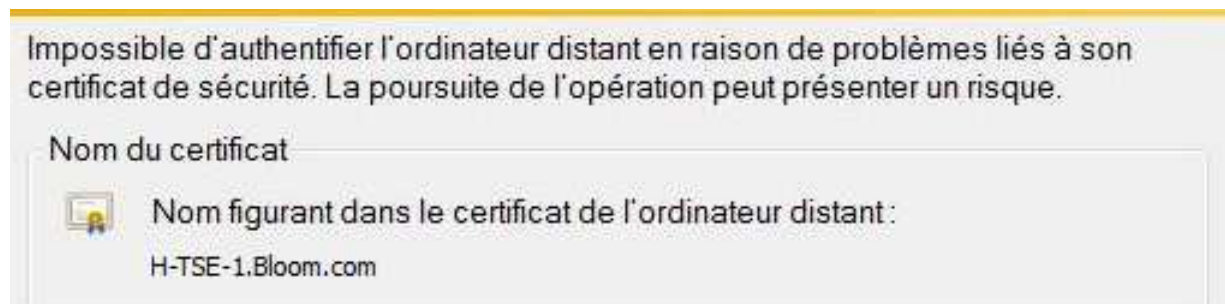
Il s'agit d'un service optionnel qui, s'il est installé, prend en charge l'équilibrage de la **charge des sessions** entre les serveurs *Terminal Server* (TS) d'une grappe de serveurs, ainsi que **la reconnexion à une session existante** dans une grappe de serveurs TS à charge équilibrée de type RCR. L'équilibrage de sessions stocke les informations d'état de session, ce qui inclut les ID de session et les noms d'utilisateurs qui leur sont associés, ainsi que le nom du serveur sur lequel réside chaque session.

Ceci permet de répartir équitablement la charge des sessions entre les serveurs d'une grappe de serveurs TS. Grâce à cette fonction, les nouvelles sessions utilisateurs sont redirigées vers le serveur TS qui héberge le plus petit nombre de sessions.

Une fois qu'un utilisateur s'est authentifié, le serveur TS qui a accepté la connexion initiale (information fournie par le service RCR) interroge le service d'équilibrage de sessions (ES) pour déterminer finalement vers quel serveur rediriger l'utilisateur.

Fiche d'incident

Message affiché par les navigateurs des boutiques lors de la connexion au serveur H-TSE-1



Détails du certificat du serveur H-TSE-1

