

Business Connect

Le magazine d'Information de Telindus n°14 • Octobre 2010



Les exigences
des nouveaux
Data Centers,
une infrastructure adaptée !

- Les tests d'intrusion, baromètres de la Sécurité en ToIP
- Le financement au service de votre Opex, élément clé de compétitivité
- Nos clients témoignent : Aix-en-Provence, Conseil Général de la Moselle

 **telindus**
belgacom ICT

together
with

belgacom



A l'image des Teltechdays que nous organisons partout en France, et que vous avez été nombreux à visiter, cette nouvelle édition de *Business Connect* a pour ambition de vous éclairer sur les opportunités technologiques qui vous sont offertes. Cet éclairage se veut à la fois stratégique et technique, mais également pratique et complet sur les problématiques des infrastructures du Data Center, des Communications Unifiées et de la Sécurité.

Nous espérons vivement que cette lecture vous aide dans votre choix et nous restons à votre disposition pour vous accompagner.

HENRI JUIN • DIRECTEUR GÉNÉRAL DE TELINDUS FRANCE



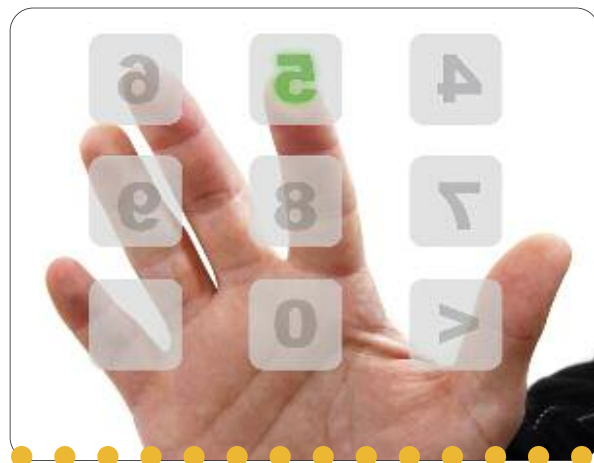
Business Connect - n° 14 - Octobre 2010

Édité par Telindus - 10 avenue de Norvège - Z.A. Courtaboeuf - BP 742 - 91962 Les Ulis Cedex France - Tél. : 01 69 18 32 32

- Directrice de la Publication : Odile Foubert
- Comité de Rédaction : Odile Foubert - Jean-Marc Chartres - Florence Nollet Le Noan - Nicolas Leseur - François Perveur - Marc Moscovitch - Stéphane Loras - Raymond Salerno
- Gestion éditoriale et conception graphique : 1000 ans Communication 8 avenue du Parc - 92400 Courbevoie contact@1000anscommunication.com
- Impression : Prisme Graphique 176 avenue Charles-de-Gaulle - 92200 Neuilly-sur-Seine

Le contenu d'un article n'engage que son auteur - Telindus et Business Connect sont des marques déposées

SOMMAIRE



EXPERT

● **PCI DSS, Sécurité ciblée** : douze exigences, deux cents recommandations pour sécuriser le paiement par carte bancaire.

Page 4

● **Contrôle d'identité sur la Toile publique** : renforcer les droits du citoyen sur Internet face aux cybercriminels.

Page 5

OFFRE

● **Utiliser les tests d'intrusion comme baromètre de la Sécurité en ToIP** permet d'évaluer les menaces et d'y remédier.

Page 6

● **Services managés et de conciergerie de vidéoconférence** : donner les moyens aux utilisateurs de tirer la quintessence des outils.

Page 7

● **Sécurité de votre entreprise** : un plan d'accompagnement pour atteindre un niveau de sécurité déterminé.

Page 8



SOMMAIRE



DOSSIER

● **Les exigences des nouveaux Data Centers, une infrastructure adaptée !**
L'hébergement des applications informatiques et des données ainsi que la gestion des Data Centers obligent l'entreprise à mettre en adéquation les exigences de performance vitales pour son activité et les contraintes en termes de dépenses



et d'investissements. Pour ce faire, elle dispose désormais de solutions privilégiant la mutualisation et l'industrialisation – architectures orientées services (SOA), virtualisation, cloud computing, applications en mode SaaS – comme autant d'alternatives à considérer avec attention.

Pages 9 à 13

EXPERIENCE

● **Sécuriser le déménagement de son Data Center** en évitant le dommage des données et la perturbation des activités de l'entreprise.

Page 14

TENDANCE

● **Le financement au service de votre Opex,** ou comment l'investissement dans une infrastructure moderne devient un élément clé pour améliorer la compétitivité de l'entreprise.

Page 15

REALISATIONS

Telindus toujours plus à l'écoute des besoins métier de ses clients.

● **Le CG 57** permet aux 94 collèges et aux 30 sites du Conseil Général de la Moselle d'accéder au réseau via une liaison optique à très haut débit.

Pages 16 et 17

● **La Ville d'Aix-en-Provence** augmente la disponibilité de connexion à Internet et lui assure une meilleure sécurité.

Page 18

● **Un groupe industriel français** adopte les nouveaux firewalls pour optimiser sa sécurité.

Page 19

PARTENAIRES

Le point sur les technologies et solutions des partenaires.

● **Check Point** sécurise aussi les environnements virtualisés avec sa solution logicielle VPN-1 Virtual Edition.

Pages 20 et 21



● **F5** accompagne la mutation des Data Centers avec la nouvelle version du BIG-IP Local Traffic Manager en offrant une consolidation des services.

Page 22

BREVE - INVITATION

● **Telindus Technology Days, Paris, Rennes, Bordeaux, Toulouse, Strasbourg...**
Réussir 2015 : quels choix structurants en 2010 pour faire face aux futurs défis technologiques ?

Inscription sur www.telindus.fr

Page 23



PCI DSS, sécurité ciblée

Internet a transformé les communications, et notamment les activités commerciales, en augmentant la vitesse, la simplicité et le périmètre géographique des transactions. Les criminels ont très vite trouvé les failles de cet environnement ouvert dont les règles diffèrent d'un pays à l'autre.

Le Conseil des normes de sécurité PCI est un forum international ouvert pour le développement, l'amélioration, le stockage, la diffusion et la mise en œuvre en continu de normes de sécurité pour la protection des données de comptes. Il est l'auteur du standard universel PCI DSS (Payment Card Industry Data Security Standard).

La dernière version de PCI DSS 1.2.1 consiste en douze exigences et plus de deux cents recommandations et procédures d'évaluation de sécurité :

- 1• Installer et maintenir la configuration d'un firewall destiné à protéger l'information des titulaires d'une carte ;
- 2• Ne pas utiliser de paramètres par défaut au niveau d'un système, d'un mot de passe ou d'autres paramètres liés à la sécurité ;
- 3• Protéger toute information stockée relative aux titulaires de cartes ;
- 4• Chiffrer la transmission d'informations des

propriétaires de cartes effectuée par le biais de réseaux publics ;

- 5• Utiliser et mettre à jour régulièrement l'application et les antivirus ;
- 6• Développer et maintenir la sécurité des systèmes et des applications ;
- 7• Restreindre l'accès aux données des titulaires de cartes en fonction des impératifs et besoins ;
- 8• Assigner un identifiant unique à chaque personne nécessitant un accès informatique ;
- 9• Restreindre l'accès physique aux systèmes hébergeant les informations des titulaires de cartes ;
- 10• Suivre et surveiller tous les accès aux ressources du réseau ainsi qu'aux données des titulaires de cartes ;
- 11• Tester régulièrement les systèmes et processus de sécurité ;
- 12• Maintenir une politique de sécurité de l'information pour les employés et les partenaires.

RECOMMANDATIONS

Attention aux réseaux plats. Ils rendent toute l'organisation sujette à PCI. PCI s'applique aux systèmes qui traitent, transmettent et stockent l'information des titulaires de carte. Il s'applique sur un périmètre informatique précis qu'il conviendra de repérer et d'isoler.

PCI représente un minimum de bonnes pratiques et, comme toujours, une bonne analyse de risques peut être salutaire dans le nombre de



mesures à mettre en œuvre. En effet, il faut s'interroger sur la nécessité de conserver des données sensibles de type bancaire. La réduction du périmètre peut conduire à revoir les processus métiers car très souvent le numéro de carte est utilisé par commodité ou habitude et non par besoin. La mise en œuvre de PCI DSS est donc l'opportunité de revoir cette utilisation et de remplacer dès que possible le PAN par un authentifiant chiffré.

Les données bancaires n'appartiennent ni au porteur ni au commerçant, mais à l'émetteur de la carte, conformément au contrat porteur. Il est nécessaire de réduire la conservation de certaines données comme le PAN et la date d'expiration, et de la justifier. Les exigences PCI de droit privé ne peuvent se substituer à la loi en vigueur sur le sol français. À ce titre, la sensibilité des données nominatives de type carte bancaire justifie au sens de la CNIL et de la loi Informatique et Libertés les exigences dictées par le PCI DSS.

ISO 27 001 doit être vu comme le socle du processus sécurité de l'information, alors que PCI DSS est une réponse au niveau de la sécurité du traitement informatique de la carte bancaire. PCI n'est pas un système de gestion de la sécurité, il ne couvre pas l'ensemble de la chaîne physique et logique du traitement de cartes. D'ailleurs, la cybercriminalité à la carte bancaire en 2009 s'oriente sur les cartes prépayées ou les DAB (Distributeurs Automatiques de Billets) ; comme toujours la sécurité faillit par ses maillons faibles.

C'est par une itération permanente sur les nouvelles menaces de bout en bout que nous réduisons les risques, sans oublier les principes d'authentification dite forte des cartes bancaires. ■

JEAN-MARC CHARTRES • CONSULTANT SÉCURITÉ

UNIVERSEL PCI DSS

Ce standard universel PCI DSS a été créé pour aider les organisations qui travaillent avec des paiements par carte de crédit à prévenir les fraudes en augmentant les contrôles afférents à l'information et à son exposition. Au plan mondial, tous les partenaires affiliés qui transmettent, traitent ou stockent des données de cartes sont tenus de respecter les directives de sécurité définies dans le PCI DSS. Si elles sont enfreintes, le rapport contractuel peut être résilié sans délai et des dommages et intérêts demandés



pour compenser d'éventuelles amendes ou prétentions.

Ces exigences s'appliquent si un Numéro de Compte Principal ou Personnel (NCP ou PAN, Primary Account Number) est stocké, traité ou transmis.

Contrôle d'identité sur la Toile publique

Une carte d'identité numérique sécurisée, en débat actuellement au ministère de l'Intérieur, renforcerait les droits du citoyen sur Internet face aux cybercriminels grâce à une meilleure protection de la vie privée dans tous les échanges sociaux sur la Toile : administratifs (téléprocédures, e-vote), services marchands (services bancaires, achats en ligne, abonnements divers) et simples communications (chat, réseaux, jeux).

Les réseaux sociaux et les blogs ont provoqué la prolifération des données personnelles. L'utilité de se présenter pour mieux communiquer, ou trouver des internautes ayant des compétences ou des centres d'intérêts proches ou complémentaires développe le narcissisme et le désir d'augmenter sa visibilité et donc son capital social. Certes, tel sujet de recherche trouvera une communauté de chercheurs, mais combien usurperont un nom connu pour s'immiscer dans telle vie privée ? La maîtrise des informations publiées dépend de nous ou de nos amis mais pas leur durée de conservation qui dépend des sites. Notre vie privée peut être divulguée par n'importe qui, sans aucune autorisation.

« À notre naissance, nous sommes, chacun, dotés d'un capital comprenant notre intimité, notre identité. Ce capital, qui appartient à notre sphère de libertés individuelles fondamentales, est fragile. Si on le mutile, il ne se reconstituera pas facilement. » déclare Alex Türk, président de la CNIL.



Or abandonner toute frontière entre identité et intimité conduit à des débordements. Les traces du net définissent une pseudo-identité selon les données collectées. Champion de *World of Warcraft*, certes... Mais pas encore directeur de

stratégie ! Il se cache toujours un modèle économique prêt à exploiter ces informations... Selon les pays et les organisations, si l'usage l'emporte pour les uns, c'est le droit de propriété qui prime pour les autres. Cette notion est primordiale, mais elle nous pose un problème culturel quand il faut légiférer sur le droit d'usage.

Si l'authentification donne des droits, l'identité ne doit pas en donner mais constituer une preuve non répudiable.

En France, le délit d'usurpation d'identité n'est directement sanctionné que dans un cas : le fait de prendre le nom d'un tiers. En effet, l'article 434-23 du code pénal punit le « fait de prendre le nom d'un tiers, dans des circonstances qui ont déterminé ou auraient pu déterminer contre celui-ci des poursuites pénales (...). Dans ce cas, elle est punie de cinq ans d'emprisonnement et de 75 000 euros d'amende. »

Et compte tenu de l'ambiguïté de l'identité numérique, il est prévu d'insérer un article 226-16-1 dans le code pénal :

« Le fait d'utiliser, de manière réitérée, sur un réseau de communication électronique, l'identité d'un tiers ou des données qui lui sont personnelles, en vue de troubler la tranquillité de cette personne ou d'autrui est puni d'un an d'emprisonnement et de 15 000 euros d'amende. »

Avant que nous maîtrisions toutes les traces que nous laissons de manière à préserver notre image numérique, notre société a besoin d'être éclairée et guidée par le droit. La loi Informatique et Libertés protège les données nominatives sur les principes de loyauté,

MÉDOR AIME LES PIZZAS...
MÉDOR EST PEUT-ÊTRE UN CHIEN



Dessin de Peter Steiner paru dans le New Yorker du 5/07/1993

L'anonymat sur Internet est un leurre, car il est toujours rattaché à des traces personnelles. L'identité affichée en ligne n'est pas forcément l'identité réelle, ni toujours la même. La capacité à assumer des identités différentes est l'un des principaux attraits de l'identité numérique. Pour les besoins informatiques, nous avons multiplié les confusions entre authentifiant(s) et identité. A vouloir plusieurs identités numériques, nous en aurons aucune. L'identité doit être unique pour servir de preuve. Ce que l'on sait caractérise le mieux l'être humain ; ce que l'on possède peut être volé ; ce que l'on sait faire peut être imité ; ce que l'on est peut être usurpé ; mais ce que l'on sait peut plus difficilement être deviné. La biométrie à ce titre améliore l'identification, mais ne doit pas être un moyen d'authentification.

de transparence, et de proportionnalité (droit à l'oubli), et elle encadre leur utilisation dans une stricte finalité déclarée, cette notion garantit la protection sur l'usage. Une image ou information personnelle sortie de son contexte et utilisée à d'autres fins est un délit. La future carte d'identité numérique s'appuiera, entre autres, sur les critères suivants : l'authentification du porteur se fera par un tiers de confiance, et devra être sécurisée et cryptée (seul le fournisseur d'identité aura accès à ces informations). Des initiatives comme OpenID se mettent en place comme SSO (Single Sign One) pour l'identité, et permettent de revenir sur les fondamentaux. ■

JEAN-MARC CHARTRES • CONSULTANT SÉCURITÉ

Le test d'intrusion baromètre de la sécurité en ToIP

Le souci de sécurité des réseaux informatiques ne doit pas faire oublier les risques qui menacent la téléphonie sur IP : surfacturation, détournement d'appels, atteinte à la confidentialité des communications... Des tests d'intrusion pour évaluer les menaces sont indispensables.



De nos jours, la téléphonie sur IP (ToIP) fait partie intégrante du Système d'Information. C'est un élément névralgique, voire même « business critical », pour beaucoup d'entreprises. Or, si les paramètres de redondance et donc de disponibilité sont, en général, adressés lors des projets, les aspects de sécurité et les menaces qui planent sur la ToIP sont souvent laissés de côté.

Certaines fonctionnalités proposées par défaut dans les systèmes de téléphonie peuvent être utilisées à des fins malicieuses, soit à l'encontre des utilisateurs, soit pour une utilisation abusive de la téléphonie. Les risques sont multiples, qu'il s'agisse par exemple de l'écoute illégale des communications (atteinte à la confidentialité), ou de la fraude (communications abusives entraînant une surfacturation), de détournement d'appels, ou même de la revente de trafic sans oublier les risques juridiques. De plus, on assiste aujourd'hui à la multiplicité des applications disponibles regroupées sous l'appellation Communications Unifiées. Ce développement des applications augmente également les risques en matière de sécurité. Il devient alors primordial de bien mesurer les impacts de ces fonctionnalités et nouvelles applications sur la sécurité du SI. Un représentant de l'équipe sécurité devrait faire partie intégrante de tous les projets de ToIP dès la phase de définition des besoins.

LE TEST D'INTRUSION, INDICATEUR DE SÉCURITÉ

Pour détecter ces dangers, le test d'intrusion s'impose. Son but : définir les impacts potentiels d'une intrusion sur le SI en mettant en situation une attaque réelle, maîtrisée par des experts, dirigée contre la ressource cible. Ces tests sont principalement menés depuis le réseau interne de l'entreprise lorsque l'on parle de ToIP.

En ce qui concerne les Communications Unifiées, le scope est plus large et des tests externes sont également nécessaires.

Les tests d'intrusion identifient les faiblesses de l'architecture et des fonctionnalités déployées, mais ils démontrent aussi souvent l'absence de politique de sécurité dédiée à ces nouveaux médias. C'est pourquoi le recours à un expert reste le meilleur garant. Non seulement il détecte les points faibles du système, mais il aide à l'élaboration d'un plan de défense et à une



LE SRC DE TELINDUS

- 10 ingénieurs sécurité spécialisés dans les tests d'intrusion
- Un service existant depuis 1999
- Plus de 150 tests réalisés par an dans le monde
- 2 vulnérabilités constructeurs publiées en 2008
- 1 présentation des menaces ToIP au CLUSIR d'octobre 2009

stratégie de sécurité, englobant l'aspect technique et humain. Or ce genre d'exercice ne s'improvise pas ; il doit être guidé par l'expérience et une connaissance approfondie des problèmes de sécurité. Les pirates débordent d'imagination ; des audits réguliers et des mises à jour des mécanismes de défense sont dès lors des incontournables. ■

FLORENCE NOLLET-LE NOAN • RESPONSABLE SECURITY RESEARCH CENTER BU SÉCURITÉ PRÉVENTION ADMINISTRATION
NICOLAS LESEUR • MARKETING BU SPA



Telindus accompagne ses clients grâce à son centre de recherche en sécurité (SRC) et via son offre de tests intrusifs sur les systèmes de ToIP.

- Disponibilité : blocage de lignes, déni de service...
- Intégrité : suppression de messageries, modification d'appels...
- Confidentialité : écoute réseau (Wiretapping), enregistrement vocal, tentative d'écoute illicite des boîtes vocales ;
- Risques financiers : abus de ressources, et charges économiques falsifiées ;
- Risques juridiques : utilisation des ressources de l'entreprise « hackée » pour réaliser des actes malveillants, répréhensibles par loi.

L'expertise de Telindus a permis de mettre en évidence les attaques pratiquées et les vulnérabilités connues.

ATTAQUES LIÉES À L'INFRASTRUCTURE VOIP :

- vol de comptes SIP (appels gratuits) ;
- écoute du réseau afin de récupérer les échanges sur tous les constructeurs téléphoniques

- usurpation d'identité d'un appelant ;
- attaque du Call Manager sur port web.

ATTAQUES DE VULNÉRABILITÉS APPLICATIVES :

- enregistrements vocaux à distance à partir de flux http ;
- interception de mot de passe à partir de la boîte vocale (Alcatel, Cisco) ;
- interception des messages textes (Alcatel) ;
- validation d'entrée utilisateur du Cisco Call Manager.

Quid des **services managés** et de **conciergerie** de vidéoconférence ?

Avec l'introduction de nouvelles technologies, il est nécessaire d'accompagner l'utilisateur dans leur prise en main et de l'aider dans le changement de son quotidien. En effet, pour maîtriser 80 % des fonctions et tirer la quintessence d'un outil simple comme un téléphone ou une nouvelle version de son PC, une formation s'impose. Dans certains cas, il est nécessaire de créer de nouveaux services délivrés par de nouveaux métiers.



La conciergerie : un service de gestion des utilisateurs finaux

La vidéoconférence n'est pas une nouvelle technologie à proprement parler, cependant son utilisation s'est peu démocratisée. Les conditions ne s'y prêtaient guère. Les vidéoconférenciers ont tous été confrontés à cette situation angoissante d'arriver pour préparer la rencontre et de trouver un matériel plus ou moins adapté : plusieurs télécommandes, manuel d'utilisation ne correspondant pas tout à fait au matériel nouvellement installé... Le temps commence alors à s'accélérer. Créer des raccourcis avec les sites distants les plus utilisés peut résoudre cette problématique. Mais si l'ajout d'un site externe, comme un client, un fournisseur ou un collaborateur occasionnel, s'avère nécessaire, la maîtrise des fonctions de base de la vidéoconférence alors ne suffit plus. Comme tout outil de communication moderne, nous souhaitons pouvoir l'utiliser dans l'urgence. Ce qui augmente encore le besoin d'assistance technique et amène bien souvent, par défaut,

la vidéoconférence à se transformer en audioconférence.

Pour répondre à cette problématique Telindus a conçu deux types de service :

- un service managé pour gérer l'infrastructure de vidéoconférence,
- un service de conciergerie pour assister les utilisateurs dans leurs conférences.

Le but des services managés pour la vidéoconférence consiste à surveiller les équipements et leurs applications en vue de répondre à la question simple : l'infrastructure est-elle en état de marche ? En complément il est possible de contrôler la qualité et la performance, d'effectuer un reporting sur l'utilisation, et d'analyser la nature des incidents et leurs causes pour décliner un plan de progrès. Ce service

.....
*Répondre à une question :
 l'infrastructure est-elle en état
 de marche ?*

managé est opéré avec les mêmes processus et les mêmes applications que les autres services managés (téléphonie, réseaux Xan, sécurité, serveurs et système d'exploitation) afin d'apporter au client une gestion globale de son infrastructure.

La conciergerie est un service de gestion des utilisateurs finaux permettant :

• **EN MODE RÉACTIF**

d'assister en temps réel un utilisateur dans l'usage quotidien de la vidéoconférence :

- par une aide lors de difficultés liées à l'utilisation (mise en route de la salle, allumage des appareils, etc.) ;
- par une réponse à une demande d'information ;
- d'aider au démarrage d'une vidéoconférence non programmée ;
- de procéder à une modification simple en cours de séance sur demande des participants (résolution, template d'affichage) ;
- d'intégrer un participant à l'évènement lors de l'appel d'une vidéoconférence.

• **EN MODE PROACTIF**

de préparer une vidéoconférence par :

- le paramétrage et la configuration de la vidéoconférence ;
- le contrôle de l'état des salles trente minutes avant le commencement ;
- une assistance au démarrage en cas de problème.

Ce service est disponible en français et en anglais pour une couverture internationale.

Pour délivrer ce service, le métier de concierge a été créé. Pour agir vite, sous la pression, et pour guider l'utilisateur, des qualités humaines sont nécessaires et sont mêmes plus importantes que les compétences techniques. ■

FRANÇOIS FERVEUR • OPERATIONAL MARKETING
 MANAGER FOR MANAGED SERVICES

Accompagner les entreprises dans leur politique de Sécurité



Nombre d'entreprises considèrent la Sécurité trop consommatrice de ressources humaines et matérielles.

La Sécurité n'est pas qu'une question d'équipements de protection. C'est aussi une méthodologie d'élaboration d'une politique de Sécurité, ainsi que sa mise en œuvre. Le plan d'accompagnement que Telindus propose aux entreprises couvre ces deux volets.

Nombre d'entreprises considèrent que la Sécurité est trop consommatrice de ressources humaines et matérielles. Pour les sensibiliser à ces problèmes et les aider à définir une véritable politique de Sécurité, puis à l'appliquer, Telindus propose un programme d'accompagnement. Le but est de renforcer la Sécurité du SI en mettant en place une véritable politique en ce domaine avec des processus structurants, pour maîtriser les coûts et tendre vers la certification ISO 27001.

Le plan d'accompagnement commence par une phase d'études et de conseils. « *La première chose à faire est de dresser un inventaire des ressources et un schéma de l'organisation de l'entreprise* », conseille Raymond Salerno, ingénieur d'affaires chez Telindus, spécialiste de l'infogérance. Il faut



également établir une liste des ressources prioritaires, tels que les serveurs de production. Or leur protection efficace passe par la connaissance de leurs points faibles. D'où la nécessité de déterminer les causes de vulnérabilité des équipements, notamment par le biais d'audits d'intrusion, et évaluer leur impact sur l'activité de l'entreprise.

ÉTABLIR UN BUDGET ET UN PLANNING

À partir de ces trois tâches, un plan de progrès est établi. Comme il est souvent impossible de tout faire en même temps, force est d'établir un planning, en fonction des priorités définies et des vulnérabilités détectées. Ce plan suppose un budget et un échéancier de réalisation. C'est de la responsabilité du DSI, assisté du RSSI

(Responsable de la Sécurité des Systèmes d'Information). Au final, un plan d'action est établi. Il précise en particulier les équipes concernées et, surtout, détermine une charte de la politique de sécurité de l'entreprise. Celle-ci se traduit notamment par la création de profils correspondants à différentes catégories d'employés (commerciaux, services financiers, direction...). Chaque profil a des droits spécifiques : accès uniquement à certaines ressources, voire certains jours à certaines heures, accès extérieurs pour les nomades.

La correction des failles passe par des mises à jour logicielles, parfois légères, mais également par des actions plus lourdes, comme une modification des architectures.

UNE SUPERVISION DE TOUS LES INSTANTS

La phase préparatoire du plan d'accompagnement achevée, il faut maintenant le mettre en œuvre : c'est l'exploitation. Elle consiste à superviser le système d'Information et à détecter les anomalies 24 heures sur 24 et 7 jours sur 7. Dans son SOC (Security Operation Center), Telindus utilise des outils SIEM, comme Sentinel ou RSA. Ces outils centralisent et corrént les logs (événements). C'est l'implémentation des règles par les experts de Telindus qui permet la corrélation entre des incidents apparemment anodins, mais qui, mis en perspective, peuvent révéler des attaques. Lors d'une attaque, les procédures prévues sont appliquées. En cas d'incident grave, elles peuvent conduire à couper totalement un flux jusqu'à la correction totale de la cause. Telindus effectue également les changements matériels (par exemple passage à une nouvelle version logicielle d'un équipement de Sécurité), mais également humains (mise à jour des profils, création de comptes pour les nouveaux venus et fermeture des comptes de ceux qui quittent l'entreprise...). Des tableaux de bord d'activité et un rapport « météo » de la Sécurité du SI sont proposés périodiquement au client. « *Il peut ainsi vérifier que le niveau de risque est conforme à la politique de Sécurité de l'entreprise* », conclut Raymond Salerno ■

Les exigences des nouveaux Data Centers, une infrastructure adaptée !

Les entreprises font face à de nombreux challenges au niveau de l'hébergement des applications informatiques, des données et de leur infrastructure logicielle et matérielle sous-jacente, appelée Data Center ou centre de données. Tirillées entre des exigences de performance vitales pour leur activité et des contraintes en termes de dépenses et d'investissements, elles se tournent le plus souvent vers des solutions privilégiant mutualisation et industrialisation. Les Architectures orientées services (SOA) – la virtualisation, le cloud computing et les applications en mode SaaS – sont de plus en plus envisagées comme autant d'alternatives que les entreprises doivent considérer avec attention.

Les organisations font face à des contextes et enjeux variés qui ont ou auront un impact plus ou moins direct sur leurs approches de l'évolution de leur Data Center, en particulier :

- **Economiques** : diminution des coûts grâce au recours à la virtualisation, entre autres, et à la consolidation des centres de données, contraction des budgets d'exploitation informatique et meilleure maîtrise de ces coûts dans un contexte économique incertain ;
- **Accueillant plusieurs générations de technologies**, la plupart des exploitants de centres de données sont confrontés à certaines limites : capacité de refroidissement, puissance électrique disponible, prépondérance des coûts de l'énergie consommée. Leurs centres conçus dans les années 1980 méritent d'être reconsidérés. A cela, deux raisons essentielles : infrastructures (béton, électricité, refroidissement) anciennes, voire obsolètes, et difficulté d'accueil des machines de nouvelles générations ;



Une des caractéristiques premières du Data Center : fournir un service performant

- **D'amélioration de la performance des environnements informatiques** afin de mieux tenir les montées en charge (événement, opération promotionnelle...);
- **De développement de l'activité** : augmentation du volume de données à stocker et à sauvegarder, adaptation des environnements informatiques aux évolutions de l'entreprise ;
- **D'administration simplifiée et de gestion plus efficace des environnements informatiques** reposant de plus en plus sur des technologies pour lesquelles l'organisation des équipes informatiques doit être revue. Les experts qui géraient seuls leur silo technologique vont nécessairement devoir faire des efforts pour apprendre à travailler ensemble ;
- **D'exigences de continuité de service** imposées par les instances réglementaires et les clients.

EFFICACITÉ, PERFORMANCE

Une des caractéristiques premières demandées au Data Center est de fournir aux utilisateurs et aux administrateurs un service performant. Le but premier recherché est en effet de permettre un accès rapide aux données, pour un confort d'utilisation maximal. Le volume de données présentes dans ces centres et le nombre élevé de connexions clients engendrent naturellement des trafics énormes sur le réseau sur ces points précis. Un support efficace de ces flux nécessite l'utilisation de liens à capacité élevée et donc d'équipements actifs (commutateurs, routeurs, firewalls, etc.) capables de supporter ces débits importants.

L'évolution des technologies et des normes IEEE permet aujourd'hui d'atteindre des débits de 10 Gigabits par seconde ; ce débit, largement suffisant le plus souvent pour la connectivité de serveurs, trouve désormais ses limites dans le contexte de centralisation des données et des Data Centers de nouvelle génération.

L'avènement des serveurs de type Lame, par exemple, nécessite des connexions réseaux très performantes : alors que, traditionnellement, chaque serveur dispose d'une connectivité réseau, dans le cas de

La consommation électrique : un paramètre primordial dans le choix des équipements du Data Center

serveurs Lame, la connectivité réseau permet d'irriguer un ensemble de Lames, d'où des besoins de débits bien supérieurs.

Cette contrainte a engendré l'apparition de sociétés proposant des équipements avec interfaces de type 40 Gb/s Ethernet, destinés aux Data Centers (et aux opérateurs).

Ces technologies, aujourd'hui relativement confidentielles, devraient se développer plus largement avec la ratification de normes IEEE qui permettront de garantir l'interopérabilité des équipements et la pérennité de ces technologies. Cette norme en cours d'élaboration sera dénommée P802.3ab et permettra d'atteindre non seulement les 40 Gb/s mais également les 100 Gb/s !

Alors que le 40 GbE devrait se développer très rapidement dans les centres de données, l'envol du marché des interfaces 100 GbE est plutôt attendu en 2013.

EFFICACITÉ ÉNERGIQUE DANS LES DATA CENTERS

La consommation électrique est désormais un paramètre primordial de choix des équipements dans les Data Centers.

Trois raisons principales :

- **le manque généralisé de puissance électrique sur ces centres.**

Le rapport espace occupé/capacité de calcul devenant de plus en plus petit (compacité des équipements, technologie Lame...), les salles informatiques ne sont plus dimensionnées en terme de capacité électrique. La consommation des équipements est une des réponses à ce problème ;

- **le coût de l'énergie.** La facture électrique d'une direction informatique correspond en moyenne à 30 % de son budget ! Ce poste de dépenses est donc particulièrement surveillé ;

- **l'impact écologique.** La réduction de la consommation électrique s'inscrit également dans le cadre d'une démarche « Green IT »

Les équipements réseau ne dérogent pas à la règle, et la consommation électrique devient un des critères des

choix de ces équipements, à plus forte raison dans les projets de centres de données.

Les constructeurs peuvent agir sur différents éléments de leur matériel pour réduire cette consommation :

- **les caractéristiques des processeurs.** Certaines solutions techniques permettent de réduire leur besoin ;

- **le refroidissement** actif (ventilateur) ou passif, variateurs de vitesse de rotation du ventilateur en fonction de la température, etc ;

- **le bloc d'alimentation.** Un bloc au rendement élevé permet de réduire les gaspillages d'électricité ;

- **le logiciel.** Implémentation de fonctionnalités telles que la « condamnation » des ports réseaux non utilisés.

Impact
écologique

Inscrit dans
une démarche
« Green IT »





Rationaliser et diminuer fortement les coûts de gestion et d'administration des fermes de serveurs

LA FLEXIBILITÉ DES DATA CENTERS

Le taux de croissance du stockage et la demande en infrastructures de stockage s'intensifient malgré un contexte économique encore incertain. Les départements informatiques doivent batailler pour maîtriser cette croissance exponentielle. Leurs budgets d'investissement restent limités, rendant difficile l'acquisition de nouvelles technologies. Ils vont devoir définir les priorités de leurs investissements dans une logique de réduction et de maîtrise des coûts. La virtualisation est un facteur clé du Data Center dynamique et présente de nombreux avantages, ainsi que de nouveaux défis. La consommation d'énergie globale va diminuer tout en variant énormément. Nous verrons moins de serveurs dans le Data Center, mais chacun d'eux sera plus crucial et nécessitera plus que jamais davantage de ressources de stockage. Les applications peuvent être rétribuées dynamiquement à la demande et l'infrastructure devra être en mesure de faire de même. L'encombrement du Data Center sera réduit, mais l'efficacité globale pourra encore évoluer. Bonne nouvelle : il existe des moyens pratiques et abordables de relever ces défis et d'améliorer par la même occasion l'efficacité du Data Center.



Un accès rapide aux données pour un confort d'utilisation maximal

L'augmentation des données à stocker : une des raisons d'évolution du Data Center

Alors qu'un nombre croissant de charges de travail est virtualisé sur des processeurs multicœurs et que les bandes passantes réseau augmentent pour atteindre jusqu'à 8 Gbps sur l'interface FC et jusqu'à 10 Gbps sur le réseau Ethernet, la pression sur l'infrastructure de stockage de base se renforce, tant en termes de capacité que de performance. Il est important que l'infrastructure de stockage qui sous-tend l'environnement virtualisé puisse évoluer de manière flexible selon les besoins de performance et de capacité. Un tel système de stockage permettant d'ajouter plus de puissance de traitement, de ports d'accès, de caches et de baies de disques pour une meilleure performance grâce à l'utilisation d'accès massivement parallèles, permet de répondre aux exigences les plus hautes des virtualisations de serveurs d'envergure.



Nous nous attendons à une hausse continue de demande en systèmes de stockage intégrant l'amélioration des performances associée à l'optimisation des capacités. Ces systèmes pourront répondre à la demande croissante en matière de réseaux et processeurs plus rapides et en systèmes d'exploitation virtuels comme vSphere et Hyper V. Toujours dans cette même logique de généralisation de la virtualisation, les solutions adressent les principales problématiques des Data Centers de trois manières.

1 • Une rationalisation de l'infrastructure physique des fermes de serveur. L'infrastructure est plus légère, donc elle permet de réduire la consommation électrique et d'accélérer les déploiements. Elle apporte aussi des économies significatives sur les éléments de raccordement des fermes de serveurs aux différents réseaux du Data Center (LAN et SAN). Exemple : permettre des déploiements de serveurs en quelques heures au lieu de quelques semaines. La convergence Ethernet dans le Data Center (FCoE*, voir encadré).

L'informatique se tourne vers un modèle d'infrastructure réseau dynamique qui recourt largement à des serveurs exploitant de nombreuses machines virtuelles et qui utilise des liaisons à bande passante élevée pour communiquer avec le stockage virtuel et les réseaux virtuels.

Cette technologie réduit :

- les dépenses d'investissement grâce à une utilisation accrue des serveurs, du stockage, du réseau et des infrastructures convergentes (ce qui signifie moins de câblage et une consolidation du matériel de type HBA et NIC) ;
- les coûts d'exploitation par une meilleure utilisation de l'espace des Data Centers ;
- la consommation d'énergie.

L'adoption au niveau du serveur avec une interface de commutation FCoE sera la première évolution puisque les tarifs des CNA et des infrastructures 10 Gbps diminuent. Nous nous attendons à ce que





La virtualisation : un facteur clé du Data Center dynamique

l'adoption au niveau du stockage se répande, de nouvelles normes métier étant établies afin de permettre la création de chemins multiples et une décongestion du réseau. Nous observons également un énorme investissement dans l'infrastructure Fibre Channel (FC) qui va évoluer vers un débit allant jusqu'à 8 Gbps.

2• Une virtualisation plus poussée et plus contrôlée des environnements de production. Différentes technologies réseau ou système sont mises en œuvre pour permettre d'exécuter plus de machines virtuelles par unité de traitement. Exemple : permettre de tripler le nombre de machines virtuelles supportées pour une consommation électrique constante (exemple concret).

Rationaliser et diminuer fortement les coûts de gestion et d'administration des fermes de serveurs. Ces coûts n'ont fait qu'augmenter ces dernières années et la virtualisation quand elle est mal contrôlée ne fait qu'empirer les choses. Du fait de l'intégration des différentes fonctions de gestion de l'environnement serveurs dans un système unique et cohérent.

3• La gestion d'une infrastructure de stockage des données nécessite un personnel à plein-temps, qualifié et coûteux, ceci n'est plus compatible avec le métier des entreprises qui doivent se concentrer sur leur cœur business. Les ressources internes auparavant affectées à ces tâches courantes ne le sont plus. Désormais au sein des départements informatiques les nouvelles applications ou le reporting de la performance SAN sont pris en charge par des services managés.

L'évolution de cette demande correspond tout à fait au besoin d'avoir une architecture IT optimisée 24 heures sur 24 et 7 jours sur 7. Ainsi les clients peuvent concentrer leurs collaborateurs sur des activités à valeur ajoutée.

La sécurité
 ● ● ● ● ● ● ● ● ● ●
 un enjeu fort
 pour le Data
 Center
 virtualisé



LA SÉCURITÉ DANS LA VIRTUALISATION

La problématique de la sécurité dans les systèmes virtualisés génère actuellement des débats assez intenses, et c'est encore pour beaucoup d'entreprises un frein à l'adoption de la virtualisation. Une étude récente du Gartner (« Addressing the Most Common Security Risks in Data Center Virtualization Projects ») indique même que d'ici à 2012, 60 % des serveurs virtualisés seront moins sécurisés que les serveurs physiques qu'ils remplacent. Face à ce constat alarmiste, il convient d'analyser d'où peut provenir le manque de sécurité, car la véritable question est de savoir si cette tendance peut être inversée. Dans ce sens, le Gartner indique dans cette même étude que ce chiffre devrait tomber à 30 % d'ici à 2015. Tout n'est donc pas perdu et il y a beaucoup de choses à faire pour renforcer la sécurité des systèmes existants et définir de nouvelles architectures plus robustes.

Nous allons donc voir quels sont les points autour desquels la sécurité dans les systèmes virtualisés s'articule :

• Le système

Tout d'abord, à la différence d'une machine physique, une machine virtuelle est gérée par une surcouche logicielle de bas niveau appelée hyperviseur. C'est cet hyperviseur qui va cadencer et ordonner l'utilisation des ressources hardware pour chaque machine virtuelle. Comme tout logiciel, celui-ci peut comporter des vulnérabilités et on comprend aisément quel rapport à la sécurité il peut avoir : c'est lui qui va gérer le niveau d'étanchéité entre les machines par rapport à l'utilisation du processeur ou de la mémoire, par exemple. Si cet hyperviseur ne comporte pas de mécanismes de protection, on peut imaginer qu'une machine virtuelle comportant un système ou un logiciel mal développés, voire même compromis par un virus ou un ver, puisse consommer toutes les ressources et ainsi occasionner l'indisponibilité des autres machines virtuelles. Ces problématiques sont

maintenant identifiées par les éditeurs de solutions de virtualisation et sont intégrées dans les versions récentes ou futures (à court terme). Par ailleurs, la tendance actuelle est à l'allègement de cette couche hyperviseur pour la rendre la plus « fine » possible.

• Les flux réseaux

La particularité d'un système virtualisé est qu'il est possible de faire circuler des flux réseaux entre les machines virtuelles. Tout comme les accès au hardware, la couche réseau est gérée par l'hyperviseur (de manière native).

Or, dans les entreprises, cet hyperviseur est en général géré et administré par les services « Systèmes » et non « Réseaux ». En dehors des problématiques de responsabilité, un administrateur système ne possède pas la vision globale des flux réseaux de l'entreprise. Autre point crucial, les architectes serveurs classiques font appel à des briques de sécurité externes, la visibilité et le contrôle des flux sont assez bien maîtrisés. Or, avec l'avènement de la virtualisation, les flux internes échappent à cette visibilité et à ce contrôle.

Pour répondre à ce besoin, les éditeurs de solutions de virtualisation intègrent, via des partenaires acteurs de la sécurité des réseaux, des surcouches logicielles (API) positionnées, de la même manière que



Les équipes de sécurité ne sont pas toujours impliquées dans les projets



l'hyperviseur, en frontal – et non juste une VM parmi les autres – de toutes les virtuelles machines. Certains constructeurs proposent même, en plus du contrôle des flux, la possibilité d'organiser l'administration en fonction des rôles des différentes équipes intervenant sur le système.

• La conception

Ce point est essentiel à toute architecture de système virtualisé. Malheureusement, les équipes de sécurité ne sont pas toujours impliquées dans les projets car on a tendance à croire à tort que passer d'un serveur physique à un serveur virtuel n'impacte pas la sécurité. De plus, la tentation peut être grande de rassembler sur une machine physique des machines virtuelles ayant des niveaux de sécurité proches, mais différents.

LA CONTINUITÉ DE SERVICE

La disponibilité et la continuité de services sont de plus en plus au centre des préoccupations. La notion de PRA (Plan de Reprise d'Activité) s'efface progressivement au profit du PCA (Plan de Continuité d'Activité) car les organisations veulent tendre vers une disponibilité maximale de leur architecture. Les protocoles et mécanismes employés au niveau du réseau afin d'apporter de la redondance fonctionnent en tandem avec les technologies de virtualisation qui permettent de reconstruire ou déplacer rapidement un service perdu ou en maintenance. Le nouveau challenge des architectures est donc de pouvoir supporter le déplacement des machines virtuelles au sein de l'infrastructure de l'entreprise, tout en garantissant le même niveau de service et de sécurité.



Le Data Center évolue vers un modèle 100 % virtualisé

DEMAIN

« La virtualisation de l'infrastructure réseau, serveur et de stockage entraîne une transformation radicale du Data Center d'aujourd'hui. »

Le Data Center évolue vers un modèle 100 % virtualisé.

Ce concept constituera la fondation du cloud computing et permettra aux entreprises de souscrire à des services informatiques à la demande (ITaaS, IT as a Service). Dans ce scénario, l'informatique deviendra une ressource qui s'adaptera aux besoins de l'entreprise. Ces clouds privés ou publics permettront de déplacer les données et les applications entre eux.

Plus que jamais, il est important d'adopter une approche de type « architecture unifiée ». ■

RÉGIS BÉZIAT • DIRECTEUR DE LA BU STORAGE VIRTUALIZATION SOLUTIONS

ERIC GLACE • CONSULTANT MANAGER DATACENTER

Pourquoi la technologie FCoE ?

Le principe du FCoE (FiberChannel over Ethernet) est de transporter des données de type Fiber Channel dans des trames ethernet. Ce mécanisme permet d'atteindre les débits du protocole Ethernet, dont le débit maximum est à ce jour de 10 Gbps (40 Gbps et 100 Gbps à venir).



Les communications reposent toujours sur des données Fiber Channel (contrairement à l'iSCSI qui utilise TCP/IP) ; leur encapsulation dans des trames Ethernet permet de limiter les overheads et reste une manipulation peu gourmande en ressources CPU.

L'Ethernet utilisé dans le cadre du FCoE est une version spécifique, extrêmement proche de l'Ethernet, que l'on connaît dans le monde du réseau, mais légèrement modifiée afin d'être pertinente dans ce contexte (pas de perte de paquets, par exemple). Cette version est appelée DCE (Data Center Ethernet).

Le but final du DCE est de pouvoir transporter différents types de trafic utilisés à ce jour dans les Data Centers via des médias et des matériels actifs communs (matrices ethernet). L'avantage évident est de pouvoir remplacer toutes les interfaces spécialisées par un seul type d'interface pouvant gérer les deux trafics. Ces interfaces, appelées CNAs, (Converged Network Adapters), sont connectées aux commutateurs et aux directeurs de réseaux de stockage et proposent des débits de 10 Gbps.

Sécuriser le déménagement des Data Centers

Le déménagement d'un centre d'hébergement ou sa relocalisation présentent un risque important de perturbation des activités essentielles de l'entreprise et/ou de perte de données, qui peut gravement endommager sa production et porter atteinte à sa réputation.



Les difficultés propres au projet complexe de déménagement des Data Centers ne peuvent pas être réglées par la seule mise en place d'une équipe IT pluridisciplinaire dédiée, agissant comme maîtrise d'œuvre du Plan de Relocalisation IT (PRIT). C'est dans ce contexte que Christophe Genet, Directeur de la Production de Personal Finance, filiale de la BNP Paribas, a fait appel à la BU Conseil Telindus pour sécuriser la relocalisation d'environ 850 serveurs dans deux nouveaux centres d'hébergement.

LE BILAN D'IMPACT SUR LES ACTIVITÉS (BIA)

Sécuriser le service rendu par le SI et anticiper les impacts sur la production métier – dont les partenaires et les filiales à l'international – sont les objectifs permanents du BIA.

Comme représentant de la maîtrise d'ouvrage, par sa vision globale des enjeux métier, le consultant Telindus apprécie la criticité des serveurs, l'impact de leur indisponibilité sur l'activité commerciale, et apporte à la MOE l'éclairage métier sur les actions de maîtrise IT ou d'organisation nécessaire au bon

déroulement de l'opération.

Il s'agit de déterminer avec les Maîtrises d'Ouvrage (MOA) ou leurs représentants informatiques, quels sont les serveurs critiques dont l'arrêt non planifié a un impact direct sur les activités de production avec, pour conséquence, des pertes financières importantes ou une détérioration de l'image de l'entreprise vis-à-vis de ses clients, de ses partenaires ainsi qu'en interne.

Cette étape capitale commence dès les étapes techniques de préparation de l'inventaire des équipements à déplacer jusqu'à la validation de bon fonctionnement après relocalisation.

LE PLAN DE CONTINUITÉ DE SERVICE IT (PCSIT)

Le contrôle des risques passe par la mise en place d'actions de maîtrise :

- utilisation de la résilience entre serveurs ;
- application de prérequis techniques avant relocalisation ;
- sauvegardes des systèmes d'exploitation et des données utilisateurs ;
- disponibilité de matériel de rechange pour

les équipements en fin de vie ;

- extension des garanties fournisseurs pendant le déménagement ;
- implication du management en cas de difficulté et de crise ;
- procédure de retour arrière et rétablissement du service initial dans le cas où la résolution des problèmes ne peut s'effectuer sur le site de destination dans un délai raisonnable ;
- validation par les maîtrises d'ouvrage du niveau de service après son retour à disposition.

La communication se fait partie intégrante de la maîtrise des risques. Il faut donner aux utilisateurs de la visibilité sur le projet de déménagement et s'appuyer sur le centre d'appel pour les prévenir d'éventuelles interruptions de service.

LE PLAN DE RELOCALISATION INFORMATIQUE ET TÉLÉCOMMUNICATIONS (PRIT)

Le PRIT se construit par étapes successives dans les ateliers de préparation avec toutes les équipes de maîtrise d'œuvre (MOE), à partir d'un inventaire technique précis des systèmes d'exploitation, des applications, du plan d'adressage réseau, des bases de données et de l'implantation physique des matériels.

LE BILAN APRÈS RELOCALISATION (BAR)

Le BAR permet de capitaliser sur le retour d'expérience dans un objectif d'amélioration continu de la démarche. ■

MARC MOSCOVITCH • CONSULTANT SENIOR



Le PRIT

• • • • •
*Le Plan de
 Relocalisation
 Informatique et
 Télécom se prépare
 avec toutes
 les équipes de
 maîtrise d'œuvre*

Le financement au service de votre **Opex**



Faire évoluer une partie du matériel pendant la location

Au moment où les premiers signes de reprise économique apparaissent, l'investissement dans une infrastructure moderne devient un élément clé pour améliorer la compétitivité de l'entreprise.

Les investissements en matériels, logiciels et prestations représentent un poste lourd pour une entreprise, dans un contexte où, de plus en plus, la logique d'utilisation prime sur la problématique de possession et où le manque de visibilité à long terme impose aux entreprises une flexibilité importante, y compris dans ces investissements. Au-delà du contrat de location financière, il existe aujourd'hui des contrats de location simple, dite location opérationnelle ou operating lease, dont les principes sont régis par les normes internationales IAS17 (IFRS) qui, financièrement, impactent différemment les comptes de l'entreprise.

REVUE DE DÉTAIL

A la différence d'un contrat de location financière, la location opérationnelle est un contrat de location de longue durée d'un bien sans que l'entreprise ne dispose de la faculté de l'acquérir après une période d'utilisation donnée. Le client a la possibilité de faire évoluer tout ou partie du matériel pendant la durée de la location, selon des conditions préétablies ou avec des clauses de renégociation. Ce mode de contrat répond au besoin de déléguer la gestion d'un parc, plus ou moins

QUATRES CRITÈRES POUR UN CONTRAT CLASSIFIÉ EN LOCATION OPÉRATIONNELLE

- à l'issue de la location, le contrat ne transfère pas la propriété du bien loué au locataire ;
- le locataire ne possède pas d'option d'achat à un prix trop favorable qui rendrait l'exercice de cette option quasi certain ;
- la durée de location est sensiblement inférieure à la durée de vie économique du bien ;
- à la signature du contrat, la valeur actualisée des loyers est sensiblement inférieure à la « juste valeur » du bien loué.

avancée selon les services proposés par le loueur. Une entreprise peut également recourir à ce type de contrat via le rachat de son parc informatique : le loueur l'acquiert alors au prix convenu, et met en place une location évolutive avec un loyer pour chaque élément. Une solution qui peut être utilisée pour augmenter sa trésorerie et lisser ses dépenses.

TRAITEMENT COMPTABLE

Sur le plan comptable, le traitement s'apparente à une location simple. Les loyers dans ce cas sont considérés comme une charge opérationnelle à comptabiliser au compte de résultats en tant que charges d'exploitation. Cela implique donc une diminution de l'Ebitda mais cela n'a pas d'impact sur les Capex. Au démarrage du contrat, le traitement comptable et fiscal des opérations de location doit être soumis pour validation au commissaire aux comptes de l'entreprise locataire, qui doit apprécier la réalité de la transaction.

Telindus est à même aujourd'hui d'accompagner ses clients dans cette approche et de leur proposer, avec ses partenaires, des solutions de financement adaptées à leurs besoins. ■
STÉPHANE LORAS • DIRECTEUR ADMINISTRATIF ET FINANCIER



Le CG 57 met le très haut débit au service des Mosellans



Permettre à tous les collégiens mosellans d'accéder dans les mêmes conditions à la connaissance : c'est l'un des principaux objectifs du projet réseau CG57, lancé par le Conseil Général et dont Telindus est l'intégrateur. L'entreprise est également chargée de la formation des équipes techniques. Le raccordement de 130 sites a commencé en début d'année et il devrait être achevé à la fin de l'année, soit avec une avance de plus de deux ans sur le calendrier initial. Une course contre la montre que Telindus est en passe de remporter.

UN RÉSEAU HERTZIEN ÉGALEMENT EN PROJET

Bien que très maillé, le réseau haut débit ne dessert pas toutes les zones du département.

Le Conseil Général étudie, avec Telindus, un prolongement du réseau par voie hertzienne pour desservir une quarantaine d'autres sites.

La technologie retenue est celle du français Nomotech, qui a développé le WifiMax. Elle combine les avantages de Wifi, tels que la simplicité, et ceux d'une technologie robuste d'opérateur. En particulier, elle intègre les couches de Sécurité (802.11i) et de qualité de service (802.11e). Gros atout de WifiMax, il se déploie en mode Mesh : chaque antenne qui dessert des abonnés sert également de relais aux antennes voisines. Ce qui limite d'autant l'infrastructure filaire de raccordement des antennes les plus éloignées. Un avantage en zones rurales.

Quatre-vingt-quatorze collèges et une trentaine de sites du Conseil Général de la Moselle (services administratifs, centres médico-sociaux, sites culturels, bibliothèques, unités territoriales routières, etc.) accèdent au réseau via une liaison optique à haut débit (200 Mbit/s, autorisant des pointes à 1 Gigabit/s). À la clé du projet, l'égalité d'accès à la communication et à la connaissance des administrés du département de la Moselle.

« Auparavant, certains collèges en zone rurale étaient pénalisés. Il n'y avait pas d'égalité des chances, » note Rachid Dekiouk, adjoint au DSI du Conseil Général de la Moselle. En effet, chaque site était raccordé via des liens ADSL, dont le débit variait de quelques centaines de Kbit/s à quelques Mbit/s, en fonction de leur éloignement du centre de rattachement (NRA). Désormais, « le réseau du CG57 s'appuie sur l'infrastructure optique du RHD ou Réseau haut débit de la Moselle, dont l'exploitation a été concédée à une délégation de service public (DSP) confiée à Moselle Télécom, explique Thomas Rémond, ingénieur commercial chez Telindus, mais le Conseil Général s'est réservé deux paires de brins optiques pour son usage propre. Ce sont elles qui supportent le réseau CG57 ».

Le reste de l'infrastructure optique est exploité par Moselle Télécom, qui la loue à d'autres opérateurs. Ceux-ci fournissent les services haut débit aux entreprises du département. À l'issue d'un appel d'offre en 2009, Telindus a été retenu pour bâtir le réseau GC57 en partenariat avec Transmode et en assurer la maintenance ; son exploitation était prise en charge par la DSI du Conseil Général.

PLATE-FORME PÉDAGOGIQUE CENTRALISÉE ET BÉNÉFICES IMMÉDIATS

L'arrivée de ces autoroutes de la communication a profondément bouleversé le mode de fonctionnement des collèges. Avant, chaque établissement était autonome. Il gérait lui-même ses serveurs abritant les documents pédagogiques électroniques. De plus, les postes de travail étaient des PC traditionnels, qu'il fallait renouveler quasiment tous les trois ans. Un professeur, nommé

correspondant informatique, faisait le lien avec la DSI.

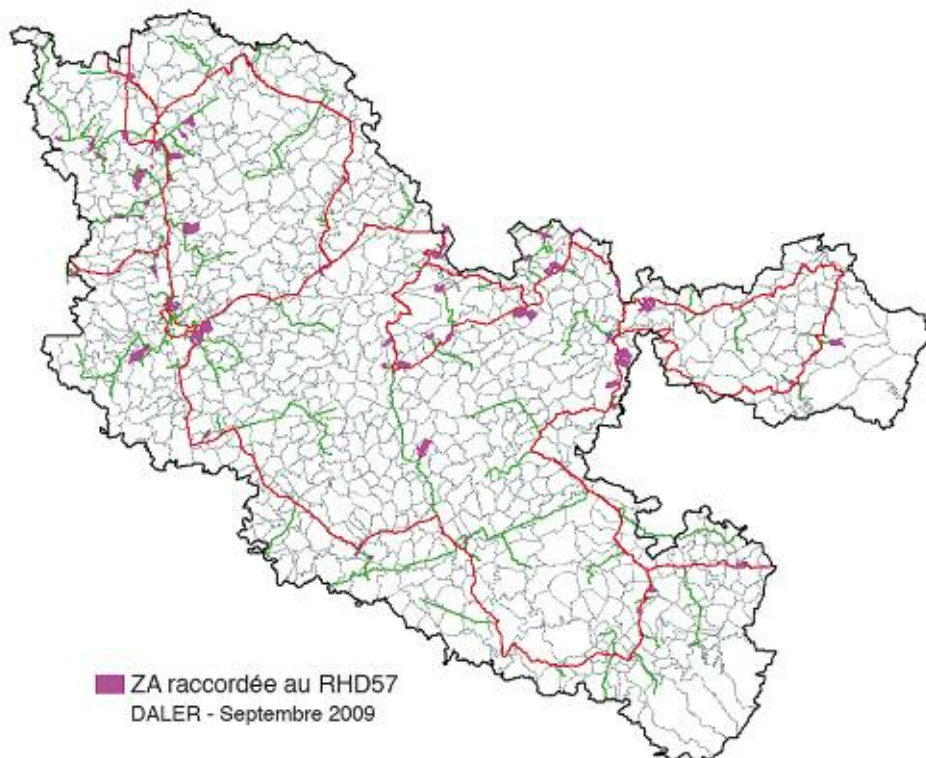
Grâce à ce réseau haut débit, tous les documents sont désormais centralisés sur une plate-forme pédagogique abritée dans la salle blanche (centre névralgique du stockage de données) de la DSI du Conseil Général. Quel que soit l'établissement,

les élèves accèdent via le réseau à cette plate-forme. Leurs postes de travail sont des terminaux légers (Citrix). Résultat, il n'y a plus de serveurs à acheter, à installer dans les établissements et à maintenir. Plus de PC à renouveler régulièrement, puisqu'ils ont été remplacés par des terminaux Citrix. Plus d'abonnements DSL pour chaque collège ou bâtiment départemental. À noter que les services départementaux sont également passés depuis 2003, au client léger Citrix pour quasiment toutes les applications (financières, messagerie, subventions, bureautique). « Grâce à cette nouvelle architecture, nous prévoyons un retour sur investissement en deux ans et demi », souligne Rachid Dekiouk.

UNE RÉACTIVITÉ IMPRESSIONNANTE

Pour parer à la défaillance d'un serveur de la salle blanche, des procédures de Sécurité spécifiques ont été mises en place : une seconde salle blanche, située sur ●●●

A
la clé
du projet :
l'égalité d'accès
pour tous



LE RÉSEAU MOSELLAN

L'infrastructure haut débit sur laquelle s'appuie le réseau du Conseil Général de la Moselle compte 1 350 kilomètres de fibre. Il traverse plus de 360 communes et comporte 305 points de raccordement. Des interconnexions sont en cours avec le Luxembourg, la Sarre, la Meurthe-et-Moselle et le Bas-Rhin.

« UNE EXPERTISE REMARQUABLE »

« Dans la réponse de Telindus à l'appel d'offre, la proposition technique nous a tout de suite convaincus. Et nous n'avons pas été déçus, les équipes de Telindus ont rempli leur contrat. Elles ont fait preuve d'une expertise remarquable lors de la phase d'ingénierie optique. Il n'était pas évident de concevoir notre réseau, irriguant tout le département, avec seulement deux paires de fibres. Telindus a respecté le calendrier et les équipes ont raccordé une dizaine de collèges par semaine. Cela comprend l'activation des fibres, mais également, la connectique, la configuration et le paramétrage des équipements de réseau, comme les routeurs. »

●●● un autre site et reliée à la première par une fibre optique, travaille en partage de charge avec la première. En cas de défaillance de l'une des salles blanches, la seconde est immédiatement prête à prendre le relais auprès des utilisateurs qui y étaient connectés. Changement technique, mais également administratif : si les serveurs dépendent du Conseil Général, les programmes pédagogiques sont du ressort de l'Éducation nationale.

Ce sont donc les services nancéens de cette administration qui les gèrent, sur les serveurs à Metz. Aujourd'hui tout fonctionne parfaitement, grâce aux ajustements faits sur les matériels en début de projet. « Les équipes de Telindus ont rapidement détecté les problèmes, se souvient Rachid Dekiouk. Nous avons été impressionnés par leur réactivité et leur efficacité. » ■

UNE TECHNOLOGIE ÉCONOMIQUE

Le réseau haut débit utilise la technologie de multiplexage de longueur d'onde (WDM ou Wavelength Division Multiplexing) de la société Transmode. Chaque fibre transporte plusieurs longueurs d'onde (couleur). Chacune d'elles véhicule des informations. Tout le problème réside dans « l'espacement » entre ces longueurs d'onde afin qu'il n'y ait pas d'interférence optique. Les opérateurs utilisent le DWDM (Dense WDM) dans lequel les longueurs d'onde sont très rapprochées. D'où une forte capacité, mais aussi des lasers très chers. Le réseau mosellan utilise le CWDM (Coarse WDM), c'est-à-dire un espacement plus large entre les différentes longueurs d'onde. Le nombre de multiplexage est plus petit (16 couleurs au lieu de 80 et plus), et les équipements sont moins chers et moins gourmands en énergie tout en pouvant évoluer facilement vers du DWDM.

L'Équipe Telindus en charge du projet

- Sébastien Mutel, Directeur de projet
- Angélique Di Bartolo, Coordinateur technique
- Hervé Reimel, Ingénieur réalisation



Rachid Dekiouk, adjoint du DSI du Conseil Général de la Moselle.

Aix-en-Provence renforce sa sécurité sur son réseau Internet

La ville souhaite faire évoluer la zone d'accès Internet de son réseau informatique privé. L'objectif est d'assurer une meilleure disponibilité de cet accès tout en renforçant la sécurité.

JOSÉ MELGAR,
Responsable réseau de la Ville d'Aix-en-Provence :
« La solution doit présenter des capacités de traitement de 10 Go avec un contrôle des applications véhiculées et sécurisées au travers de politiques de sécurité. Elle possédera donc un minimum de dix interfaces Go et permettra ainsi de bien séparer et différencier les règles gérant les flux d'Internet/DMZ des flux DMZ/Intranet. L'équipement de sécurité, situé au cœur de l'infrastructure, permettra aussi de cloisonner les flux entre différents VLAN afin d'appliquer des politiques d'accès aux ressources internes. »



© Wolf Meusel

Ville d'art et de culture, fondée par les Romains en 123 av. J.-C., Aix-en-Provence marie un passé historique à un futur de haute technologie.

La communauté du Pays d'Aix abrite à Cadarache le projet ITER (Réacteur expérimental thermonucléaire international), destiné à vérifier la fusion nucléaire en tant que nouvelle source d'énergie. Cette sous-préfecture est également un carrefour de transports de voyageurs avec sa gare TGV ainsi qu'un axe économique grâce aux technopôles de l'Arbois et de Rousset. Ses nombreuses universités (lettres, droit, économie, sciences politiques, arts et métiers, beaux-arts) jouissent d'une grande réputation. Grâce à une communication centrée sur les nouvelles technologies, la Ville bénéficie d'un réseau Internet de haut de gamme. Récemment, elle a décidé d'optimiser son accès Internet déjà équipé d'une sécurité qui réunit firewall, VPN et système IDP. Ces équipements protègent les Systèmes d'Information et les bases de données, aussi bien pour les entreprises que pour les opérateurs, contre les vers, redoutables chevaux de Troie, les logiciels espions et autres menaces émergentes. Aujourd'hui, la municipalité veut aller plus loin.

« Nous avons choisi de booster la sécurité sur la zone d'accès Internet, c'est-à-dire le périmètre situé entre le

réseau informatique privé de la mairie et le réseau public Internet » explique José Melgar, Responsable réseau de la ville. « Cette zone a pour mission de sécuriser les échanges des flux autorisés tout en bloquant les tentatives d'intrusion et les attaques au sens large ».

DES BÉNÉFICES IMMÉDIATS

Pour renforcer sa sécurité, Aix-en-Provence a choisi Telindus qui est son partenaire depuis une dizaine d'années et qui connaît parfaitement les équipements déjà installés.

« Telindus s'est appuyée sur la solution Palo Alto explique Michel Ellul, Ingénieur Avant-Vente chez Telindus. Ce choix a été fait car il fallait être capable d'une part, d'avoir une visibilité des applications pour en assurer la sécurité et d'autre part, de tenir la charge de 10 Go tout en appliquant des règles de firewalling. »

L'architecture est proposée en mode Bridge pour tous les flux à destination d'Internet et en mode Routage pour tous les flux Inter VLAN, caractéristique plutôt rare dans les standards présents sur le marché. Le rapport qualité/prix, compte tenu des performances du boîtier a aussi été un critère déterminant dans le choix de la solution.

« Telindus a une très bonne connaissance de l'architecture réseaux de la ville, et donc la possibilité de nous proposer la solution la plus adéquate » ajoute

José Melgar.

Pour la Ville, les bénéfices sont immédiats. Désormais, la solution mise en place permet les filtrages sans pertes de performances, une sécurisation des communications et segmentation des flux de communications (TOiP, vidéo, administration réseaux), une sécurisation des interconnexions avec les partenaires de la mairie (Communauté du Pays d'Aix...) et elle donne aussi la possibilité de créer des filtres très fins (application, utilisateurs). Telindus a accompagné son projet d'une offre de service d'intégration sur site ainsi que d'un contrat de maintenance cinq jours sur sept, de 8 heures à 18 heures. ■

Pour la ville, les bénéfices sont immédiats

Projet ambitieux sur la Sécurité du réseau d'un **groupe industriel**

Grâce aux nouveaux firewalls sortis récemment sur le marché, la Sécurité des flux est largement simplifiée. Un groupe industriel français, avec l'aide de Telindus, en a profité pour optimiser la Sécurité d'un périmètre de son réseau.

Un groupe industriel français désirait se doter d'un outil capable de l'aider à consolider plusieurs étages de la Sécurité de son réseau. L'objectif à atteindre était d'aménager et de sécuriser une zone interne accessible à un public extérieur. Le but était de pouvoir autoriser ou refuser des accès à son réseau, selon les utilisateurs, tout en effectuant un filtrage à partir des fonctions de certaines applications. Pour répondre à la demande de son client, Telindus l'a orienté sur les firewalls multifonctions de son partenaire Palo Alto, une solution simple à intégrer et à déployer. Palo Alto propose une appliance et des logiciels d'administration très bien packagés sous forme d'images avec un très bon support technique.

SIMPLIFIER À L'EXTRÊME

Plutôt que d'établir des règles qui paraissent d'un autre temps, la solution permet tout simplement de contrôler quelles applications et quels utilisateurs sont autorisés à transiter par le firewall. Pour cela, la solution est capable de reconnaître un nombre très important d'applications. Plutôt que d'avoir à gérer des adresses IP et des ports correspondants à des applications, la solution embarque une base de connaissance sans cesse enrichie. De ce fait, elle est capable instantanément de reconnaître les applications au sein des flux entrants et sortants d'un périmètre.

Par ailleurs, la solution identifie les utilisateurs plutôt que l'adresse interne des postes de travail, ce qui est beaucoup plus explicite dans le monitoring et les rapports d'activité. L'interconnexion avec les annuaires est mise en œuvre ce qui permet pour chaque flux d'identifier l'utilisateur associé. Les administrateurs disposent donc d'une bonne visibilité de l'activité qui se déroule au sein du réseau en temps réel et/ou a posteriori.

Pour le client, les règles de Sécurité sont grandement simplifiées par rapport à ce qui existait auparavant. Ce nouvel outil ajoute des fonctionnalités tant au niveau de la reconnaissance des utilisateurs que des

applications. On peut désormais connecter des annuaires d'entreprise avec des règles de Sécurité pare-feu, ce qui se faisait auparavant au sein des proxy, et qui est traité maintenant au sein des firewalls.

La solution a rendu possible des règles d'autorisation de passage entre des groupes d'identifiant. Des fonctionnalités techniques ont ensuite été rajoutées, notamment des systèmes d'intrusion et des anti-virus qui permettent de corréler le niveau d'alerte avec les règles qui sont dans les pare-feu. Ce qui rend la solution économiquement intéressante.

Pour le responsable informatique du groupe Industriel, « La solution Palo Alto pourrait se comparer à un couteau suisse avec ses nombreuses options disponibles. La fonction de visibilité constitue souvent le point d'entrée dans les réflexions menées actuellement dans de nombreux projets de Sécurité que nous conduisons. Le produit proposé par Telindus s'inscrit dans cette stratégie et permet dès le début de procéder à la mise en œuvre de cette solution dans un mode non intrusif sur les infrastructures existantes, ce qui représente un plus ».

En complément, les autres fonctions du produit permettent de participer activement aux politiques de Sécurité et offrent une visibilité et un contrôle permanent sur les applications, les utilisateurs et les contenus de flux au sein du réseau de l'entreprise. ■

La solution proposée pourrait se comparer à un couteau suisse



« Le gros avantage de Telindus, qui est un intégrateur sérieux, c'est d'être parti sur ce produit-là dès qu'il s'est présenté sur le marché. Telindus nous a prêté du matériel, a répondu à nos attentes, s'est mis à notre dimension. Nous avons exigé que les équipes de Telindus répondent aux questions auxquelles on ne sait pas répondre, qu'elles soient réactives, commercialement et technologiquement, du jour au lendemain. »

A PROPOS

Grâce à ses multifonctions, le firewall redevient l'élément clé d'une architecture de Sécurité permettant de contrôler les applications, avec plus de granularité, en fonction des utilisateurs et du contenu •

Check Point sécurise également les environnements virtualisés



La virtualisation se généralise. Les analystes estiment qu'en 2012, elle concernera la moitié de la charge informatique des entreprises.

Mais elle ouvre des brèches dans les dispositifs de protection. Check Point, acteur majeur dans le domaine de la Sécurité, propose la solution VPN-1 Virtual Edition (VE). Aux fonctions traditionnelles du pare-feu, elle ajoute la protection entre machines virtuelles.

Toute médaille a son revers. Si la virtualisation permet d'optimiser l'usage des ressources physiques des serveurs, notamment dans les Data Centers, elle introduit également de nouveaux risques sécuritaires. « Aux dangers suscités par les attaques venant de l'extérieur ou de l'intérieur de l'entreprise, s'ajoute un risque d'étanchéité insuffisante entre machines virtuelles sur un même serveur physique, signale Philippe Rondel, directeur technique de Check-Point France. *Check Point répond à cette problématique avec son produit VPN-1 VE* ».

MUTUALISER LES RESSOURCES PHYSIQUES

Avant l'ère de la virtualisation, dans l'entreprise, les différents environnements (finances, R&D, marketing, direction...) étaient physiques et chacun possédait ses serveurs et son réseau. Il en était de même chez les hébergeurs. Chaque client disposait de ses propres ressources. Il était donc relativement facile d'isoler les environnements et les clients. Satisfaisante sur le papier, la solution était coûteuse, car les serveurs tournaient rarement au maximum de leur capacité. De plus, lorsqu'une nouvelle application entrait en service, il fallait acheter un autre serveur.

Avec la virtualisation, il devient facile de mutualiser les ressources physiques, puisqu'il y a décorrélation entre la machine physique et les applications qui fonctionnent dessus par le biais d'une couche de virtualisation (hyperviseur). VMware est à la fois le pionnier et le champion de cette technologie, détenant environ 80 % du marché. Grâce à ce découplage entre matériel et logiciel, il est possible de créer sur un même serveur physique des serveurs virtuels, chacun correspondant, par exemple, à un environnement à l'intérieur d'une entreprise ou à un client chez les hébergeurs.

Profitant de cette possibilité, nombre d'entreprises ont remis à plat leur infrastructure informatique, englobant l'ensemble de leurs ressources dans un vaste réseau IP, afin de réduire les coûts. Même démarche chez les hébergeurs, surtout depuis l'arrivée du phénomène de Cloud Computing, très gourmand en ressources physiques. En même temps, les entreprises, comme les hébergeurs, ont attendu de retrouver, dans cette nouvelle organisation, les mêmes critères de Sécurité. Or, la segmentation physique des architectures précédentes a disparu. Il fallait donc la remplacer par une solution logicielle. « C'est là qu'intervient VPN-1 VE de Check Point », précise Philippe Rondel.

EN FRONTAL DES SERVEURS

Sur chaque interface virtuelle entre un serveur virtuel et l'hyperviseur s'active comme un agent ●●●

« Les systèmes virtuels font partie du réseau et doivent être protégés avec le même niveau de sécurisation que celui fourni par des appliances physiques. Le VPN-1 VE prouve l'engagement de Check Point à protéger les entreprises lorsque de nouvelles technologies arrivent sur le réseau. L'architecture ouverte de Check Point fournit aux entreprises une sécurisation sans pareille, gérée de manière centralisée, autant pour les réseaux physiques que pour les environnements virtuels. »



PHILIPPE RONDEL
directeur technique
de Check-Point France

- logiciel, qui agit comme une sorte de pare-feu. D'ordinaire, un pare-feu est un boîtier installé à l'entrée du réseau, qui filtre les accès et les sorties, détecte les attaques et les bloque. On appelle cela : la défense périphérique. Placé à l'intérieur du réseau, en frontal des serveurs, VPN-1 VE assure une défense rapprochée. Ces agents communiquent avec une passerelle, qui sert de relais avec le Smart Center (un par serveur physique), qui contient les règles de Sécurité définies par l'entreprise et une boîte à outils pour les modifier le cas échéant. Ces agents logiciels agissent comme de véritables pare-feu, bloquant les attaques internes et externes (dans le cas où il n'y a pas déjà de pare-feu de périphérique). Ils garantissent également l'étanchéité entre les serveurs virtuels. Par exemple lorsqu'un serveur virtuel veut prendre l'adresse IP d'un autre serveur. La solution VPN-1 VE fonctionne avec ou sans pare-feu périphérique. Une entreprise peut, par exemple, placer cette solution dans son Data Center, qui regroupe tous ses serveurs, et se contenter de pare-feu classiques dans ses agences, qui ne contiennent pas de serveurs virtualisés.

UNE PROTECTION DYNAMIQUE

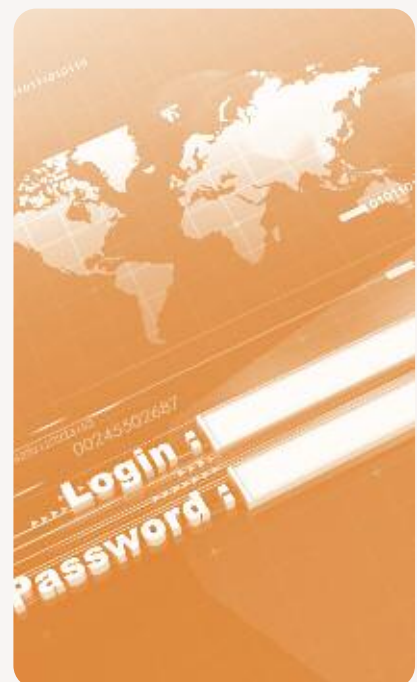
Voilà pour l'aspect statique. Mais il faut également prendre en compte la dimension dynamique. En effet, l'un des atouts maîtres de virtualisation est de permettre de s'adapter, en temps réel, aux besoins de l'utilisateur. Par exemple, chez un hébergeur abritant une boutique de vente en ligne, un afflux de requêtes peut submerger les ressources existantes, suite au lancement d'une nouvelle ligne de produits. Avec la virtualisation, il est facile d'ajouter rapidement autant de serveurs virtuels que de besoins. Une souplesse impossible avec des serveurs physiques. Il fallait, soit choisir un très gros serveur sous-utilisé la plupart du temps, soit



La passerelle de sécurité de Check Point Virtual Edition offre les fonctions d'un pare-feu classique (pare-feu, passerelle VPN, sonde IPS et antivirus).

installer un second serveur physique – ce qui nécessite une préparation – puis le démonter lorsque le trafic revient à la normale. Dans l'entreprise, la souplesse de virtualisation peut être utilisée, par exemple, en cas de plantage d'un serveur, pour faire redémarrer l'application sur un autre serveur. Même en dépit de ces changements, la Sécurité doit être garantie. L'une des forces de VPN-1 VE est de s'adapter dynamiquement à l'infrastructure. Ainsi, lorsque un serveur virtuel est créé le Smart Center du serveur physique concerné génère automatiquement un agent sur l'interface virtuelle de la nouvelle machine virtuelle. Ainsi, la Sécurité est assurée.

« Une solution qui répond à une forte tendance du marché puisque, selon le cabinet Gartner Group, en 2012, la moitié de la charge informatique des entreprises sera virtualisée, révèle Philippe Rondel. En outre, toujours selon le Gartner Group, 60 % des DSI jugent qu'il est difficile d'assurer la Sécurité des machines virtuelles. » ■



F5 accompagne les Data Centers de nouvelle génération



L'ARX GÈRE SIMPLEMENT LE STOCKAGE NAS

Avec la ligne de produits ARX, F5 simplifie le stockage en mode NAS (Network Attached Storage). Ainsi, pour gérer automatiquement plusieurs NAS, il suffit de définir les règles sur l'ARX. Par exemple, d'indiquer que les fichiers les plus anciens se trouvent sur tel NAS et les plus récents sur tel autre (ou encore par types de fichiers). Pour l'utilisateur, ils sont tous accessibles de la même manière. Mais s'il ouvre un « vieux » fichier, celui-ci redevient d'actualité, et l'ARX le déplace automatiquement sur le NAS correspondant, sans aucune intervention de l'utilisateur. Une forme de virtualisation du stockage.



Fruit de l'acquisition, mi-2007, d'Acopia par F5, le boîtier ARX gère dynamiquement les serveurs de stockage NAS.

Dans les entreprises comme chez les opérateurs, l'heure est à la virtualisation et à la consolidation des services. Au cœur des flux applicatifs traversant le Data Center, on trouve désormais le BIG-IP de F5, en version boîtier ou logicielle, qui facilite ces évolutions.

La nouvelle génération de Data Centers se caractérise par la recherche d'une plus grande adaptabilité et par la réduction des coûts, observe Vincent Lavergne, directeur technique Europe du Sud de F5, partenaire de Telindus depuis huit ans. L'un des outils pour y parvenir est la virtualisation, qui permet la mutualisation dynamique des ressources physiques. F5 accompagne cette mutation avec la nouvelle version du BIG-IP Local Traffic Manager, qui offre une consolidation des services. S'ajoute une version purement logicielle, le Traffic Local Manager Virtual Edition, qui fonctionne sur VMware. »

SEGMENTATION LOGIQUE DE L'ÉQUILIBREUR DE CHARGE

Traditionnellement, les Data Centers étaient organisés en « silos ». À chacun d'eux correspondait un environnement physique, par exemple applicatif dans une grande entreprise ou pour un client chez un hébergeur. Chaque silo disposait de son réseau et de sa Sécurité (commutateur, pare-feu, équilibreur de charge entre serveurs). La virtualisation des serveurs de fichiers et d'applications a permis d'optimiser l'usage des machines physiques. Il restait à en faire autant pour la partie amont. « Il est désormais possible de segmenter logiquement un Big-IP en plusieurs équilibreurs de charge, chacun correspondant à un contexte client ou applicatif, et isolés les uns des autres, afin de garantir la Sécurité et la confidentialité des flux », précise Vincent Lavergne. D'où une réduction significative du nombre d'équipements. Une possibilité offerte sur la plupart des boîtiers jusqu'au Viprion, le châssis à lames, qui découple la puissance de l'ADC (Application Delivery Controller), le fer de lance de l'offre de F5.

UNE VERSION LOGICIELLE DU BIG-IP

F5 va un cran plus loin dans la virtualisation, avec la Virtual Edition de son BIG-IP, qui s'affranchit d'un boîtier spécifique et fonctionne déjà sur couche VMware et bientôt également sur Hyper-V de Microsoft. D'où une optimisation des ressources dans le Data Center, puisque le BIG-IP s'installe sur un serveur virtualisé, remplissant par ailleurs d'autres fonctions (serveur web et



Le Viprion est un châssis à lames qui permet de découpler la puissance de calcul du BIG-IP.

d'applications). Cette Virtual Edition intéresse en premier lieu les opérateurs de services (ceux du Cloud Computing), qui gèrent de multiples environnements, mais aussi l'ensemble des clients et partenaires F5 qui pourront reproduire dans un laboratoire les environnements F5/VMware. Ils n'ont plus besoin d'affecter à chacun d'eux une machine physique. Aujourd'hui, cette version ne propose que l'équilibrage de charge, alors que la version boîtier cumule celles de haute disponibilité (équilibrage de charge), de Sécurité (Authentification-Autorisation, pare-feu applicatif...) et d'optimisation (notamment des flux Web). « F5 travaille à porter ces deux dernières tâches en Virtual Edition » confirme Vincent Lavergne.

CONNAÎTRE À TOUT MOMENT LES SERVEURS DISPONIBLES

L'une des possibilités offertes par la virtualisation consiste à provisionner, dynamiquement, des ressources supplémentaires, selon le trafic. Par exemple, d'ajouter automatiquement des serveurs web, en fonction de la demande (par exemple lors d'une période de soldes sur un site de e-commerce). F5 travaille à l'orchestration grâce à l'intégration du dialogue entre le BIG-IP, qui répartit la charge entre ces serveurs et la couche de virtualisation (VMware et Hyper-V de Microsoft) et qui décide de l'ajout ou du retrait de serveurs virtuels. « Le BIG-IP sait ainsi à tout moment quels sont les serveurs disponibles, sans qu'il soit nécessaire de le configurer manuellement », souligne Vincent Lavergne. Une fonction qui peut également servir en cas de sinistre du Data Center principal, en aiguillant automatiquement les requêtes vers le site de backup. ■

SUCCESS WAY



 together
with



Réussir 2015

Quels choix structurants en 2010 pour
faire face aux futurs défis technologiques ?

A Paris le 14 octobre, Rennes le 19 octobre,
Bordeaux le 9 novembre, Toulouse le 16 novembre et
Strasbourg le 23 novembre
Inscription sur www.telindus.fr

Une occasion unique de
rencontrer Telindus et les
meilleurs partenaires du marché
réunis à votre porte ...
autour de **conférences, de
débats et d'échanges informels**
... **d'avis d'experts et de retours
d'expériences** ..

Une journée «**à la carte**» pour
être en ordre de marche face
à la déferlante des nouvelles
technologies.



Inscription sur www.telindus.fr

Pour toute information complémentaire,
contactez Caroline Seguret au 01 69 18 98 30
ou par mail teltechdays@telindus.fr

TELINDUS EN FRANCE

AGENCE ILE-DE-FRANCE

10, avenue de Norvège - BP 742
91962 LES ULIS Cedex
Tél. : 01 69 18 32 32 - Fax : 01 69 59 28 50

AGENCE BORDEAUX

Parc Cadéra Sud - 36, avenue Ariane
33700 MERIGNAC
Tél. : 05 56 13 46 46 - Fax : 05 56 13 46. 47

AGENCE GRENOBLE

Les Jardins d'Entreprise de Maupertuis
Bâtiment Le Sarde - BP 112
38243 MEYLAN
Tél. : 04 76 90 34 34 - Fax : 04 76 41 12 02

AGENCE LILLE

Parc Club des Prés - 1, rue Denis Papin
59650 VILLENEUVE D'ASCQ
Tél. : 03 20 61 79 61 - Fax : 03 20 61 79 60

AGENCE LYON

Rue de Lombardie
69150 DECINES CHARPIEU
Tél. : 04 72 78 04 78 - Fax : 04 78 01 60 64

AGENCE MARSEILLE

Immeuble le Grand Bleu
29, boulevard Gay Lussac
13323 MARSEILLE CEDEX 14
Tél. : 04 91 63 63 63 - Fax : 04 91 63 75 20

AGENCE RENNES

Forum de la Rocade - 40 rue du Bignon
35510 CESSON SEVIGNE
Tél. : 02 99 53 29 53 - Fax : 02 99 53 88 03

AGENCE SOPHIA ANTIPOLIS

2229, route des Crêtes
06560 SOPHIA ANTIPOLIS
Tél. : 04 88 57 75 14 - Fax : 04 88 57 75 20

AGENCE STRASBOURG

Espace Plein Sud - 12, rue des Hérons
67960 ENTZHEIM
Tél. : 03 90 29 88 30 - Fax : 03 88 68 67 57

AGENCE TOULOUSE

Z.A.C de Basso Cambo
46 avenue du Général de Croutte - BP 63727
31037 TOULOUSE Cedex 1
Tél. : 05 34 40 91 20 - Fax : 05 34 40 91 21

www.telindus.fr

