

Documentation relative à l'infrastructure d'hébergement des produits de **SALLEMÉDIA**

Introduction

Le présent document a pour objet d'offrir un aperçu de l'infrastructure d'hébergement utilisée pour notre éventail de produits Web hébergés et de fournir des renseignements logistiques. Les installations d'hébergement ont pour propriétaire-exploitant ViaWest, fournisseur suprarégional fiable et expérimenté de solutions d'hébergement géré en colocation et de continuité des opérations.

Le présent document traite des sujets suivants :

- Structure d'hébergement (redondance et équilibrage de charge)
- Redondance réseau et matérielle
- Sauvegarde et récupération
- Systèmes d'alimentation sans coupure (UPS)
- Politique de sécurité informatique
- Surveillance (alertes et journal de bord)
- Systèmes

Aperçu des installations d'hébergement

Les centres de données conçus par ViaWest sont dotés de multiples entrées de fibres optiques et de circuits afin d'assurer la redondance de la couche physique. Ces points d'entrée répondent, et sont parfois supérieurs, aux normes de Bellcore en ce qui a trait aux entrées multiples et à la séparation physique.

Routeurs multicœurs

- Les centres de données de ViaWest sont dotés de routeurs multicœurs, ce qui permet à ViaWest d'étendre son réseau sans pratiquement aucune incidence sur la clientèle.

Multicommutateurs satellite

- La défaillance de la couche d'agrégation est atténuée par des dispositifs redondants eux aussi directement interconnectés et chacun relié à un routeur de cœur. ViaWest offre également des connexions redondantes au moyen de commutateurs de distribution uniques.

Redondance logique

- Les routeurs d'infrastructure de ViaWest exécutent un protocole OSPF (Open Shortest Path First) afin de trouver le meilleur chemin d'un emplacement à l'autre. Si un circuit ou un dispositif tombe en panne pour quelque raison que ce soit, chaque routeur calcule automatiquement le nouveau « meilleur chemin » pour acheminer le trafic afin de minimiser toute éventuelle incidence sur la clientèle.

Diversité physique

- ViaWest a quatre centres de données dans la région des Rocheuses, chacun offrant un niveau donné de redondance et de miroitage des opérations de l'ensemble des centres de données.

Redondance de réseau

- Les centres de données de ViaWest sont reliés au moyen d'une boucle en fibre optique IP sur SONET utilisant des circuits redondants de différents fournisseurs.

Sauvegarde et récupération

- Les services suivants de reprise en cas de sinistre sont fournis :
 1. **Stockage** – Les données sont régulièrement sauvegardées et les bandes sont transférées vers une chambre forte hors site résistant au feu; ainsi, en cas de sinistre à l'installation principale, une copie de sauvegarde pourra être récupérée dans un emplacement hors site.
 2. **Équilibrage de charge** – Les sites Web et les données sont gérés par au moins deux serveurs utilisant un équilibreur de charge pour acheminer le trafic entre des instances distinctes sur différents serveurs. Si un serveur éprouve un problème, la charge peut être transférée aux autres serveurs, sans pratiquement aucune interruption de service ou perte de données.
 3. **Mise en grappe** – De multiples serveurs sont utilisés au sein d'un unique réseau en grappe. Si un système fait défaut, les autres serveurs redistribueront la charge automatiquement, sans aucune incidence sur les services.

Maintien/Rétablissement des activités

- Tous les centres d'exploitation de réseau de ViaWest sont indépendants les uns des autres et sont en mesure d'assurer la surveillance et le maintien de l'ensemble des éléments du réseau et de l'infrastructure de ViaWest de façon autonome.
- S'il est nécessaire de récupérer des données pour reprendre les activités normales, des copies à distance de toutes les données critiques sont stockées en dehors du site et peuvent être utilisées pour la restauration des systèmes d'exploitation, des données de production, des banques de données, des configurations et d'autres fichiers au besoin.
- Les données critiques sont conservées en ligne dans différents emplacements et peuvent être récupérées par le truchement du réseau dans le but de restaurer des copies locales.

Systemes d'alimentation sans coupure (UPS)

- Dans chaque emplacement, de multiples systèmes d'alimentation sans coupure sont disponibles dans le but de fournir une alimentation redondante à la charge critique. Tous les emplacements ont au moins deux de ces systèmes déployés dans une configuration N+1, ainsi les clients peuvent demander que chacun des systèmes alimente leur équipement.
- Dans les installations de ViaWest, tous les câbles d'alimentation sont placés sous un faux-plancher et sont imperméables; ainsi, ils ne peuvent être endommagés par l'eau ou une inondation. En outre, des détecteurs d'eau placés sous le faux-plancher alerteront immédiatement le personnel sur place ou en dehors du site de la présence de liquide sous le plancher.

CVCA

- Chaque centre de données ViaWest est doté de plusieurs systèmes de chauffage, de ventilation et de climatisation d'air (CVCA) indépendants refroidis par condenseur/aéroréfrigération/refroidissement sec/glycol/eau destinés à minimiser le point de défaillance unique caractéristique des systèmes à refroidisseur.
- Tous les centres de données de ViaWest sont aménagés sur de faux-planchers et sont dotés d'appareils de traitement de l'air descendant pour un maximum de capacité de refroidissement. Dans les situations de charge critique, ces appareils introduisent de l'air froid au travers des perforations pratiquées dans les tuiles du faux-plancher et aspirent l'air chaud par les systèmes de filtration placés au-dessus des appareils de traitement de l'air.

Détection et extinction d'incendie

- Toutes les installations de ViaWest sont dotées de systèmes de détection d'incendie à deux zones et à deux alertes. Un système à deux zones atténue la possibilité d'alarme injustifiée grâce à l'installation de chaque détecteur dans une zone différente du voisin le plus proche.

Sécurité physique

- Une carte d'accès à photo sera remise à toute personne ayant un accès autorisé à une installation de ViaWest. Les formats des laissez-passer varient en fonction du niveau de sécurité qui y est associé. Chaque carte a un numéro de série individuel et chaque entrée dans l'installation est enregistrée électroniquement.

Surveillance (alertes et journal de bord)

- Le fonctionnement de chaque système environnemental critique est contrôlé individuellement. Si un système échoue au diagnostic interne, signale une erreur, ou est en dehors de sa plage d'exploitation nominale, ce symptôme est immédiatement relayé par connexion hors bande à un poste de contrôle éloigné qui se chargera de dépêcher immédiatement un technicien sur les lieux où le problème est survenu.
 1. **Alertes** – Un avis est émis électroniquement chaque fois que le centre d'exploitation de réseau détecte une interruption de service (HTTP, MySQL, SMTP, etc.).
 2. **Alertes de secours** – Un courriel est automatiquement envoyé dès qu'une erreur est détectée lors des sauvegardes de données nocturnes.
 3. **Notifications d'événements d'applications** - Nos applications reposent sur plusieurs processus chronométrés qui transmettent des renseignements diagnostiques régulièrement concernant chacune de nos applications Web. Par exemple, si un modèle de site progresse à l'étape de la réalisation, ou en cas d'erreur d'inscription sur une liste de messagerie.

Infrastructure et architecture des serveurs

Coupe-feu

- ViaWest a recours à la meilleure technologie de coupe-feu sur le marché pour protéger l'ensemble des applications et des données. Le trafic externe et interne est contrôlé constamment par les administrateurs de la sécurité informatique de la société. Tous les systèmes administratifs sont protégés par le protocole SSL (Secure Socket Layer) standard.

Configuration du coupe-feu :

- NetScreen : gérée par les experts en sécurité informatique de ViaWest, notre installation a deux coupe-feu configurés en mode haute disponibilité. Ce mode permet la perte complète d'un coupe-feu et le réacheminement imperceptible du trafic vers le pare-feu auxiliaire.

Routeurs, commutateurs et serveurs

- Tous les routeurs, commutateurs et serveurs sont placés dans des endroits sécurisés. L'accès à ces lieux est réservé à un nombre restreint de personnes. Une topologie du réseau est établie et tenue à jour suivant les nouvelles affectations de matériel et de ports.

Détection et prévention des intrusions dans un réseau

- ViaWest s'associe au plus grand spécialiste de la sécurité Internet en mettant en œuvre un outil de sécurité nous permettant de sécuriser nos systèmes en surveillant tout signe au sein du réseau ou des serveurs indiquant d'éventuelles attaques. Le coupe-feu de ViaWest et les configurations de réseaux de données sont maintenus à des niveaux de sécurité stricts. Chaque port de réseau externe est configuré selon des lignes directrices internes et fait l'objet d'une surveillance systématique.

Déni de service et attaques par déni de service

- La stratégie de ViaWest en vue de combattre les dénis de services et attaques par déni de service repose sur une approche à multiples facettes comprenant la détection, le traçage et l'isolement des événements de malveillance informatique. La politique de ViaWest consiste à agir avant que d'autres clients ne subissent de conséquences. Le centre d'exploitation de réseau possède le matériel nécessaire pour contrôler toutes les alertes, ce qui permet d'apporter les correctifs nécessaires et d'atténuer les répercussions d'une attaque.
- ViaWest a des relations de travail et des contacts de sécurité directs avec tous les principaux fournisseurs de réseau.
- ViaWest surveille les communautés et les listes de diffusion en lien avec la sécurité et les équipes de réaction en informatique et y prend une part active.

Infrastructure et architecture de solutions Web

Toutes les solutions Web reposent sur notre plateforme SPIN exclusive. Le présent document traite des sujets suivants :

- Exigences relatives à la base de données
- Caractéristiques logicielles (configuration de la plateforme SPIN)
- Mise en antémémoire

Exigences relatives à la base de données

- Un site/une application reposant sur la plateforme SPIN exclusive a des exigences très simples en ce qui a trait à la base de données :
 - Une seule base de données MySQL
 - Un seul utilisateur MySQL avec les privilèges INSÉRER, METTRE À JOUR, SÉLECTIONNER ET SUPPRIMER pour cette base de données
- La plateforme SPIN a été mise à l'essai à ce jour sur les versions de MySQL jusqu'à MySQL 5. Les exigences actuelles du système sont les suivantes :
 - RedHat Enterprise ES 3 (bien que n'importe quel système Linux devrait suffire)
 - Apache 2.0 (ou encore 1.3)
 - MySQL 4.1.8 – standard

Configuration

- Nous utilisons les serveurs Web conjointement avec un dispositif redondant d'équilibrage des charges.
- Les serveurs de bases de données exploitent MySQL 5 Cluster, une base de données transactionnelle en temps réel conçue pour assurer un accès rapide permanent aux données dans des conditions à haut débit. MySQL Cluster repose sur une architecture de type « shared nothing » (rien partagé) qui ne requiert aucune architecture additionnelle.
- Les serveurs sont spécialisés, ce qui élimine les contraintes liées aux services partagés en raison de l'accaparement de l'unité centrale/mémoire vive. Notre utilisation moyenne actuelle s'établit entre 15 % et 30 % de cette capacité.

Serveur de base de données

- Serveur spécialisé DB-EdgeServer 200 Red Hat Linux ES
- Processeur Intel Quad Core Xeon
- License de serveur de système d'exploitation Red Hat Linux ES
- Surveillance sur place tous les jours, 24 heures par jour, avec notification d'événements et ouverture de billets
- Gestion de matériel sur place tous les jours, 24 heures par jour
- Matériel local de réserve

Serveur d'application Web

- Serveur spécialisé Web AppServer 300 Red Hat Linux ES
- Processeur Intel Dual Core Xeon
- License de serveur de système d'exploitation Red Hat Linux ES
- Surveillance sur place tous les jours, 24 heures par jour, avec notification d'événements et ouverture de billets
- Gestion de matériel sur place tous les jours, 24 heures par jour

- Matériel local de réserve

Mise en antémémoire

- Nos produits Web utilisent une mise en antémémoire côté serveur de pages HTML entières. L'avantage consiste à réduire le nombre de requêtes redondantes dans la base de données, ce qui peut accroître considérablement la performance d'un site achalandé. Quand une page est éditée dans Site Manager, toute la mémoire cache du site est purgée. Nous n'avons connaissance d'aucune limitation relative à notre mise en antémémoire, ni de limitations de mémoire ou de disque.
- Le répertoire cache d'un site a suffisamment d'espace disque pour prendre en charge l'écriture de toutes les pages d'un site à ce répertoire, mais ceci devrait être négligeable. Une page est « publiée » (en temps réel) lorsque la page en question a été éditée avec le logiciel Site Manager et qu'on a cliqué sur « Sauvegarde ».
- Une page est prise en charge par le répertoire cache côté serveur lorsque le premier utilisateur accède à cette page.