Dossier d'architecture technique

Whatsup au service de la performance

Qwirk

|  |  |  |
| --- | --- | --- |
| **Diffusion interne** | | **Code** |
| **Commercial** |  | I |
| **Avant-vente** |  | I |
| **Chef de Projet** |  | ACR |
| **Consultant(s)** | Equipe projet | C |

|  |  |  |
| --- | --- | --- |
| **Diffusion client** | | **Code** |
| **DSI** |  | AC |
| **Chef de Projet** |  | I |
|  |  |  |

***Code : A****pprobation,* ***I****nformation, a****C****tion, a****R****chivage*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Informations qualité** | | | | | |
| **Date de sortie** | 11/12/2017 | **Numéro de la dernière page** | | | 21 |
| **Rédigé par** |  | | | | |
| **Vérifié par** |  | | **Visa** |  | |
| **Approuvé par** |  | | **Visa** |  | |

| **Version** | **Date** | **Auteur** | **Nature des modifications** |
| --- | --- | --- | --- |
| 0.1 |  |  | Création du document |
| 0.2 |  |  | Description des modules |

Table des matières

[1. Présentation 3](#_Toc446411714)

[2. Architecture générale 3](#_Toc446411715)

[2.1. Rappel du besoin 3](#_Toc446411716)

[2.2. Objectifs du projet 3](#_Toc446411717)

[2.3. Schéma de principe d'architecture 4](#_Toc446411718)

[2.4. Serveurs d'infrastructure 4](#_Toc446411719)

[3. Architecture physique 5](#_Toc446411720)

[4. Architecture logique 7](#_Toc446411726)

[5. Services Cloud 14](#_Toc446411734)

[6. Sécurité 15](#_Toc446411737)

[7. Administration 17](#_Toc446411742)

[8. Annexes 20](#_Toc446411745)

[8.1. Schéma du workflow 20](#_Toc446411746)

# Présentation

Ce document constitue le Dossier d'Architecture Technique (DAT) concernant le projet d'intégration et de déploiement de l'infrastructure de haute disponibilité avec répartition de charge sur le site Web de l'entreprise Qwirk. Ce document a pour but de faire l'adéquation entre les besoins spécifiques de l'entreprise et la façon dont ceux-ci sont intégrés à l'infrastructure déployée. Ce document décrit l'ensemble du paramétrage que préconise **Nom de notre societe** pour l'intégration de cette infrastructure.

# Architecture générale

*Cette section définit le contexte du projet haute disponibilité*

## Rappel du besoin

*Ce chapitre présente le problème à résoudre, tel que nous l'avons perçu pour établir cette spécification*

## Objectifs du projet

## Schéma de principe d'architecture

*Voici le schéma d'architecture général de l'infrastructure mise en place*

## Serveurs d'infrastructure

|  |  |
| --- | --- |
| Type | Description |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Architecture physique

*Cette section définit l'architecture physique de la solution mise en place dans le cadre du projet haute disponibilité du site Qwirk*

## Equipement

Pour le site primaire, il est prévu de fournir un espace de stockage pour l'hébergement du site sur l'un de nos serveurs. Ce serveur ne sera pas dédié à ce projet.

Pour le site secondaire, nous utiliserons un PC sur lequel nous installerons une plateforme de virtualisation VMware Workstation.

*Site primaire*

|  |  |
| --- | --- |
| Composants | Descriptif |
| Carte mère | Asus Z99 deluxe |
| Processeur | Intel Core i7-5960x |
| Mémoire | 64GB DDR4 2400Mhz |
| Stockage | 1TB RAID1 |
| Connexion | FastEthernet |

*Site secondaire*

|  |  |
| --- | --- |
| Composants | Descriptif |
| Base | MSI Windows 10 Professionnel |
| Processeur | Intel I7 4720HQ CPU 2,6GHz |
| Mémoire | 16GB |
| Stockage | 1TB HDD + 128GB SSD |
| Connexion | FastEthernet |

*Caractéristiques techniques des équipements*

Cf. versions logicielles pour les caractéristiques sur les couches logicielles hôte (de 1er niveau).

## ESXi

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nom | ESX1 | ESX2 | ESX3 | ESX4 |
| Hyperviseur | ESXi | ESXi | VMware Workstation | VMware Workstation |
| Mémoire | 8GB | 8GB | 6,1GB | 6,1GB |
| Nombre de vCPU | 2 | 2 | 4 | 4 |
| Disque | 150GB (thin provision) | 150GB (thin provision) | 200GB (thin provision) | 200GB (thin provision) |
| Interface réseau | eth0 | eth0 | eth0 eth1 | eth0 eth1 |

*Caractéristiques techniques des hyperviseurs ESXi virtualisés*

*Caractéristiques techniques du vCenter sur site primaire*

|  |  |
| --- | --- |
| vCenter | Site primaire |
| Hyperviseur | ESXi |
| Mémoire | 8GB |
| Nombre de vCPU | 2 |
| Disque | 40GB |
| Interface réseau | eth0 |

Pour le site secondaire, on utilise le client vSphère version 6 pour administrer les serveurs.

## Load Balancer

*Caractéristiques techniques des load balancers*

|  |  |  |
| --- | --- | --- |
| Modèle ALOHA VA | Site primaire | Site secondaire |
| Nom | HAProxy1 | HAProxy2 |
| Hyperviseur | ESXi | VMware Workstation |
| Mémoire | 4GB | 4GB |
| Nombre de vCPU | 2 | 2 |
| Disque | 64MB | 64MB |
| Interface réseau | eth0 | eth0 |

## Serveurs Web

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Site primaire | | Site secondaire | |
| Nom | IIS1 | IIS2 | IIS3 | IIS4 |
| Hyperviseur | ESXi1 | ESXi2 | ESXi3 | ESXi4 |
| Mémoire | 8GB | 8GB | 4GB | 4GB |
| Nombre de vCPU | 2 | 2 | 4 | 4 |
| Disque | 50GB | 50GB | 105GB | 105GB |
| Interface réseau | eth0 | eth0 | eth0 | eth0 |

*Caractéristiques techniques des serveurs web IIS*

## Content Delivery Manager

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Site primaire | | Site secondaire | |
| Nom | CDN1 | CDN2 | CDN3 | CDN4 |
| Hyperviseur | ESXi1 | ESXi2 | ESXi3 | ESXi4 |
| Mémoire | 2GB | 2GB | 1GB | 1GB |
| Nombre de vCPU | 1 | 1 | 2 | 2 |
| Disque | 4GB | 4GB | 40GB | 40GB |
| Interface réseau | eth0 | eth0 | eth0 | eth0 |

*Caractéristiques techniques des CDN*

# Architecture logique

*Cette solution définit l'architecture logique de la solution mise en place dans le cadre du projet haute disponibilité du site Qwirk*

## Versions logicielles

*Ce chapitre présente les caractéristiques logicielles des équipements utilisés*

Les équipements sont installés avec les versions logicielles suivantes :

|  |  |  |
| --- | --- | --- |
| Service | Version | Site |
| Hyperviseur Type 1 | ESXi 6.0.0 Update 1 build 3029758 | primaire |
| Hyperviseur Type 2 | VMware Workstation 9 | secondaire |
| Serveur Web | IIS 8.0 | primaire / secondaire |
| CDN | Debian 8.2.0 | primaire |
| CDN | CentOS 7 | secondaire |
| vCenter Server | 6.0.0 Build 3018524 | primaire / secondaire |
| HAProxy | aloha 7.5.0 7530 (2015-11-10) | primaire / secondaire |

## Virtualisation

*Ce chapitre présente les caractéristiques des plateformes de virtualisation mises en place*

Nous mettons en place deux plateformes de virtualisation réparties sur deux sites physiquement séparés.

La première est de type 1, c'est-à-dire installée directement sur la couche matérielle du serveur. Le choix s'est porté sur l'ESX Server de VMware.

La seconde est de type 2, c'est-à-dire un logiciel qui s’installe et s’exécute sur un système d’exploitation déjà en place. Le choix s’est porté sur VMware Workstation.

La virtualisation a plusieurs avantage par rapport aux machines physiques :

* Elle permet la gestion de plusieurs systèmes d'exploitation.
* Elle facilite les migrations de données entre sites.
* Elle permet de répartir la charge sur plusieurs serveurs en fonction du trafic.

Sur chacune de ces plateformes, nous avons mis en place deux datacenters. Avoir 2 serveurs sur 2 sites permet donc une redondance de l'information, avec un risque de panne divisé par 2 x 2 = 4.

Sur chaque site physique, nous utiliserons des clusters pour basculer automatiquement d'un datacenter à l'autre.

Et pour basculer d'un site à l'autre en cas de perte de connexion sur un site, nous utiliserons une redirection DNS.

Nous verrons par la suite en détail les solutions utilisées.

**Capacités des machines virtuelles sous ESXi**

Les machines virtuelles s’exécutant sur ESXi présentent les caractéristiques suivantes :

* Les machines virtuelles peuvent prendre en charge jusqu’à 128 CPU virtuels.
* Les machines virtuelles peuvent prendre en charge jusqu’à 4 To de RAM.
* Le contrôleur xHCI prend en charge les périphériques USB 3.0.
* L’interface AHCI (Advanced Host Controller Interface) prend en charge jusqu’à 120 périphériques par machine virtuelle.
* La taille maximum d’un disque de machine virtuelle est de 62 To.
* La fonctionnalité de récupération d’espace de stockage de l’OS client rend au pool de stockage l’espace disque libéré au sein de l’OS client.
* La virtualisation du CPU est optimisée, grâce à la présentation d’un plus grand nombre d’informations sur l’architecture du CPU hôte aux machines virtuelles. Cette meilleure exposition du CPU permet de déboguer, d’affiner et de dépanner plus facilement les systèmes d’exploitation et les applications dans la machine virtuelle.
* L’efficacité du CPU est accrue par la fonctionnalité LRO (Large Receive Offload) qui regroupe les paquets TCP entrants en un paquet unique plus important.

**Capacités des machines virtuelles sous Workstation**

La plateforme de VMware Workstation prend en charge des configurations comprenant jusqu’à 16 vCPU, des disques de 8 To, 64 Go de RAM et 2 Go de RAM vidéo.

**Utilisation de vCenter Server**

 vCenter Server est le composant de gestion centralisé d’un datacenter virtuel vmware. Il joue le rôle d’administrateur des hôtes ESX/ESXi connectés au réseau, et des machines virtuelles présentes sur ces différents hôtes.

vCenter Server utilise un Système de Gestion de bases de données relationnelles de manière à stocker les informations relatives aux hôtes et configurations. Ici nous utilisons la version allegée du SGBDR Microsoft SQL Server 2005 Express packagée avec les fichiers d’installation de vCenter Server.

Ces composants supplémentaires sont installés sans notification lors de l'installation de vCenter Server :

* vCenter Inventory Service
* PostgreSQL
* vSphere Web Client
* vSphere ESXi Dump Collector
* VMware vSphere Syslog Collector
* Service VMware Syslog
* vSphere Auto Deploy

**Datastore**

Les datastores, ou banque de données, sont des conteneurs logiques qui masquent les caractéristiques propres à chaque périphérique de stockage. Elles sont caractérisées par une partition d’un volume formaté en VMFS. Les limitations suivantes doivent-être respectées :

* 1 banque de données = 1 seul système de fichiers.
* Jusqu’à 256 banques de données VMFS par système.
* 8 Banques de données NFS par système.

Une banque de données peut contenir les fichiers des machines virtuelles (disques, métadatas, …) et également des images ISO de disques (pour l’installation d’OS par exemple).

Ici nous créons un datastore par datacenter.

## HAProxy

*Ce chapitre présente la solution de clusterisation et load balancer utilisée*

**Load Balancer**

Cette solution, appelée Aloha dans la dernière version de son service Load Balancer, est basée sur un noyau Linux. Elle permet de répartir les connexions reçues d'un protocole sur plusieurs serveurs. Elle permet aussi de détecter l'indisponibilité d'un des serveurs. Elle peut être utilisée pour les applications utilisant TCP. HAProxy sait gérer plusieurs proxy à la fois, c'est un reverse-proxy très utilisé pour les sites Web, soit dans sa version opensource, soit dans sa version commerciale.

La solution a de nombreux avantages :

* elle peut tenir des charges très importantes comme plusieurs milliers de connexion par seconde,
* elle peut de gérer les pics de charge,
* elle assure la sécurité en ligne des applications les plus critiques,
* elle nécessite des ressources matérielles très faibles,
* elle permet une supervision permanente des serveurs
* elle possède une interface Web de configuration

Cette solution est de type actif/actif, c'est-à-dire qu'elle permet d'avoir les deux systèmes en fonctionnement en parallèle. Un seul des deux systèmes peut fonctionner en solo.

La solution se présente sous la forme d'une appliance virtuelle clef en main installable sur tout type d'hyperviseur. Ici nous l'installerons au niveau 1 de la virtualisation. Elle sera chargée de la gestion des 2 datacenters.

|  |  |
| --- | --- |
| Hostname | ALOHA1 |
| Version | aloha 7.5.0 |
| Firmware revision | 7530 (2015-11-10) |
| Model | albva |
| UUID | 4235F59394663EDCC77844991B4A626C |
| ETHID | 005056B575F6 |

**Licences**

Par défaut, l'appliance est fournie en version d'évaluation, limité à 10 connexions par secondes. Ce sera suffisant pour notre POC*.* La licence full sera nécessaire pour la mise en production.

**Firmware**

Pour connaître la version actuelle du firmware :

* Depuis la console, exécuter en tant que root : fgrep -i version /usr/share/factory/version
* Dans l'interface web, cliquer sur l'onglet "Setup". Au niveau de la section "Firmware"

L'upgrade de patchs se fait depuis l'interface Web sur l'onglet "Setup", section "Firmware". Il suffit de télécharger sur le site la dernière version du firmware et de l'importer dans la console. L'update se fait au prochain boot et nécessite donc une bascule sur l'autre site si celui-ci est actif. De la même façon il est possible de faire un rollback vers la version précédemment installée.

Les versions de firmware sont supportées pendant 3 ans après leur release. Il est possible de consulter les changelogs des releases ainsi que leur roadmap sur leur site.

**GUI**

HAProxy est construit comme tous les équipements réseau et fonctionne donc sur le même principe. Sa configuration est stockée à deux endroits :

* running configuration: celle stockée dans la RAM
* startup configuration: celle lue au redémarrage

NOTE : la version d’évaluation ne permet pas la sauvegarde sur la NVRAM.

Les changements de configuration sont appliqués à la *running* configuration et ne sont pas écrits dans la mémoire flash. Pour enregistrer les changements dans la flash :

* aller sur l'onglet "Setup"
* localiser la section "Local configuration"
* cliquer sur le bouton Inserting image...

## IIS

*Ce chapitre présente les caractéristiques des serveurs IIS mis en place*

Les caractéristiques logicielles sont les mêmes sur les 2 serveurs Web de chaque site.

**Windows 2012 R2 Standard**

Ces serveurs sont basés sur le système d’exploitation Windows Server 2012 R2 Standard 64 bits.  
**Windows Server 2012 R2** aide à créer, déployer et faire évoluer des applications et des sites Web rapidement. Il apporte la souplesse nécessaire pour déplacer les charges de travail entre des environnements locaux et le cloud. Ses points forts :

* Evolue pour exécuter les plus grandes charges de travail
* Options de récupération robustes afin de se protéger contre les pannes de service
* Une infracture sous-jacente simple
* Réduction des coût en exploitant le matériel standard

**IIS 8**

Le système d’exploitation Windows Server 2012 R2 Standard fournit une plateforme unifiée pour la publication de sites Web en intégrant les services Internet (IIS), ASP.NET et Windows Communication Foundation. IIS version 8.0 joue un rôle central dans l’intégration des technologies de plateforme Web.

Les caractéristiques principales d’IIS 8.0 sont les suivantes :

* Modèle d’extensibilité flexible pour une personnalisation de pointe
* Outils de diagnostic et de dépannage puissants
* Administration déléguée
* Sécurité accrue et surface d’attaque réduite grâce à la personnalisation
* Déploiement fidèle d’applications avec xcopy
* Gestion d’applications et d’intégrité intégrée pour les services WCF (Windows Communication Foundation)
* Outils d’administration améliorés

De par ces caractéristiques, IIS 8.0 est une plateforme unifiée qui fournit un modèle de développement et d’administration unique et cohérent pour les solutions Web.

## NGINX

*Ce chapitre présente les caractéristiques des reverse-proxies mis en place*

Les Content Delivery Network sont assurés par des serveurs Nginx, qu’ont appelle aussi dans ce cas des reverse proxy, ou serveur frontal.

Un CDN permet de stocker des ressources sur de multiples serveurs externes. Le but est de pouvoir fournir à chaque internaute les fichiers dont il a besoin de la manière la plus rapide possible. Pour cela, le CDN se base sur plusieurs éléments :

* Chaque fichier est présent sur plusieurs serveurs, permettant de réduire l’encombrement du site lors de pics de trafic.
* Les CDN sont équitablement répartis géographiquement, réduisant la distance serveur-ordinateur.
* Ces serveurs sont sans cookies, permettant de réduire le poids de chaque transfert en enlevant ces données inutiles pour les ressources statiques.
* Certains fichiers étant sur des serveurs différents, cela augmente le nombre de connexion simultanées autorisées entre l’ordinateur et les fichiers à télécharger.

Ces serveurs sont installés sur une base linux, Debian pour le site primaire et CentOS pour le site secondaire. La configuration des Nginx est la même sur les deux distributions.

A la première requête au serveur, le CDN cache les ressources statiques dans un répertoire préalablement défini. La répartition entre les CDN du cluster se fait en fonction des règles du HAProxy.

## DNS Failover

*Ce chapitre présente la solution de DNS Failover utilisée*

**Principe du Round Robin**

Le DNS Failover se base sur l'algorithme de round robin. Il permet de répartir la charge sur plusieurs serveurs. Le principe est de créer plusieurs enregistrement A associant différentes adresses IP avec un même nom de domaine.

Ici, on crée deux enregistrement A, traincommander.me pointant sur 91.69.239.33 et traincommander.me pointant sur 82.246.192.187. On crée ensuite un enregistrement CNAME www.traincommander.me, alias de tous les enregistrements root. La charge sera alors répartie équitablement, à 50% sur le serveur primaire ayant l'IP 91.69.239.33 et à 50% sur le serveur secondaire ayant l'IP 82.246.192.187.

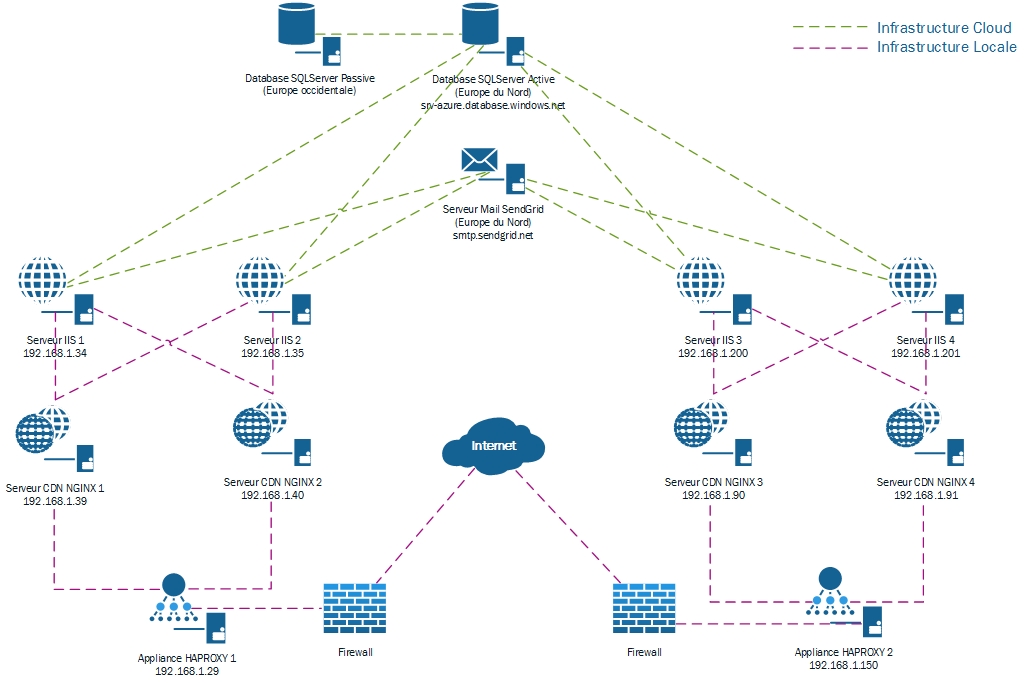
|  |  |  |
| --- | --- | --- |
| Nom/Hôte/Alias | Type d'enregistrement | Valeur/Réponse/Destination |
| 91.69.239.33 | A | traincommander.me |
| 82.246.192.187 | A | traincommander.me |
|  | CNAME | traincommander.me |

**Fonctionnement du DNS Failover**

Le service DNS Failover de DNS MADE EASY est utilisé pour assurer la connexion des sites et web services dans le cas d'un sinistre système ou réseau. Il s'agit de rediriger le traffic DNS d'une IP vers l'autre. Le service peut aussi être utilisé pour migrer le traffic entre des connexions internet redondées. Le DNS Failover en round robin répartit le traffic entre les hôtes à condition que tous les hôtes soient joignables. Si un hôte n'est pas joignable, il est retiré du pool round robin.

Le DNS Failover est configuré avec des enregistrements A pointant sur des adresses IP. Les serveurs de supervisions de DNS MADE EASY vérifient la connexion à l'adresse IP primaire toutes les 2 à 4 minutes. On peut configurer les serveurs de supervision pour qu'ils vérifient si le service utilisent les protocoles TCP, UDP, HTTP ou HTTPS et sur quel port. Dés que le serveur primaire ne répond pas à au moins 2 serveurs de supervision situés à des endroits géographiquement différents, le DNS est directement mis à jour sur tous les serveurs de DNS MADE EASY pour pointer sur une adresse IP secondaire, tant que cette IP répond sur le même port et protocole. Il est possible d'ajouter jusqu'à 5 adresses IP.

## Schéma d’architecture logique

*Voici le schéma d'architecture logique de l'infrastructure mise en place*

# Services Cloud

## DBaaS Azure

Azure SQL Database est une base de données DBaaS (base de données en tant que service) relationnelle hébergé dans le cloud public d’Azure. Elle est optmisée pour le développement d’applications qui interagissent avec des services du cloud. Azure SQL Database repose sur du matériel et des logiciels standardisés, qui sont détenus, hébergés et gérés par Microsoft. Ses points forts sont :

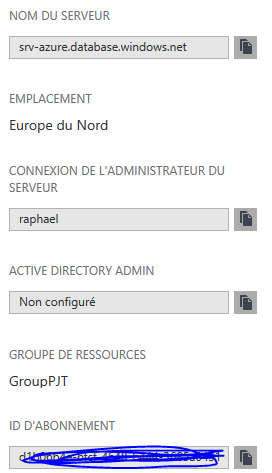
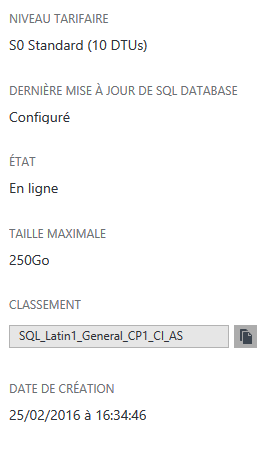
* Capacité d’1TB de données de base
* Restriction des droits d’administration
* Elimine les coût du matériel SQL Server
* Support et maintenance Microsoft
* Solution de haute disponibilité et récupération d’urgence
* Sauvegardes et restorations simples
* Vendue sous la forme d’un service sans licence
* Seuls les coûts de stockage sont facturés

NOTE : Nous assurons la redondance du service en répliquant les données sur un site en Europe Occidentale alors que la base de données principale sera sur un site en Europe du Nord.

Microsoft administre le matériel physique, réplique automatiquement toutes les données pour assurer la haute disponibilité, configure et met à niveau le logiciel de base de données, gère l’équilibrage de charge et procède au basculement transparent en cas de défaillance du serveur. On peut continuer d’administrer la base de données, mais on a plus à gérer le moteur de base de données, ni le système d’exploitation ou le matériel du serveur. Parmi les éléments qu’on peut continuer d’administrer, il y a les bases de données et les connexions, l’optimisation des index et des requêtes, ainsi que l’audit et la sécurité.

La géo-réplication est activée sur la base de données. Elle permet d’assurer la redondance de base de données dans une même région Microsoft Azure ou dans différentes régions (géo-redondance). La géo-réplication réplique de manière asynchrone les transactions validées à partir de la base de données sur une copie de la base de données sur un autre serveur. Elle fournit aussi une solution de récupération d’urgence.

Propriétés de la base de données Azure :



## Service de messagerie SendGrid

SendGrid est un [service de messagerie dans le cloud](https://sendgrid.com/email-solutions) qui fournit des fonctionnalités fiables en matière de [remise de courrier électronique transactionnelle](https://sendgrid.com/transactional-email), d'extensibilité et d'analyse en temps réel, ainsi que des API flexibles qui facilitent l'intégration personnalisée.

Un email transactionnel ("messages de services") est un email très attendu par l'internaute car son envoi se déclenche automatiquement à la suite d’une transaction, un évènement bien précis. Les exemples classiques sont: ouverture de compte et message de bienvenue, confirmation d'expédition d'une commande, suivi/statut d'envoi d'une commande, inscription via un formulaire de contacts, clôture de compte, confirmation de paiement, envoi de facture...

Plusieurs plans ont disponibles selon son usage. Ici, le plan F1 Free est sélectionné. Il offre les fonctionnalités suivantes :

* Jusqu’à 12000 emails par mois
* Jusqu’à 400 emails par jour
* Intégration d’APIs personnalisée
* Reporting avancé
* Fonctionnalités d’envoi avancées
* Support

# Sécurité

## Renforcement de la sécurité ESXi

L’optimisation de l’accès et du contrôle basés sur des rôles supprime la dépendance vis-à-vis d’un compte root partagé. Les utilisateurs et les groupes peuvent être dotés de droits d’administration complets. Il n’est pas nécessaire de partager un accès ni un compte super utilisateur commun pour pouvoir effectuer des tâches administratives.

**Journaux et audits exhaustifs**

vSphere ESXi enregistre toute l’activité des utilisateurs depuis le Shell et depuis l’interface utilisateur de console directe au titre du compte utilisateur. Cette journalisation garantit la responsabilisation et facilite les activités d’audit utilisateur.

**vMotion**

La migration à chaud de VMware vSphere vous permet de déplacer toute une machine virtuelle active d’un serveur physique à un autre, sans interruption de service. Les clients peuvent migrer les machines virtuelles actives entre les clusters, les commutateurs distribués et les instances vCenter sur de longues distances avec un temps de latence aller-retour jusqu’à 100 ms.

**Pare-feu sans état**

ESXi inclut un pare-feu sans état, orienté services. Ce pare-feu permet de définir des règles d’accès aux ports pour les services. Il permet aussi d’indiquer des plages d’adresses IP ou des adresses IP individuelles, qui peuvent se connecter à des services d’hôte.

## Sécurité applicative HAProxy

La solution HAProxy, étant le point d’entrée de l’infrastructure de chaque site, agit comme un véritable garant de la sécurité. Elle assure plusieurs niveaux de protection :

* Validation protocolaire (HTTP)
* Protection contre les attaques DoS, DDoS, vers, injections SQL, etc.
* Gestion des ACLs
* Gestion des listes noires / blanches
* Filtrage des URLs et la possibilité de restreindre l'accès par un système d'authentification
* Blocage des fuites d'information
* Filtrage des requêtes et des réponses HTTP/HTTPS

## Sécurisation de la couche Données

La base de données SQL Microsoft Azure offre des mesures de sécurité à tous niveaux :

* **Sécurité de la connexion :**

On crée une règle de pare-feu au niveau du portail de Microsoft Azure pour refuser toute tentative de connexion d’une adresse IP qui ne serait pas celle du site primaire ou celle du site secondaire.

Toutes les données en transit depuis et vers la base de données sont chiffrées (SSL/TLS). Dans la chaîne de connexion de l’application, on spécifie les paramètres **Encrypt = True** et **TrustServerCertificate = False,** permettant de chiffrer la connexion et de ne pas accepter le certificat du serveur. Sans cela, la connexion ne vérifie pas l’identité du serveur et peut faire la cible d’attaques de types PITM.

* **Authentification :**

Il s’agit du processus de validation de son identité lorsqu’on se connecte à la base de données. Pour le master, on utilise l’authentification SQL qui utilise un nom et un mot de passe. On ajoute un autre administrateur de serveur qui utilise des identités gérées par Azure Active Directory et est prise en charge pour des domaines gérés et intégrés. Cet administrateur peut effectuer toutes les opérations de l’administrateur master. On utilise cet utilisateur depuis l’application. Cela permet de limiter les autorisations accordées à l’application et de réduire les risques d’activité malveillante comme les attaques par injection de code SQL.

* **Autorisation :**

Les actions que l’on peut exécuter dans une la base de données sont contrôlées par les permissions et l’appartenance au rôle du compte utilisateur. Pour limiter le nombre d’actions que peut réaliser un utilisateur, nous définissons des autorisations granulaire, c’est-à-dire que certaines colonnes sont accessibles en lecture seule, d’autres en lecture écriture et d’autres en lecture écriture et modification.

* **Chiffrement :**

Vos données « au repos » ou stockées dans des fichiers de base de données et des sauvegardes sont chiffrées en AES 256B. Il est possible aussi de chiffrer vos données au niveaux des cellules ou bien via un module de sécurité matériel.

* **Audit :**

La fonction d’audit permet d’enregistrer les évènements survenus dans la base de données dans un journal d’audit au sein de votre compte Microsoft Azure Storage. Elle permet aussi d’en sortir des rapports et des analyses.

* **Conformité :**

Elle participe à des audits de sécurité régulier et est certifiée conforme avec de nombreuses normes.

* **Backup intégré :**

Les bases de données sont automatiquement sauvegardées dans la base de données SQL Azure. Ces sauvegardes sont gardées pendant 7 jours. Avec ces sauvegarde, la base de données SQL Azure supporte 2 options de restoration :

* Restoration Point in Time : elle permet à la base de données d’être restorées n’importe quand, à la milliseconde près. Elle utilise les sauvegardes de la base de donnée
* Restoration Géolocalisée : elle utilise la sauvegarde de la dernière base de donnée redondée dans le cas un incident s’est produit dans la région où est hébergée la base de donnée.

## Email chiffré et sécurisé

Tous les emails envoyés via SendGrid utilisent l’encryption TLS, du moment que le serveur mail du destinataire supporte le TLS. Les emails sont donc protégés des interceptions / modifications d’un adversaire passif. Si le FAI du destinataire ne supporte pas le TLS, le message est quand même délivré par SendGrid – juste sans l’encryption TLS.

En plus de l’encryption, la solution assure :

* Authentification de l’émetteur de l’email et vérification de la légitimité de l’émetteur et du contenu.
* Protection de la connexion serveur à serveur et de tous les blocs de données envoyés (pieces jointes, adresse email de l’émetteur, etc.)
* Activation du service dés l’enregistrement. Pas de coût additionnel.

*Support Client Live :*

SendGrid propose du support gratuit par téléphone ou par chat, la semaine entre 6h et 18h (heure Pacifique) avec un support pour les incidents critiques disponible 7 jours sur 7 toute l’année. Une base de connaissance et une communauté de développeur sont aussi disponibles depuis leur site.

# Administration

*Cette section définit les modes d'administration de la solution dans le cadre du projet haute disponibilité du site Qwirk*

## Accès à l'équipement

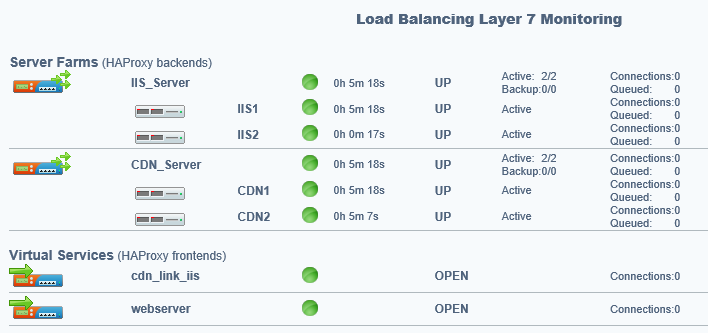
Les serveurs sont stockés dans des environnements adaptés et sécurisés dont l’accès est restreint aux personnes responsables.

Pour toute action nécessitant une intervention physique sur nos serveurs, nous faisons appel à nos équipes sur place.

Pour l’accès à distance, nous nous connectons en RDP (port standard sécurisé 3389) sur le serveur VCenter.

## Supervision des serveurs

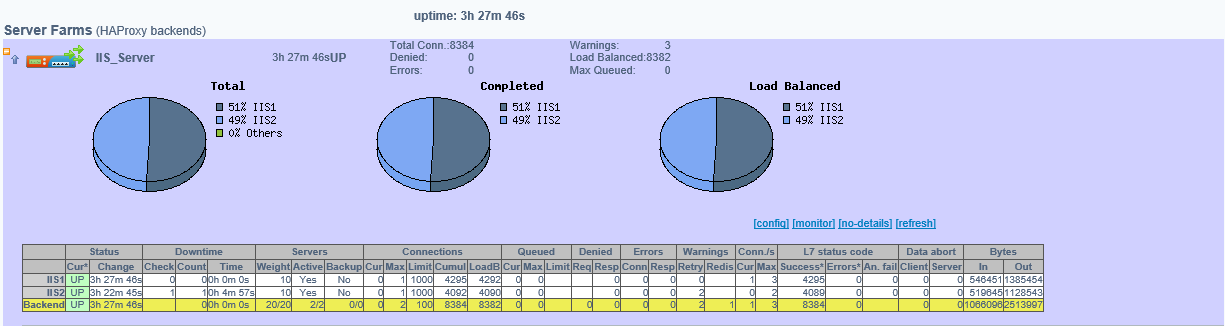
L'outil de monitoring de HAPROXY permet d’observer l'état des services et serveurs en temps réel. Il remonte plusieurs information facilitant le dépannage.

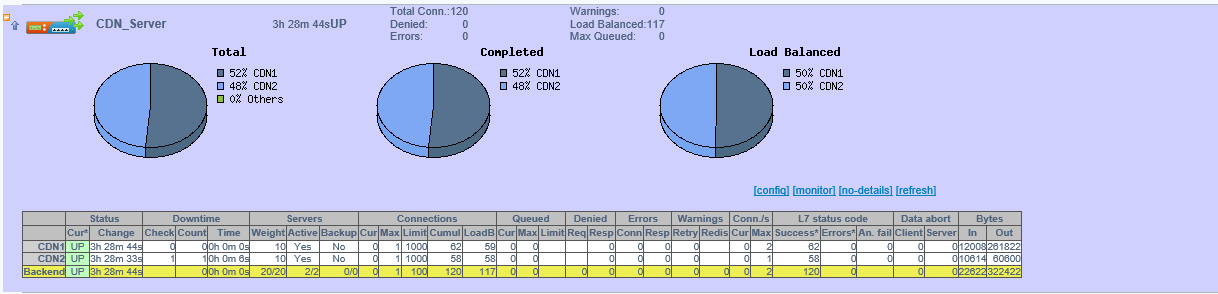


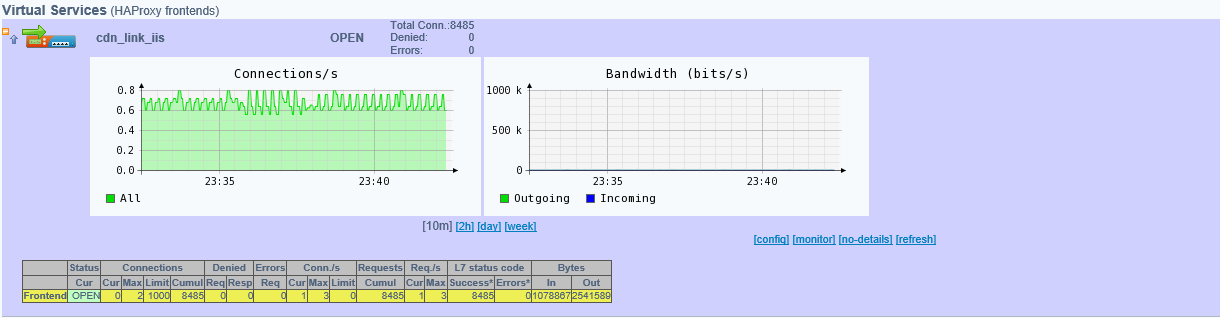
*Etats des fermes de serveurs et services frontend*

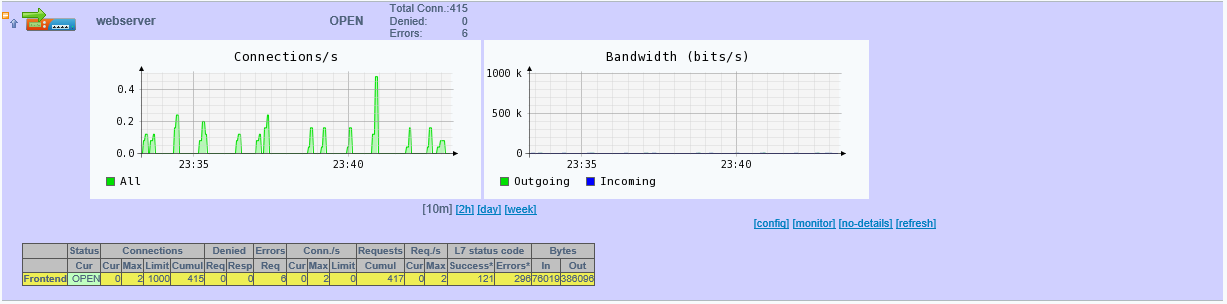
Pour chaque service, des statistiques sont disponibles. Elles indiquent notamment l'occupation de l'espace par chaque service, la charge répartie sur les serveurs, et le trafic en bytes qui traverse les services.

Elles montrent aussi les période de downtime, les erreurs et warnings relevés, et les refus de connexion, aussi bien au niveau des services frontend que des clusters.









La génération de logs permet la journalisation de l’activité, et permet d’identifier les status critiques.

* Logs système
* Logs des évènements
* Logs trafic
* Logs console

# Annexes

## Schéma du workflow

