

Bsc.1 – Année 2015-2016

Rapport technique Infrastructure

Train Commander



SUPINFO
International University

Groupe 1600

FRANÇOIS A., TOM B., THOMAS C., BENJAMIN F., ANTHONY R.,
NOE V.

Sommaire

INTRODUCTION.....	2
1. PRESENTATION DE L'INFRASTRUCTURE	3
2. PRESENTATION DES OUTILS UTILISES	4
3. MISE EN PLACE DE L'INFRASTRUCTURE.....	6
3.1. GESTION DU STOCKAGE	6
3.2. GESTION DE LA HAUTE DISPONIBILITE.....	8
3.3. GESTION DE LA VIRTUALISATION	11
3.3.1. <i>Le contrôleur de domaine</i>	13
3.3.2. <i>Le serveur web</i>	15
3.3.3. <i>Le serveur de la base de données</i>	16
3.3.4. <i>La machine client</i>	17
3.4. GESTION DE LA SECURITE	18
3.5. GESTION DU CONTENT DELIVERY NETWORK	19
CONCLUSION	21
BIBLIOGRAPHIE.....	22
TABLE DES ILLUSTRATIONS.....	23
ANNEXES.....	24

Introduction

L'objectif de l'application Train Commander est de consulter les trajets des trains en France d'un point A à un point B et dans les autres pays desservis par la SNCF, et de pouvoir réserver son billet.

Couplées à une API commune avec l'application WEB et iOS, les deux applications communiquent de manière synchrone en temps réel (grâce à une base de données commune) et disposent des mêmes fonctionnalités.

L'application a été entièrement développée en anglais.

De nos jours, il est nécessaire d'avoir une infrastructure solide et stable pour avoir une qualité à la hauteur. Celle-ci doit être bien définie dès le départ ce qui permet d'assurer une continuité des services.

A travers ce rapport, nous commencerons par vous présenter l'architecture de manière générale. Puis, nous évoquerons les outils techniques utilisés et enfin, la mise en place de cette infrastructure en vous montrant la démarche que nous avons suivie.

Précisons qu'en annexes, vous trouverez un glossaire et un lexique expliquant les termes les plus techniques (identifiés par une « * »).

1. Présentation de l'infrastructure

L'architecture réseau se compose de :

- 3 serveurs physiques :
 - o 2 serveurs avec le rôle Hyper-V gérant le cluster*
 - o 1 serveur faisant office de baie de SAN* iSCSI*
- 3 serveurs virtualisés :
 - o 1 serveur contrôleur de domaine*
 - o 1 serveur web
 - o 1 serveur de base de données
- 1 pare-feu/routeur
- 1 machine de test

Cette architecture se base sur 3 différents réseaux :

- 1 réseau LAN* gérant l'administration
- 1 réseau LAN destiné à la connexion au stockage (baie de SAN)
- 1 réseau WAN* pour la connexion à Internet

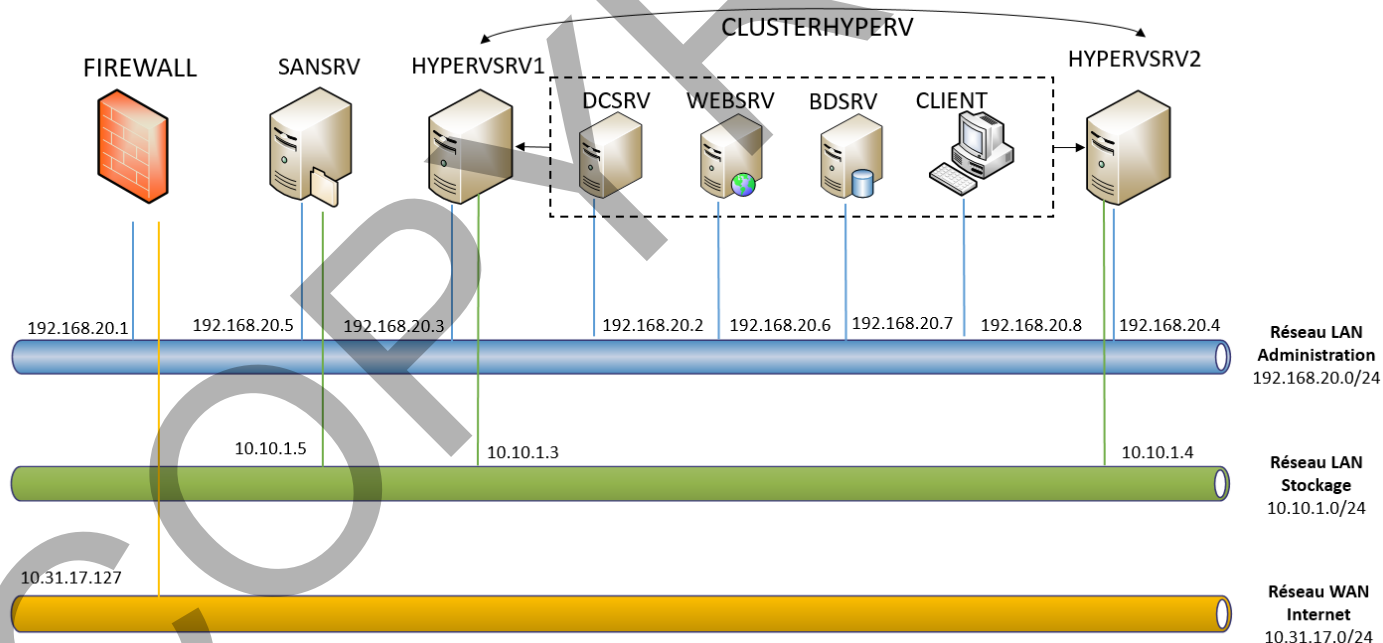


Figure 1. Schéma de l'infrastructure

Ci-dessous un récapitulatif des différentes machines avec leurs adressages IP* :

Serveur	Descriptif	Adresse IP	Passerelle	DNS
FIREWALL	Pare-feu PfSense	192.168.20.1 10.31.17.127	X X	192.168.20.2 X
DCSRV	Contrôleur de domaine, DNS, Active Directory, Superviseur de HYPERVCLUSTER	192.168.20.2	192.168.20.1	127.0.0.1
SANSRV	Baie de stockage SAN ISCSI	192.168.20.3 10.10.1.3	192.168.20.1 X	192.168.20.2 192.168.20.2
HYPERVSRV1	Premier nœud de l'hyperviseur	192.168.20.4 10.10.1.4	192.168.20.1 X	192.168.20.2 192.168.20.2
HYPERVSRV2	Deuxième nœud de l'hyperviseur	192.168.20.5 10.10.1.5	192.168.20.1 X	192.168.20.2 192.168.20.2
WEBSRV	Serveur web IIS 8.0	192.168.20.6	192.168.20.1	192.168.20.2
BDSRV	Base de données SQL* Server 2014 Enterprise	192.168.20.7	192.168.20.1	192.168.20.2
CLIENT	Machine de test sous Microsoft Windows 10 Pro	192.168.20.8	192.168.20.1	192.168.20.2

Figure 2. Tableau récapitulatif de l'infrastructure réseau (en bleu : les serveurs virtualisés ; en vert : les serveurs physiques)

2. Présentation des outils utilisés

Durant notre projet, nous avons dû utiliser les outils suivants :

- **Microsoft Windows Server 2012 R2** : système d'exploitation réseau Windows Server. Plusieurs versions existent dont :



- o Version « Standard » : principale édition offrant toutes les fonctionnalités du produit (serveur IIS, Active Directory*, Hyper-V, serveur de fichier...). Cependant, le nombre de machines virtuelles* couvertes par la licence est limité à deux.

→ Utilisé par SANSRV, DCSR, BDSRV et WEBSRV

- o Version « Datacenter » : offrant les mêmes fonctionnalités que la version « Standard » mais ici, le nombre de machines virtuelles couvertes par la licence est illimité.

→ Utilisé par HYPERVSRV1 et HYPERBBSRV2



- **Microsoft SQL Server 2014 Standard** : système de gestion de base de données (SGBD). C'est une suite composée de 5 services principaux :
 - o Un moteur relationnel : SQL Server
 - o Un moteur décisionnel incluant un moteur de stockage, des algorithmes de forage et différents outils de Business Intelligence : SQL Server Analysis Services
 - o Un « Extract Transform and Load » destiné à la mise en place de logiques de flux de données, notamment pour alimenter des entrepôts de données :
 - o Un outil de génération : SQL Server Reporting Service
 - o Un système de planification de travaux et de gestion d'alerte : Agent SQL
 - o De nombreux outils de développement comme pour les bases transactionnelles avec SQL Server Management Studio
 - Utilisé par BDSRV
- **Microsoft Windows 10 Professionnel** : système d'exploitation destiné aux clients particuliers ou entreprises. Cette version permet de se connecter à un nom de domaine.
 - Utilisé par CLIENT
- **PfSense 2.3** : Routeur/pare-feu open source basé sur le système d'exploitation FreeBSD. Il utilise le pare-feu à états Packet Filter et permet de créer des fonctions de routage et de NAT lui permettant de connecter plusieurs réseaux informatiques. Il se comporte comme l'équivalent libre des outils et services utilisés sur des routeurs professionnels propriétaires. L'administration est simple et se configure soit en ligne de commande ou via une interface graphique web.
 - Utilisé par FIREWALL

3. Mise en place de l'infrastructure

3.1. Gestion du stockage

Lors de la mise en place d'une infrastructure, il est important de séparer les données d'un côté et les « services » de l'autre. C'est pourquoi, nous avons créé une baie de stockage en SAN iSCSI grâce au rôle « Microsoft iSCSI Software Initiator Windows », disponible sur le serveur SANSRV. Sur celui-ci, nous avons installé en plus du disque dur où est stocké le système d'exploitation (OS*), quatre autres montés en RAID1* (2x2 RAID1) permettant d'assurer la redondance des données. En cas de dysfonctionnement d'un des disques durs, le second permettra la restauration des données sur le nouveau.



Figure 3. Disques durs (DATASRV & SAVEVM) en RAID 1

Nous avons créé sur le « DATASRV » des disques virtuels iSCSI en raison d'un par machine virtuelle (VM). Chacun fait référence à une Target* spécifique permettant de mieux s'organiser.

Path	Virtual Disk Status	Target Name	Target Status	Initiator ID	Size
SANSRV (6)					
Filescsvirtualdisk\databd.vhdx	Not Connected	target-databd	Not Connected	IQNiqn.1991-05.com.microsoft.hyperv.sv1.traincommander.local; IQNiqn.1991-05.com.microsoft.hyperv.sv2.traincommander.local	28,0 GB
Filescsvirtualdisk\databev.vhdx	Not Connected	target-databev	Not Connected	IQNiqn.1991-05.com.microsoft.hyperv.sv1.traincommander.local; IQNiqn.1991-05.com.microsoft.hyperv.sv2.traincommander.local	28,0 GB
Filescsvirtualdisk\dcsrv.vhdx	Not Connected	target-dcsrv	Not Connected	IQNiqn.1991-05.com.microsoft.hyperv.sv1.traincommander.local; IQNiqn.1991-05.com.microsoft.hyperv.sv2.traincommander.local	20,0 GB
Filescsvirtualdisk\client.vhdx	Not Connected	target-client	Not Connected	IQNiqn.1991-05.com.microsoft.hyperv.sv1.traincommander.local; IQNiqn.1991-05.com.microsoft.hyperv.sv2.traincommander.local	20,0 GB
Filescsvirtualdisk\quorum.vhdx	Not Connected	target-quorum	Not Connected	IQNiqn.1991-05.com.microsoft.hyperv.sv1.traincommander.local; IQNiqn.1991-05.com.microsoft.hyperv.sv2.traincommander.local	1,00 GB
Filescsvirtualdisk\savevm.vhdx	Not Connected	target-savevm	Not Connected	IQNiqn.1991-05.com.microsoft.hyperv.sv1.traincommander.local; IQNiqn.1991-05.com.microsoft.hyperv.sv2.traincommander.local	19,0 GB

Figure 4. Présentation des disques durs iSCSI

Sur le disque dur « SAVEVM », nous stockons les snapshots* des VM (Cf. 3.3).

Ensuite, les deux hyperviseurs se connectent aux disques durs récupérés via l'interface Initiator* iSCSI.

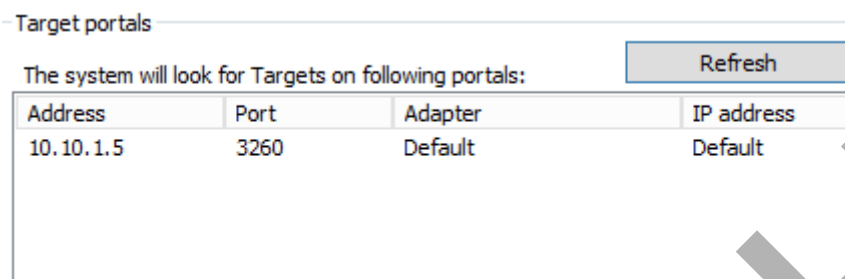


Figure 5. Recherche de toutes les Target disponibles sur le SANSRV.

Name	Status
iqn.1991-05.com.microsoft:sansrv-target-client-target	Connected
iqn.1991-05.com.microsoft:sansrv-target-databd-target	Connected
iqn.1991-05.com.microsoft:sansrv-target-dataweb-target	Connected
iqn.1991-05.com.microsoft:sansrv-target-dcsrv-target	Connected
iqn.1991-05.com.microsoft:sansrv-target-quorum-target	Connected
iqn.1991-05.com.microsoft:sansrv-target-savevm-target	Connected

Figure 6. Connexion aux Target permettant de récupérer les disques durs virtuels iSCSI

Nous avons activé le multi-path* sur chacun de ses disques pour que les deux hyperviseurs puissent se connecter simultanément. Il suffit ensuite en se rendant dans le gestionnaire de disques, de les initialiser puis de créer un nouveau volume et enfin les ajouter dans le cluster (Cf. §3.2) pour que les VM puissent être stockés dessus.

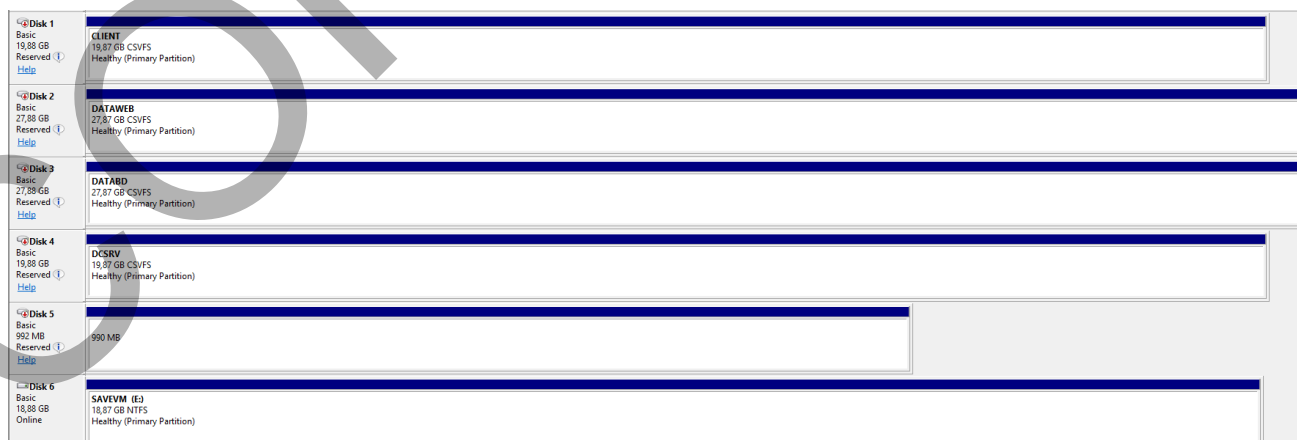


Figure 7. Nouveaux volumes créés

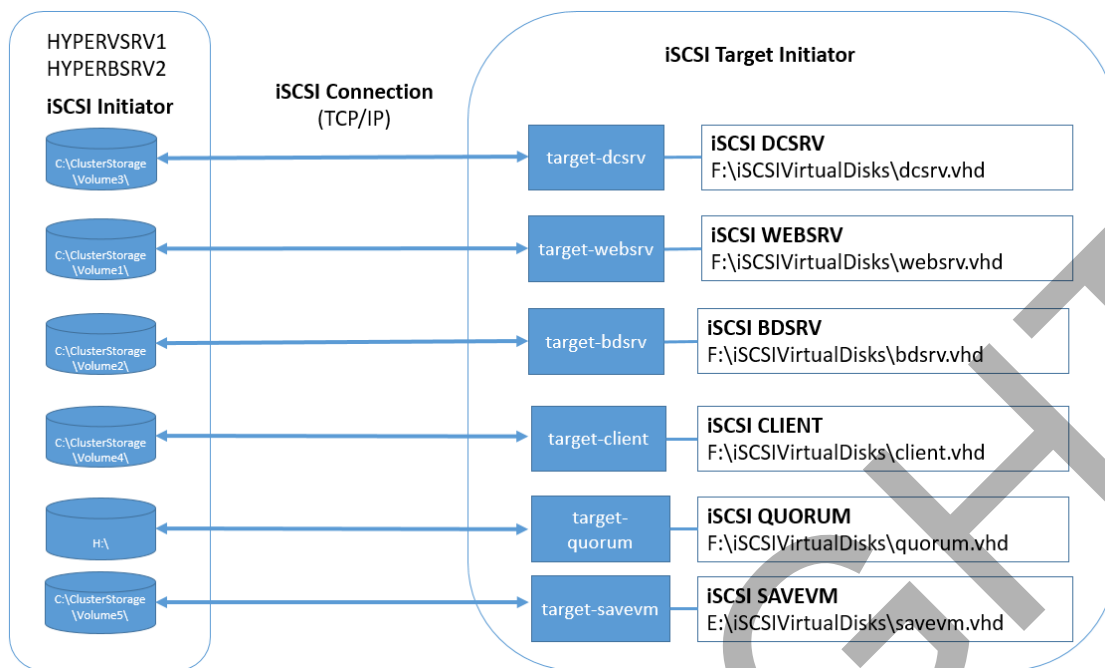


Figure 8. Schéma récapitulatif représentant une connexion entre une Target et un Initiator

3.2. Gestion de la haute disponibilité

Aujourd'hui, la disponibilité est en enjeu important dans l'infrastructure informatique. Elle permet d'assurer la continuité d'un service en cas de dysfonctionnement. Nous avons mis en place un cluster à basculement (CLUSTERHYPERV) entre les deux machines HYPERVSRV1 et HYPERVSRV2. Chacune a le rôle « Hyper-V » d'installé, ce qui permet d'avoir un cluster de deux hyperviseurs. Chacun de ces hyperviseurs ont des machines virtuelles.

A noter, l'interface « Failover Cluster Manager » permettant de contrôler le cluster se trouve sur le serveur « DCSRVR ».

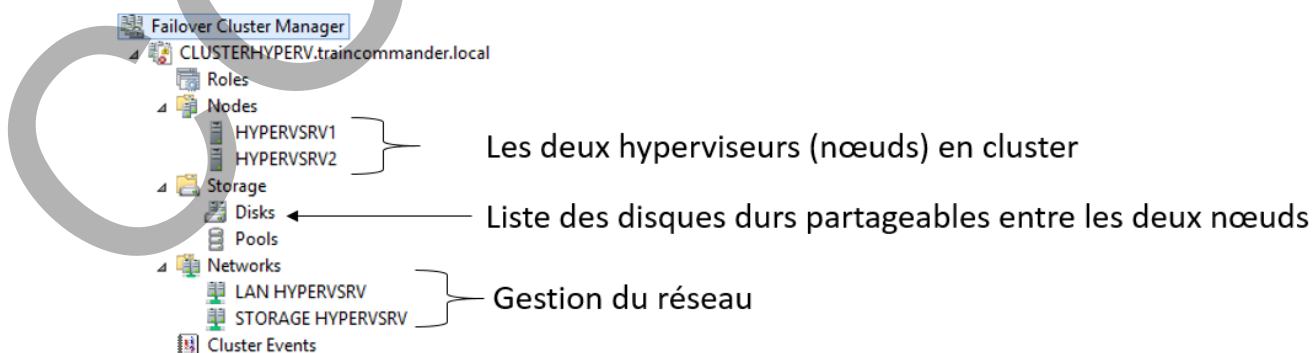


Figure 9. Description des onglets dans l'interface du cluster

Pour chaque VM, on peut connaître son nom, son état (en cours, arrêté, en pause...) et sa priorité (ordre de passage en cas de reboot ou de changement d'hyperviseur en cas de panne).

Name	Status	Type	Priority	Information
DCSRV	Running	Virtual Machine	High	
WEBSRV	Running	Virtual Machine	Medium	

Name	Status	Type	Priority	Information
BDSVR	Off	Virtual Machine	Medium	
CLIENT	Off	Virtual Machine	Low	

Figure 10. Machines virtuelles présents sur chaque hyperviseur

Nous pouvons également, définir plusieurs paramètres sur la VM tels que :

DCSRV Properties - General Tab

- Hyperviseur favoris:** Preferred Owners list includes HYPERVSRV1 and HYPERVSRV2.
- Priorité de la VM:** Priority is set to High.

DCSRV Properties - Failover Tab

- Nombre maximum de test de basculement en espace de temps:** Maximum failures in the specified period is 3.
- Basculement immédiat en cas de panne:** Failback is set to Immediately.

Figure 11. Propriété d'une machine virtuelle

Le cluster fonctionne comme l'exemple ci-dessous :

A et B sont des hyperviseurs. A contient deux machines virtuelles (VM) : A1 et A2. B contient 2 VM : B1 et B2.

Si A devient hors ligne, B prend la main et récupère les VM A1 et A2. Lorsque A est de nouveau en ligne, B donne à A ses VM (A1 et A2). Ce schéma fonctionne aussi si c'est B qui est hors ligne.



Figure 12. Simulation d'une panne sur le serveur HYPERVSRV2

Roles on HYPERVSRV1 (4)

Search

Name	Status	Type	Priority
BDSVR	Off	Virtual Machine	Medium
CLIENT	Off	Virtual Machine	Low
DCSRV	Running	Virtual Machine	High
WEBSRV	Running	Virtual Machine	Medium

Figure 13. Le serveur HYPERVSRV1 récupère les VM de HYPERVSRV2

Roles on HYPERVSRV2 (0)

Search

Name	Status	Type	Priority	Information
------	--------	------	----------	-------------

Figure 14. Le serveur HYPERVSRV2 ne possède plus de VM

Ce dispositif est possible étant donné que les disques durs de ces VM sont stockés dans une baie de SAN. En effet, si les disques durs étaient stockés sur les hyperviseurs en cas de panne de l'un des deux, les données ne seraient plus accessibles par l'autre.

Depuis l'onglet « disk » présent dans l'interface permettant de gérer le cluster, nous avons accès aux disques durs qui seront utilisés pour les VM. Il faut les mettre en « Cluster Shared Volume » pour que ce volume soit partagé dans le cluster.

Egalement, nous avons ajouté un disque dur « QUORUM » qui est important pour la gestion du cluster. Le quorum détermine le nombre d'échecs que le cluster peut supporter (dans notre cas, il est paramétré à 3 échecs en l'espace d'une heure). S'il y a un échec supplémentaire, le cluster doit cesser de s'exécuter. Notre disque dur se comporte comme un témoin de disque, c'est-à-dire qu'il contient une copie de la configuration du cluster.

Disks (6)						
Search						
Name	Status	Assigned To	Owner Node	Disk Number	Capacity	Information
CLIENT	Online	Cluster Shared Volume	HYPERVSRV1	1	20 GB	
DATABD	Online	Cluster Shared Volume	HYPERVSRV1	3	28 GB	
DATAWEB	Online	Cluster Shared Volume	HYPERVSRV1	2	28 GB	
DCSRV	Online	Cluster Shared Volume	HYPERVSRV1	4	20 GB	
QUORUM	Online	Disk Witness in Quorum	HYPERVSRV1	5	1 GB	
SAVEVM	Online	Cluster Shared Volume	HYPERVSRV2	6	19 GB	

Figure 15. Listes des disques durs utilisés par les VM (1 disque dur = 1 VM sauf pour le QUORUM et SAVEVM)

3.3. Gestion de la virtualisation

Afin de mutualiser les capacités de chaque serveur, permettant de réaliser des économies et de réduire les investissements en infrastructures physiques, nous avons décidé de virtualiser les serveurs au sein de notre cluster. Pour rappel, chaque disque dur de ces serveurs virtualisés est stocké dans une baie de SAN. Avantage de cette virtualisation : on peut faire fonctionner différents systèmes d'exploitation sur une même machine physique. Plusieurs solutions de virtualisation existent tels que : VMware vSphere, Citrix Xen Server, Oracle VM, Microsoft Hyper-V... C'est cette dernière que nous avons mise en place. Il s'agit dans notre cas d'un hyperviseur de type 2. C'est-à-dire qu'on exécute sur le matériel physique, un OS (Windows Server 2012 R2) avec le rôle « Hyper-V » d'installé et c'est ce dernier qui va virtualiser un autre OS. Notons que cette solution existe aussi en hyperviseur de type 1.

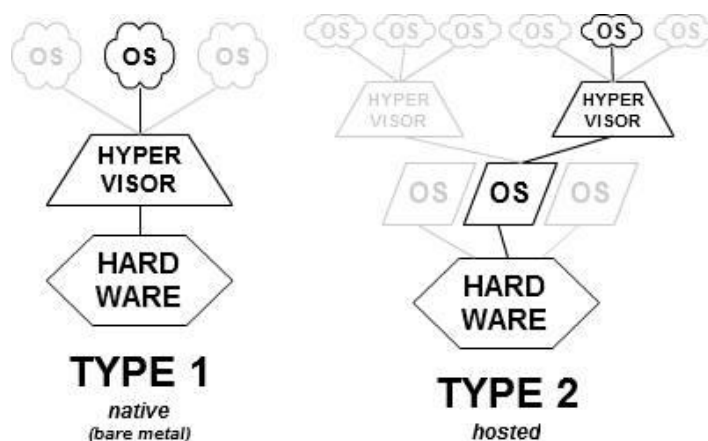


Figure 16. Différences entre les types d'hyperviseurs

Nous avons virtualisé le contrôleur de domaine, le serveur web, le serveur SQL Server et une machine client pour tester l'application.

Pour gérer les VM dans chaque hyperviseur, nous devons nous rendre dans l'interface « Hyper-V Manager », puis sélectionner la VM souhaitée. En faisant un clic-droit dessus, nous pouvons la démarrer, l'arrêter, la mettre en pause, et se connecter à la VM.

A noter que pour préserver les données et les modifications de chaque VM en cas de crash, nous pouvons prendre des snapshots permettant de la restaurer à un état donné. Pour rappel, ils sont stockés sur la baie de SAN iSCSI (Cf. 3.1).

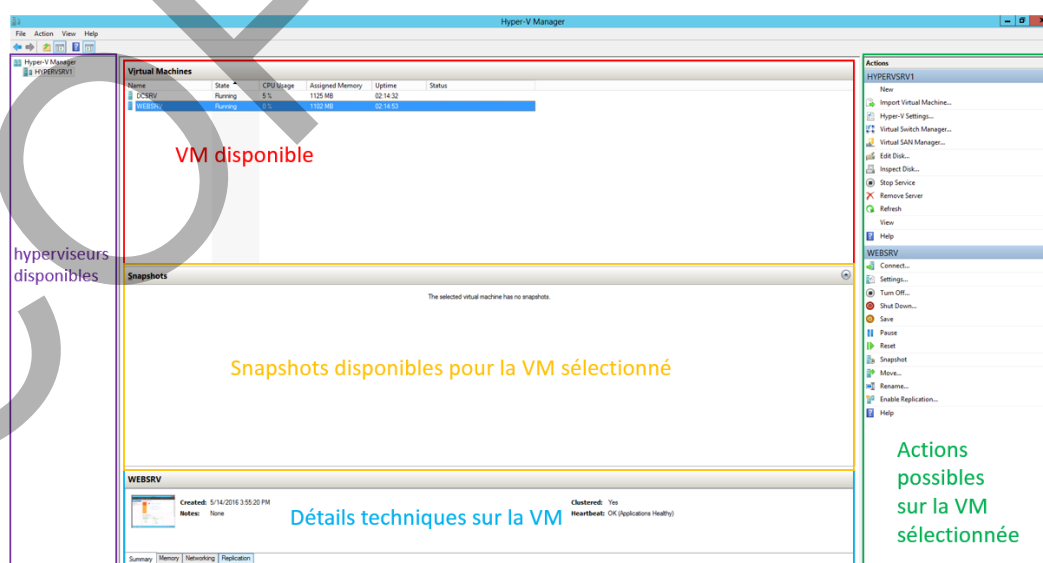


Figure 17. Gestionnaire de l'Hyper-V (ici sur HYPERVSRV1)

3.3.1. Le contrôleur de domaine

Le serveur « DCSRVS » est le contrôleur de domaine de « traincommander.local ». Sur celui-ci, nous avons installé le rôle « Active Directory Domain Services » qui va nous créer notre Annuaire Active Directory. C'est sur ce serveur que nous allons pouvoir créer des objets comme des utilisateurs, des groupes, des GPO*...

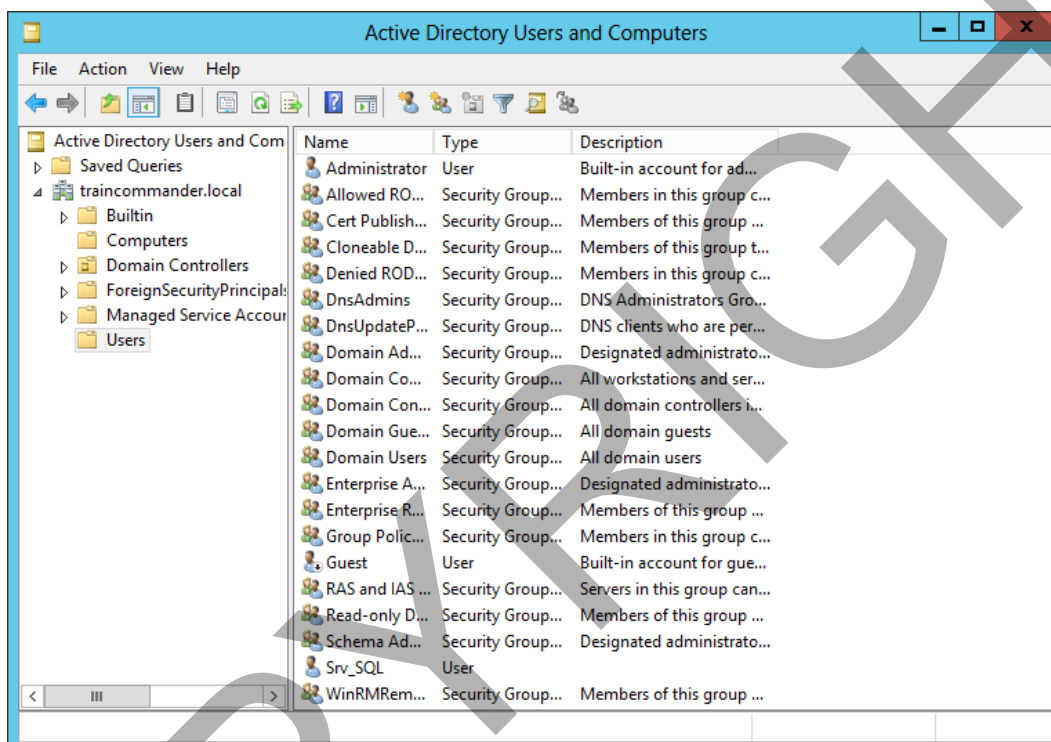


Figure 18. Interface Active Directory Users and Computers

Egalement, il fait office de serveur DNS*. Celui-ci contient 3 zones :

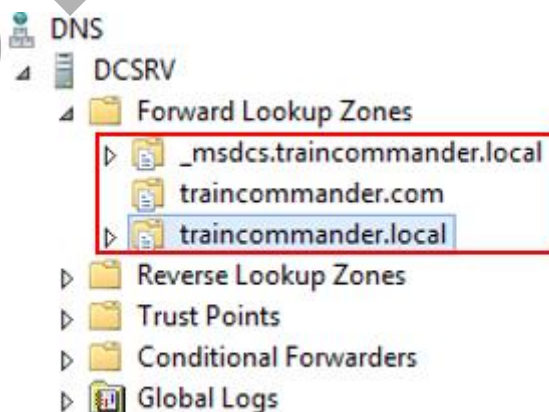


Figure 19. Zones présents dans le serveur DNS

La zone primaire « traincommander.local » contient tous les pointages d'un nom d'une VM (dcsrv) vers son adresse IP locale (192.168.20.2).

La zone primaire « traincommander.com », permet de faire pointer cette zone vers l'adresse IP du serveur Web. Ainsi, lorsqu'on souhaite accéder au site internet de l'application « TrainCommander », il suffira de taper dans le navigateur l'URL suivante : « traincommander.com », et cela nous redirigera vers le serveur web.

Name	Type	Data	Timestamp
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[217], dcsrv.traincomman...	static
(same as parent folder)	Name Server (NS)	dcsrv.traincommander.loc...	static
(same as parent folder)	Host (A)	192.168.20.2	6/4/2016 9:00:00 PM
BDSRV	Host (A)	192.168.20.7	6/4/2016 10:00:00 PM
CAUCLUSTjeu	Host (A)	192.168.20.3	6/4/2016 9:00:00 PM
CAUCLUSTjeu	Host (A)	192.168.20.4	6/4/2016 9:00:00 PM
CLUSTERHYPERV	Host (A)	192.168.20.100	6/4/2016 11:00:00 PM
dcsrv	Host (A)	192.168.20.2	static
HYPERVSRV1	Host (A)	192.168.20.3	6/4/2016 11:00:00 PM
HYPERVSRV2	Host (A)	192.168.20.4	6/4/2016 11:00:00 PM
SANSRV	Host (A)	192.168.20.5	6/4/2016 9:00:00 PM
WEBSRV	Host (A)	192.168.20.6	6/5/2016 4:00:00 PM

Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[5], dcsrv.traincommande...	static
(same as parent folder)	Name Server (NS)	dcsrv.traincommander.loc...	static
(same as parent folder)	Host (A)	192.168.20.6	static

Figure 20. Zones du serveur DNS (en haut : "traincommander.local"; en bas : "traincommander.com")

Pour rappel, il dispose aussi de l'interface permettant de gérer le cluster à basculement entre les deux hyperviseurs (Cf. §3.2).

A noter, qu'il est important qu'il reste toujours allumé car sans lui, les autres serveurs ne pourront pas communiquer entre eux, ni s'authentifier depuis la page de login. C'est pourquoi, faire des snapshots de ce serveur est primordial.

3.3.2. Le serveur web

Le serveur « WEBSRV » s'occupe de gérer nos deux sites web. C'est ici qu'est hébergé le back-end* et le front-end* de l'API*. Ce serveur fonctionne sous Internet Information Services¹ (IIS) avec le Framework ASP.NET² installé pour pouvoir faire tourner du code C#*.

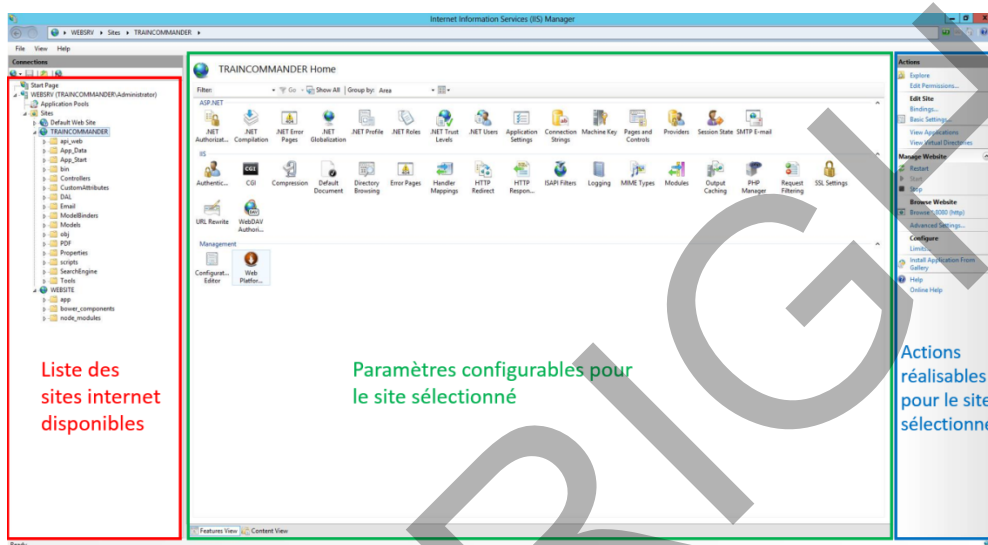


Figure 21. Interface d'administration IIS permettant la gestion des sites internet

Dans l'interface IIS, nous avons mis deux sites :

- Un faisant tourner l'API en C# (back-end) sur le port* 8080.
- Un faisant tourner l'API en Angular JS³* (front-end) sur le port 80.

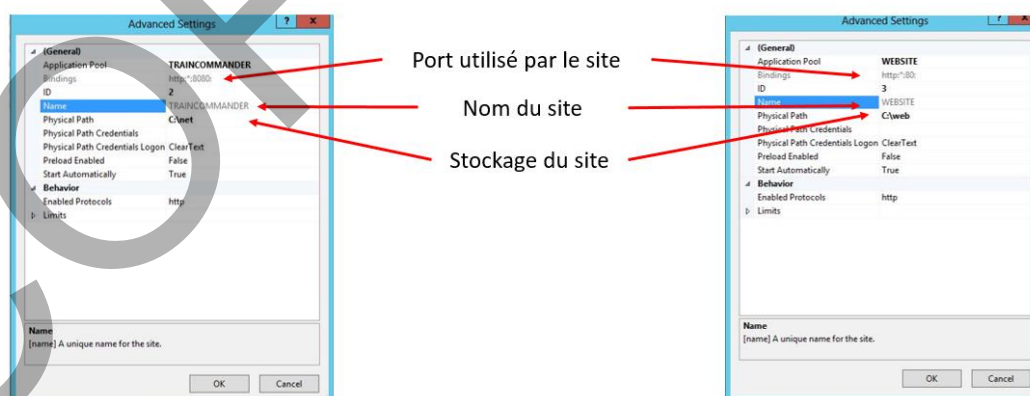


Figure 22. Propriétés des deux sites

¹ Version 8

² Version 4.5.2

³ Version 1.5.5

A noter que l'API back end se connecte à la base de données (Cf. §3.3.3).

3.3.3. Le serveur de la base de données

Le serveur « BDSRV » contient la base de données. On la gère avec SQL Server 2014 Standard. Nous avons dû ouvrir plusieurs ports tel que 1433 pour que l'API puisse se connecter. Egalement, nous avons créé un utilisateur SQL Server « ServeurSQLTC » qui permet ainsi de contrôler la base de données depuis l'extérieur en se connectant à l'adresse IP externe du pare-feu et au bon port externe (Cf. 3.4). Pour se connecter à la base de données depuis le serveur « BDSRV », nous pouvons utiliser l'authentification de Windows.

Pour l'administration, nous utilisons SQL Management Studio nous permettant de visualiser la structure et le contenu de notre base de données.

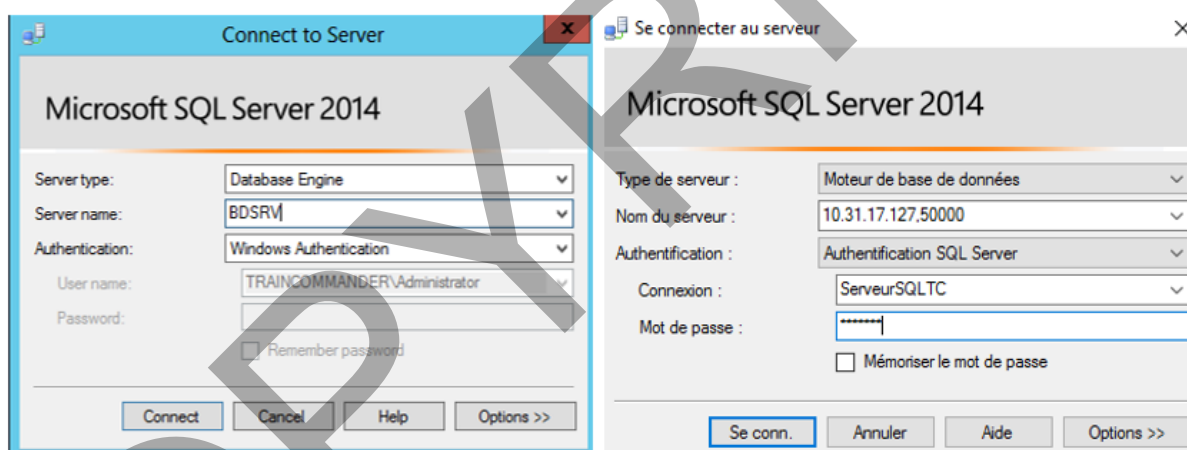


Figure 23. Connexion au serveur SQL Server 2014 en local (à gauche) et depuis l'extérieur (à droite)

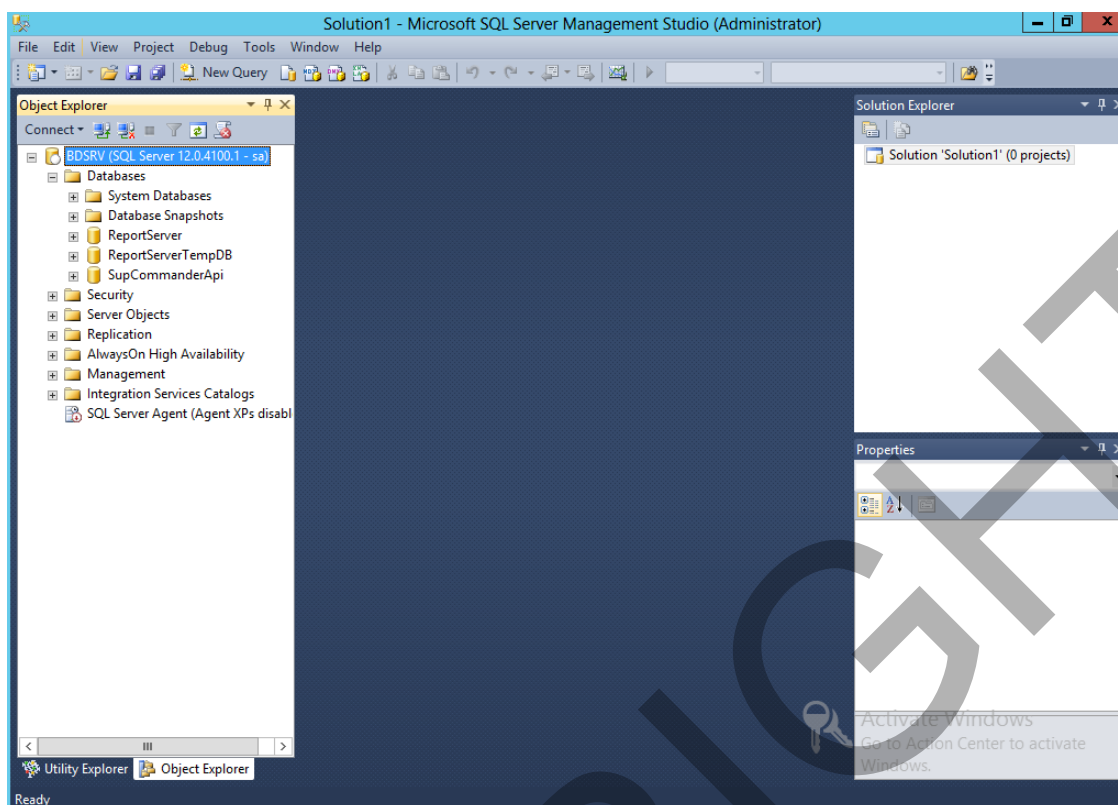


Figure 24. Administration de la base de données

3.3.4. La machine client

La machine « CLIENT » fonctionne sous Windows 10 Professionnel, et nous permet de faire nos tests en interne. Depuis le navigateur, nous tapons l'URL : « traincommander.com » Il nous redirige vers le front-end de l'API. L'utilisateur peut donc commencer à utiliser l'application.



Figure 25. Site internet depuis un navigateur web en local

3.4. Gestion de la sécurité

La sécurité est d'or dans une infrastructure, c'est pourquoi, l'utilisation d'un routeur et pare-feu est fortement recommandée. Notre choix s'est porté vers « PfSense⁴ ».

Lorsqu'un des serveurs tente d'accéder à Internet, sa requête transite vers le pare-feu et c'est ce dernier qui l'autorise ou non. De même lorsqu'un appareil tente d'y accéder depuis l'extérieur.

C'est à travers l'administration web que nous pouvons créer des règles pour le WAN ou le LAN. Pour faciliter l'organisation, nous avons créé des « alias » pour chacun de nos serveurs.

Firewall Aliases IP		
Name	Values	Description
BDSRV	192.168.20.7	Serveur BDSRV
CLIENT	192.168.20.8	Machine de test CLIENT
DCSRV	192.168.20.2	Serveur DCSRV
HYPERVSRV1	192.168.20.3	Serveur HYPERVSRV1
HYPERVSRV2	192.168.20.4	Serveur HYPERVSRV2
SANSRV	192.168.20.5	Serveur SANSRV
WEBSRV	192.168.20.6	Serveur WEBSRV
pfSense	192.168.20.1	Routeur/Pare-feu

Figure 26. Tableau d'alias correspondant à une machine spécifique

Rules										
	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	
<input type="checkbox"/>	WAN	TCP	*	*	*	50008	CLIENT	3389 (MS RDP)	Remote Desktop CLIENT	
<input type="checkbox"/>	WAN	TCP	*	*	*	50007	BDSRV	3389 (MS RDP)	Remote Desktop BDSRV	
<input type="checkbox"/>	WAN	TCP	*	*	*	50006	WEBSRV	3389 (MS RDP)	Remote Desktop WEBSRV	
<input type="checkbox"/>	WAN	TCP	*	*	*	50005	SANSRV	3389 (MS RDP)	Remote Desktop SANSRV	
<input type="checkbox"/>	WAN	TCP	*	*	*	50004	HYPERVSRV2	3389 (MS RDP)	Remote Desktop HYPERVSRV2	
<input type="checkbox"/>	WAN	TCP	*	*	*	50003	HYPERVSRV1	3389 (MS RDP)	Remote Desktop HYPERVSRV1	
<input type="checkbox"/>	WAN	TCP	*	*	*	50002	DCSRV	3389 (MS RDP)	Remote Desktop DCSRV	
<input type="checkbox"/>	WAN	TCP	*	*	*	8080	WEBSRV	8080	Serveur WEB API	
<input type="checkbox"/>	WAN	TCP	*	*	*	80 (HTTP)	WEBSRV	80 (HTTP)	Serveur Web Interface Web	
<input type="checkbox"/>	WAN	TCP	*	*	*	50000	BDSRV	1433	Port 1433 SQL Serveur	

⁴ Version 2.3

Rules (Drag to Change Order)										
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	
<input checked="" type="checkbox"/> 0/2.84 MiB	IPv4+6 TCP/UDP	*	*	WAN address	*	*	none			
<input checked="" type="checkbox"/> 0/0 B	IPv4+6 TCP/UDP	*	*	WAN net	*	*	none			
<input checked="" type="checkbox"/> 0/0 B	IPv4+6 ICMP	*	*	WAN address	*	*	none			
<input checked="" type="checkbox"/> 0/0 B	IPv4 TCP	*	*	BDSRV	1433	*	none		NAT Port 1433 SQL Serveur	
<input checked="" type="checkbox"/> 0/0 B	IPv4 TCP	*	*	WEBSRV	80 (HTTP)	*	none		NAT Serveur Web Interface Web	
<input checked="" type="checkbox"/> 0/0 B	IPv4 TCP	*	*	WEBSRV	8080	*	none		NAT Serveur WEB API	
<input checked="" type="checkbox"/> 0/0 B	IPv4 TCP	*	*	DCSRV	3389 (MS RDP)	*	none		NAT Remote Desktop DCSRV	
<input checked="" type="checkbox"/> 0/0 B	IPv4 TCP	*	*	HYPERVSRV1	3389 (MS RDP)	*	none		NAT Remote Desktop HYPERVSRV1	
<input checked="" type="checkbox"/> 0/0 B	IPv4 TCP	*	*	HYPERVSRV2	3389 (MS RDP)	*	none		NAT Remote Desktop HYPERVSRV2	
<input checked="" type="checkbox"/> 0/0 B	IPv4 TCP	*	*	SANSRV	3389 (MS RDP)	*	none		NAT Remote Desktop SANSRV	
<input checked="" type="checkbox"/> 0/0 B	IPv4 TCP	*	*	WEBSRV	3389 (MS RDP)	*	none		NAT Remote Desktop WEBSRV	
<input checked="" type="checkbox"/> 0/0 B	IPv4 TCP	*	*	BDSRV	3389 (MS RDP)	*	none		NAT Remote Desktop BDSRV	
<input checked="" type="checkbox"/> 0/0 B	IPv4 TCP	*	*	CLIENT	3389 (MS RDP)	*	none		NAT Remote Desktop CLIENT	

Figure 27. Règles appliquées pour le WAN

Rules (Drag to Change Order)										
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	
<input checked="" type="checkbox"/> 0/0 B	*	*	*	LAN Address	50001	*	*		Anti-Lockout Rule	
<input checked="" type="checkbox"/> 4/156.88 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input checked="" type="checkbox"/> 0/0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Figure 28. Règles appliquées pour le LAN

3.5. Gestion du Content Delivery Network

Le Content Delivery Network (CDN) est recommandé lorsqu'on met en place des sites internet. Son but : rediriger la requête du client vers un serveur le plus proche de chez lui lorsqu'il veut accéder à notre site internet. En quelque sorte, le serveur contient une copie en cache des éléments statiques (image, vidéo, texte...). Ce serveur communique avec le serveur dit « origine » qui contient, tous les éléments du site internet y compris ceux dynamiques (connexion à une base de données...). Dès qu'un changement au niveau statistique est modifié, le serveur « origine » envoie aux autres serveurs CDN répartis dans le monde, une copie de ses données. En faisant cela, nous permettons au client de se connecter plus rapidement au site internet et donc de gagner du temps.

Par rapport à notre infrastructure, nous n'avons pas su trouver une solution adéquate pour mettre en place un CDN. Toutefois, cela reste comme une amélioration possible.

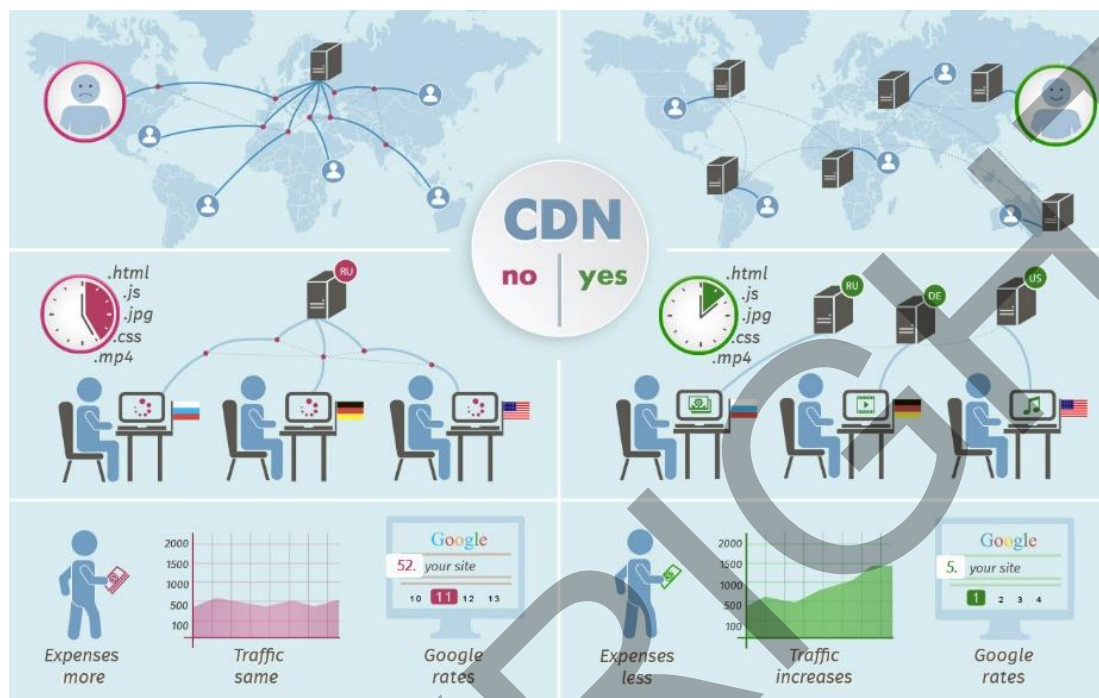


Figure 29. Différence entre une architecture avec et sans CDN

Conclusion

Au travers de ce rapport, nous avons pu voir que mettre en place une infrastructure pour TrainCommander pouvait paraître simple au premier abord, mais reste en fait assez complexe. En effet, il faut bien définir avec l'équipe de développeur, les ressources auxquelles ils auront besoin. Dans notre cas, l'application tourne avec le Framework ASP.NET et une base de données SQL Server. Il était plus approprié de s'orienter vers une architecture Microsoft plutôt que Linux.

Le choix de la virtualisation de nos serveurs est primordial. D'un côté, cela permet d'économiser des ressources matérielles et d'un autre côté, nous pouvons gérer les pannes avec la mise en place d'un cluster à basculement et une baie de stockage SAN externe. Notons aussi l'importance de faire des sauvegardes des machines virtuelles sous forme de snapshots.

La mise en place d'un pare-feu est important étant donné qu'il permet de rendre l'infrastructure plus résistante en cas d'attaque depuis l'extérieur.

Notons que cette infrastructure sera présentée le jour de la démonstration. Cependant, si nous avions eu plus de ressources (financières), nous nous serions orientés vers l'externalisation des serveurs (cloud), une solution moins coûteuse et plus sûre pour l'avenir.

Vous trouverez en annexe 3, le coût de l'architecture réseau (hors main d'œuvre).

Bibliographie

<http://www.mailinblack.com/wp-content/themes/mib/images/logo.png>

http://www.pulsar-informatique.com/images/easyblog_images/155/o365-logo.jpg

<https://fr.wikipedia.org/wiki/Hyperviseur#/media/File:Hyperviseur.png>

<http://ahcdn.com/images/info-cdn-en.jpg>

COPYRIGHT

Table des illustrations

FIGURE 1. SCHEMA DE L'INFRASTRUCTURE	3
FIGURE 2. TABLEAU RECAPITULATIF DE L'INFRASTRUCTURE RESEAU (EN BLEU : LES SERVEURS VIRTUALISES ; EN VERT : LES SERVEURS PHYSIQUES)	4
FIGURE 3. DISQUES DURS (DATASRV & SAVEVM) EN RAID 1	6
FIGURE 4. PRESENTATION DES DISQUES DURS ISCSI	6
FIGURE 5. RECHERCHE DE TOUTES LES TARGET DISPONIBLES SUR LE SANSRV	7
FIGURE 6. CONNEXION AUX TARGET PERMETTANT DE RECUPERER LES DISQUES DURS VIRTUELS ISCSI	7
FIGURE 7. NOUVEAUX VOLUMES CREEES	7
FIGURE 8. SCHEMA RECAPITULATIF REPRESENTANT UNE CONNEXION ENTRE UNE TARGET ET UN INITIATOR	8
FIGURE 9. DESCRIPTION DES ONGLETS DANS L'INTERFACE DU CLUSTER	8
FIGURE 10. MACHINES VIRTUELLES PRESENTS SUR CHAQUE HYPERVISEUR	9
FIGURE 11. PROPRIETE D'UNE MACHINE VIRTUELLE	9
FIGURE 12. SIMULATION D'UNE PANNE SUR LE SERVEUR HYPERVSRV2	10
FIGURE 13. LE SERVEUR HYPERVSRV1 RECUPERE LES VM DE HYPERVSRV2	10
FIGURE 14. LE SERVEUR HYPERVSRV2 NE POSSEDE PLUS DE VM	10
FIGURE 15. LISTES DES DISQUES DURS UTILISES PAR LES VM (1 DISQUE DUR = 1 VM SAUF POUR LE QUORUM ET SAVEVM)	11
FIGURE 16. DIFFERENCES ENTRE LES TYPES D'HYPERVISEURS	12
FIGURE 17. GESTIONNAIRE DE L'HYPER-V (ICI SUR HYPERVSRV1)	12
FIGURE 18. INTERFACE ACTIVE DIRECTORY USERS AND COMPUTERS	13
FIGURE 19. ZONES PRESENTS DANS LE SERVEUR DNS	13
FIGURE 20. ZONES DU SERVEUR DNS (EN HAUT : "TRAINCOMMANDER.LOCAL"; EN BAS : "TRAINCOMMANDER.COM")	14
FIGURE 21. INTERFACE D'ADMINISTRATION IIS PERMETTANT LA GESTION DES SITES INTERNET	15
FIGURE 22. PROPRIETES DES DEUX SITES	15
FIGURE 23. CONNEXION AU SERVEUR SQL SERVER 2014 EN LOCAL (A GAUCHE) ET DEPUIS L'EXTERIEUR (A DROITE)	16
FIGURE 24. ADMINISTRATION DE LA BASE DE DONNEES	17
FIGURE 25. SITE INTERNET DEPUIS UN NAVIGATEUR WEB EN LOCAL	17
FIGURE 26. TABLEAU D'ALIASES CORRESPONDANT A UNE MACHINE SPECIFIQUE	18
FIGURE 27. REGLES APPLIQUEES POUR LE WAN	19
FIGURE 28. REGLES APPLIQUEES POUR LE LAN	19
FIGURE 29. DIFFERENCE ENTRE UNE ARCHITECTURE AVEC ET SANS CDN	20

Annexes

ANNEXE 1 : GLOSSAIRE	25
ANNEXE 2 : LEXIQUE	26
ANNEXE 3 : COUT DE L'HEBERGEMENT DE L'INFRASTRUCTURE PHYSIQUE CHEZ LE CLIENT VS L'HEBERGEMENT SUR LE CLOUD (POUR 3 ANS).....	27

COPYRIGHT

Annexe 1 : glossaire

IP : Internet Protocol, protocole utilisé pour les adresses IP.

LAN : Local Area Network, réseau local .

WAN : Wide Area Network, réseau Internet.

iSCSI : Internet Small Computer System Interface, protocole de stockage en réseau basé sur le protocole IP.

OS : Operating System (Système d'exploitation), par exemple Microsoft Windows 10.

GPO : Group Policy Object, permettent de configurer des restrictions d'utilisation de Windows où des paramètres à appliquer soit sur un ordinateur donné soit sur un compte utilisateur donné.

DNS : Domain Name System, permet de faire pointer un nom vers une adresse IP.

API : Application Programming Interface, est un ensemble normalisé de classes, méthodes et de fonctions qui sert de façade pour laquelle un logiciel offre des services à d'autres logiciels.

C# : Langage de programmation orienté objet.

AngularJS : Framework JavaScript libre et open-source développé par Google.

SQL : Structured Query Language, permet de requêter une base de données à l'aide de requêtes.

URL : Uniform Resource Locator, adresse web.

Annexe 2 : Lexique

Adresse IP : numéro unique permettant à un ordinateur de communiquer dans un réseau. Elle est représentée sous la forme suivante : xxx.xxx.xxx.xxx (avec xxx un nombre compris entre 0 et 255). Existe en norme IPv4 et v6.

RAID1 : Redundant Array of Independent Disks, un RAID1 correspond à deux disques en miroir.

Target : périphérique qui reçoit et traite les commandes.

Initiator : composant logiciel côté serveur, comportant un pilote permettant de gérer et transporter les blocs de commandes sur le réseau IP.

Multi-path : permet à plusieurs PC d'accéder à la même ressource en même temps.

Machine virtuelle : illusion d'un appareil informatique créée par un logiciel d'émulation.

Cluster : grappe de serveurs sur un réseau.

Forêt : regroupement d'une ou plusieurs arborescences de domaine, autrement dit d'un ou plusieurs arbres.

Domaine : définit un ensemble de machines partageant des informations annuaire.

Annuaire Active Directory : permet de gérer les ressources du réseau : données utilisateur, imprimantes, serveurs, bases de données, groupe, ordinateurs et stratégies de sécurité.

Back-end : terme désignant un étage de sortie d'un logiciel devant produire un résultat.

Front-end : correspond à la partie visible et accessible par l'utilisateur.

Port logiciel : permet de recevoir ou d'émettre des informations.

Snapshot : capture de l'état d'un système à un instant donné.

Annexe 3 : Coût de l'hébergement de l'infrastructure physique chez le client vs l'hébergement sur le cloud (pour 3 ans)

Infrastructure physique chez le client :

Catégorie	Description	Quantité	PU HT	Remise	Total HT	Taxe	Total TTC
Serveur	DELL Serveur rack PowerEdge R630	2	8 291,00 €	3 233,49 €	13 348,51 €	20%	16 018,21 €
Onduleur	Dell Smart-UPS 8000VA	1	4 685,52 €		4 685,52 €	20%	5 622,62 €
	Multiprise 3 prises pour onduleur	6	5,52 €		33,12 €	20%	39,74 €
OS	Windows 2012 R2 Datacenter	2	4 374,96 €		8 749,92 €	20%	10 499,90 €
	Windows 2012 R2 Standard	3	666,63 €		1 999,89 €	20%	2 399,87 €
	SQL Server 2014 Standard	1	3 280,38 €		3 280,38 €	20%	3 936,46 €
	Windows 10 Pro	1	149,96 €		149,96 €	20%	179,95 €
KVM	Alten CL1000	1	649,96 €		649,96 €	20%	779,95 €
RACK	Armoire Rack 42U Dell powerRack 4210	1	790,00 €		790,00 €	20%	948,00 €
Sécurité	Netasq Appliance / Firewall U70S	2	1 150,00 €		2 300,00 €	20%	2 760,00 €
	Kaspersky Endpoint Security for Business - Advanced (10 postes) - Licence 1 an	3	790,00 €		2 370,00 €	20%	2 844,00 €
Stockage	DELL Powervault MD3420	1	11 841,00 €	5 091,63 €	6 749,37 €	20%	8 099,24 €
	SYNOLOGY DS916+	1	480,79 €		480,79 €	20%	576,95 €
	WD Red 1 To SATA 6Gb/s	4	63,96 €		255,84 €	20%	307,01 €
Switch	CISCO SMALL BUSINESS SG350XG-2F10	4	1 449,96 €		5 799,84 €	20%	6 959,81 €

Total HT	51 643,10 €
Total TTC	61 971,72 €

Cloud :

Catégorie	Description	Quantité	PU HT	Remise	Total HT	Taxe	Total TTC
Serveurs	Serveur Enterprise MG-128 - 128G 2xE5-2630v3 - 12 mois	3	2 603,88 €		7 811,64 €	20%	9 373,97 €
OS	Windows 2012 R2 Datacenter - 1 mois	36	259,98 €		9 359,28 €	20%	11 231,14 €
	Windows 2012 R2 Standard - 1 mois	72	39,98 €		2 878,56 €	20%	3 454,27 €
	SQL Server 2014 Standard - 1 mois	36	320,00 €		11 520,00 €	20%	13 824,00 €
	Windows 10 Pro - OEM	1	149,96 €		149,96 €	20%	179,95 €
CDN	CDN - 1 mois	36	9,99 €		359,64 €	20%	431,57 €

Total HT	32 079,08 €
Total TTC	38 494,90 €

Nous constatons qu'il y a une différence de 19 564,02 € HT soit **23 476,82€** TTC. Il est donc plus rentable de prendre l'hébergement sur le cloud.

Cette différence s'explique par le fait que tout ce qui est externe aux serveurs (onduleur, switch, pare-feu, électricité, climatisation, salle dédiée...) est directement géré par l'hébergeur.