Editions ENI

VMware View

Virtualisation des postes de travail

(architecture, déploiement, bonnes pratiques...)

Collection
Expert IT

Extrait

L'utilisation sur des réseaux étendus comme le WAN (*Wide Area Network*) se fera à travers du protocole d'affichage PCoIP uniquement, afin de fonctionner de manière plus optimale sur des latences élevées ainsi que sur une bande passante plus étroite, tout en proposant un poste de travail virtuel de bonne qualité.

Afin de faire fonctionner ces deux modes d'utilisation de manière sécurisée, il faudra dans un premier temps configurer le VMware View Connection Server afin d'éviter les attaques directes. Le VMware View Connection Server est un composant fondamental dans l'infrastructure VMware View, d'une part car c'est le point névralgique des connexions entre les clients VMware View et les postes virtuels, mais aussi car c'est un composant rattaché à l'Active Directory. Il est donc conseillé de placer le VMware View Connection Server dans une zone sécurisée afin de ne pas exposer les données de l'Active Directory à d'éventuelles failles de sécurité.

Pour garantir un bon niveau de sécurité, il est recommandé d'utiliser le composant VMware View Security Server afin que les utilisateurs se connectent non plus directement sur le VMware View Connection Server mais par le biais du View Security Server.

Comme tout serveur de sécurité, il sera conseillé de placer l'instance View Security dans un réseau séparé du View Connection Server et de l'Active Directory afin de ne pas compromettre l'intégrité des données.

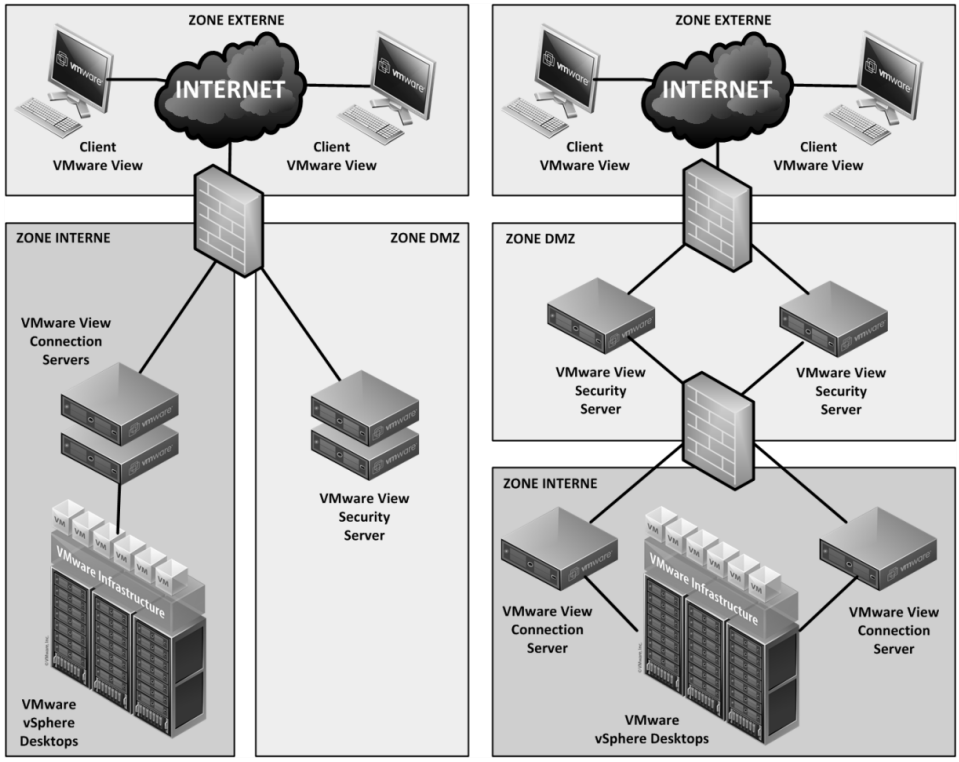
2. Configurations réseau conseillées

Il sera donc recommandé de placer le View Security Server dans une zone réseau DMZ (zone démilitarisée) afin de fournir l'accès Internet uniquement dans cette zone sécurisée et non sur le réseau interne de l'entreprise.

L'avantage de la zone démilitarisée est qu'au cas où un serveur serait attaqué dans celle-ci, le pirate n'aurait accès qu'aux serveurs de cette zone et non au réseau local comprenant les serveurs de domaine ainsi que les machines virtuelles VMware View et donc les données des utilisateurs.

Les VMware View Security Servers n'ont pas besoin d'être connectés au domaine Active Directory et peuvent donc être placés dans un réseau séparé des View Connection Servers.

Il existe plusieurs formes de zones DMZ, dont voici les deux plus répandues :



La configuration de gauche présente une DMZ avec un seul firewall ayant trois connexions réseau vers Internet (zone externe), vers le réseau interne ainsi que vers la zone DMZ. La configuration de droite est aussi composée de trois zones mais délimitées par deux firewall.

Remarque

Il est conseillé d'utiliser la configuration DMZ avec deux firewall afin de garantir un niveau de sécurité plus avancé dans le cas où le firewall utilisé pour sécuriser la zone DMZ serait attaqué.

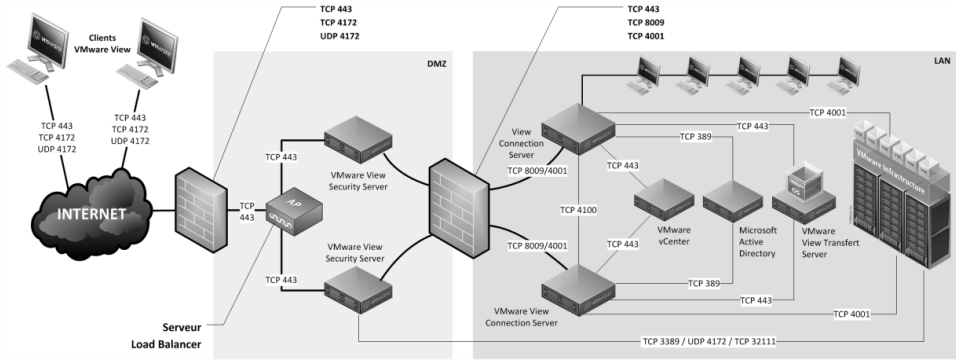
Contrairement au VMware View Connection Server, le Security Server peut supporter deux cartes réseau afin de mettre en place la configuration DMZ de droite. Le VMware View Security Server pourra donc être attaché d'un coté au réseau DMZ et de l'autre au réseau interne, le tout sécurisé par deux firewall sur chaque extrémité.

Les utilisateurs initiant des connexions dans le réseau local de l'entreprise peuvent se connecter sur n'importe quel VMware View Connection Server.

Il n'est donc pas nécessaire d'implémenter de serveur de sécurité pour les utilisateurs internes, par contre il est recommandé d'activer le tunnel SSL vers le View Connection Server pour les utilisateurs souhaitant se connecter sur le réseau local de l'entreprise.

2.1 Règles de firewall conseillées

Si vous souhaitez configurer votre infrastructure VMware View en mode DMZ avec deux types de firewall il faudra alors ouvrir certains ports TCP entre les différentes zones afin d'établir les connexions entre les différents composants VMware View, comme détaillé sur le schéma ci-dessous :



En partant de la gauche, le premier pare-feu rencontré est communément appelé le pare-feu frontal, sur lequel doivent être mises en place les règles suivantes :

– Tout le trafic sur le port TCP 443 doit être autorisé et redirigé vers le VMware View Security Server. Les clients VMware View venant de l'extérieur devront utiliser le port 443 pour se connecter au serveur VMware View Security Server placé dans la zone DMZ.
– Tout le trafic sur le port TCP 4172 devra aussi être redirigé vers le VMware View Security Server. Une fois le tunnel SSL monté, comme expliqué précédemment les clients VMware View initieront une connexion sur leurs postes de travail View via le port TCP 4172 qui sera utilisé pour crypter le signal PCoIP.
– Tout le trafic sur le port UDP 4172 devra aussi être redirigé vers le VMware View Security Server. Une fois le tunnel SSL monté, comme expliqué précédemment les clients VMware View initieront une connexion sur leurs postes de travail View via le port UDP 4172 correspondant au protocole d'affichage PCoIP. Il faudra aussi créer une règle pour accepter le trafic en sortie sur le port UDP 4172 car certaines connexions PCoIP émaneront directement de la machine virtuelle sans avoir reçu de demandes.

Concernant le deuxième pare-feu, aussi appelé pare-feu interne, il faudra activer les règles suivantes :

– Tout le trafic sur le port TCP 8009 doit être autorisé et redirigé vers le VMware View Connection Server. Ce port sera utilisé pour initier les communications entre le VMware View Security Server et le VMware View Connection Server en utilisant un trafic web.
– Tout le trafic sur le port TCP 4001 doit être autorisé et redirigé vers le VMware View Connection Server. Ce port sera utilisé pour la communication entre le VMware View Security Server et le VMware View Connection Server au travers de requêtes JMS (*Java Message Service*).
– Tout le trafic sur le port TCP 4172 devra aussi être redirigé vers le VMware View Security Server. Une fois le tunnel SSL monté, comme expliqué précédemment, les clients VMware View initieront une connexion sur leurs postes de travail View via le port TCP 4172 qui sera utilisé pour crypter le signal PCoIP.

– Tout le trafic sur le port UDP 4172 devra aussi être redirigé vers le VMware View Security Server. Une fois le tunnel SSL monté, comme expliqué précédemment, les clients VMware View initieront une connexion sur leurs postes de travail View via le port UDP 4172 correspondant au protocole d'affichage PCoIP. Il faudra aussi créer une règle pour accepter le trafic en sortie sur le port UDP 4172 car certaines connexions PCoIP émaneront directement de la machine virtuelle sans avoir reçu de demandes.

– OPTIONNEL : tout le trafic sur le port TCP 443 doit être autorisé et redirigé vers le VMware View Transfer Server si vous avez précédemment activé l'option de sécurité sur le serveur View Transfer afin que les téléchargements des images virtuelles en vue d'une utilisation en mode déconnecté soient possibles.

– OPTIONNEL : tout le trafic sur le port TCP 9427 doit être autorisé et redirigé vers le VMware View Connection Server si vous avez précédemment activé l'option de redirection multimédia sur le serveur View Connection afin d'autoriser la redirection de Flash ou de vidéos Media Player. Cette fonctionnalité de redirection multimédia n'est valable que si vous utilisez le protocole Microsoft RDP.

– OPTIONNEL : tout le trafic sur le port TCP 32111 doit être autorisé et redirigé vers le VMware View Connection Server si vous avez précédemment activé l'option de redirection USB sur le serveur View Connection afin d'autoriser la redirection de certains périphériques USB du poste VMware View vers le client View. Cette fonctionnalité de redirection USB est valable si vous utilisez le protocole Microsoft RDP ou le PCoIP.

– L'ensemble des VMware View Connection Server utilisent le port TCP 4100 afin de communiquer et de se synchroniser. De même, si vous utilisez des VMware View Replica Server, le port TCP 4100 sera utilisé afin de répliquer les données.

Le trafic de routage JMS (JMSIR) sera placé sur le port TCP 4100 entre les instances. Du fait que les VMware View Connection Server ne sont pas délimités par des pare-feu, aucune règle supplémentaire n'est nécessaire.

3. Installation du VMware View Security Server

3.1 Pré-requis matériels et logiciels

Avant de procéder à l'installation, la configuration et l'optimisation du serveur VMware View Security Server, il est important de connaître les pré-requis matériels et logiciels.

Tout d'abord, VMware View Security Server peut être installé aussi bien sur une machine virtuelle que sur un serveur physique.

Si vous avez très peu de serveurs dans votre réseau DMZ le mieux serait d'installer le composant VMware View Security Server sur un serveur physique.

Le View Security Server ne doit pas être intégré si possible dans le domaine Microsoft Active Directory afin de sécuriser les données LDAP.

VMware recommande l'utilisation de deux processeurs ayant une fréquence minimum de 2 GHz et dotés de 2 Go de mémoire dans le cas d'un système 32 bits et 4 Go pour un système 64 bits. Il est aussi recommandé pour des raisons de performance que le serveur ait une carte réseau de 10/100 Mbps minimum.

VMware View Security Server peut être installé sur les systèmes d'exploitation suivants :

– Windows Server 2008 R2 Editions, 64 bits

– Windows Server 2003 R2 Editions with SP2, 32 bits

– Windows Server 2003 Editions with SP2, 32 bits

Remarque

Il est recommandé d'installer le composant VMware View Connection Server sur un système d'exploitation 64 bits installé avec le pack de langue Anglais ou alors d'installer ce pack de langue si le système a été installé via un média d'installation en langue française.

Editions ENI

VMware vSphere 5

au sein du Datacenter

(2ième édition)

Collection
Expert IT

Extrait

Exemples

Pour un RPO de 24 heures, une sauvegarde journalière est la technique généralement utilisée. Pour un RPO de quelques heures, les techniques employées sont les snapshots ou la réplication asynchrone. Un RPO de 0 implique la mise en place d'un mode de réplication synchrone et correspond à une demande 'aucune perte de données'.

– Le **RTO** (*Recovery Time Objective*) correspond à la durée maximale d'interruption admissible. Le temps de redémarrage des applicatifs et leur mise en service détermine le RTO.

Exemples

Pour un RTO de 48 heures, il est possible d'utiliser des bandes situées sur un site distant protégé. Pour un RTO de 24 heures, la restauration à partir de bandes sur un site local peut être utilisée. Pour un RTO de 4 heures ou moins plusieurs techniques complémentaires doivent être mises en place : Clustering, réplication, techniques propres à VMware HA, FT, SRM, virtualisation du stockage...

La virtualisation simplifie certains process permettant d'atteindre des RTO réduits. Le RTO est fonction des techniques mises en place et dépend fortement du redémarrage des applications et de leur **consistance applicative** lorsque des arrêts brutaux surviennent sur le site de production. Si celle-ci n'est pas garantie, le RTO est variable et est difficilement prévisible.

Bien évidemment, toute entreprise souhaiterait pouvoir disposer de solutions permettant de ne perdre aucune donnée avec une remise en production la plus rapide possible en cas de problème. Mais il n'y a pas de secret, plus les temps de RPO et RTO sont faibles et plus la mise en place de telles solutions est coûteuse. **Il est donc fondamental d'engager les responsables et dirigeants afin de déterminer avec eux, les RTO et RPO qu'ils souhaitent en fonction des contraintes métiers et business**. On parle également de **BIA** (*Business Impact Analysis*) qui permet de quantifier la valeur réelle d'une donnée pour l'entreprise. Il n'est pas rare d'avoir trop d'investissement sur la protection des mauvaises données (importantes pour l'administrateur mais pas forcément pour l'entreprise) et pas assez sur les bonnes. Une décision collégiale est à privilégier pour valider ensemble les risques encourus en fonction des solutions choisies.

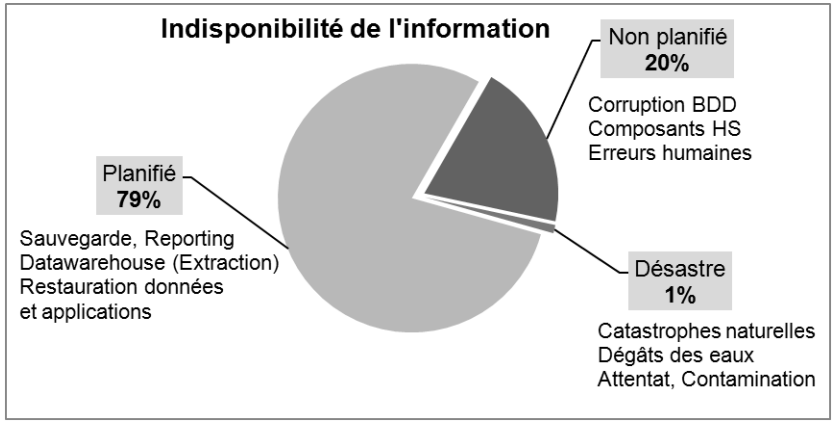
Le **SLA** (*Service Level Agreement*) est un contrat spécifiant des niveaux de services. Il s'agit d'un engagement formel et contraignant, établi entre un prestataire et son client. Les notions de RTO et RPO sont importantes lorsque ce contrat s'établit.

1.2 La disponibilité de l'information

Remarque

***Statistiques** : 93 % des entreprises ayant perdu leur Datacenter pendant dix jours ou plus à la suite d'une panne majeure ont fait faillite dans l'année suivante (NARA : National Archives and Records Administration).*

Le système d'information est essentiel pour une entreprise. Celui-ci permet aux utilisateurs d'être productifs et de disposer de moyens de communication efficaces tels que l'usage d'une messagerie, d'outils collaboratifs, réseaux sociaux… Pour l'entreprise le système d'information fournit les applications métiers pour accompagner le Business. Une indisponibilité même partielle de tel ou tel service peut faire perdre beaucoup d'argent à une entreprise. Il est donc crucial de mettre en place des dispositifs qui réduisent les interruptions de service et de pouvoir remettre le système en fonctionnement en cas d'incidents majeurs survenant sur le site de production.



Causes de l'indisponibilité de l'information généralement constatées.

Comme on peut le constater sur ce graphique, la plus grande part du temps d'indisponibilité (79 % du temps) vient de maintenances planifiées pour des opérations de sauvegarde, rajout de matériel, migration, extraction de données (Datawarehouse) qui sont donc prévisibles mais qui peuvent provoquer malgré tout des indisponibilités de service. Les autres types d'indisponibilité concernent des événements imprévisibles qui ne peuvent être anticipés dont les conséquences peuvent être dramatiques si des mesures et procédures fiables ne sont pas mises en place.

La disponibilité de l'information est établie selon le calcul suivant :

IA = MTBF / (MTBF + MTTR)

IA (*Information Availability*) : disponibilité de l'information.

MTBF (*Mean Time Between Failure*) : temps moyen pour un système ou un composant avant de tomber en panne.

MTTR (*Mean Time To Repair*) : temps moyen pour réparer un composant HS. MTTR inclut le temps passé à détecter le composant HS, planifier l'intervention d'un technicien, diagnostiquer le composant, obtenir le composant de remplacement (Spare) puis réparer et remettre en production le système.

La disponibilité de l'information se mesure en pourcentage, en nombre de 9 et permet de répondre aux besoins métiers pour une durée déterminée. Plus le nombre de 9 est élevé et plus la disponibilité est haute. On parle généralement de Haute Disponibilité à partir de 99,999 %.

Voici un tableau de correspondance entre la disponibilité (en nombre de 9) et le temps d'indisponibilité que cela représente.

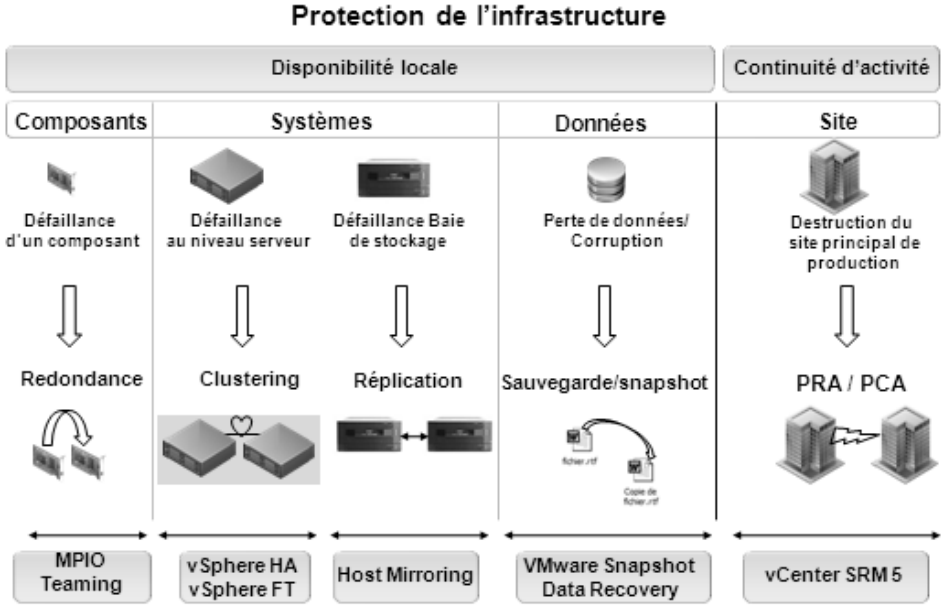
Pourcentage de disponibilité	Temps d'indisponibilité
98 %	7,3 jours
99 %	3,65 jours
99,80 %	17 hrs 31 min
99,90 %	8 hrs 45 min
99,99 %	52,5 min
99,999 %	5,25 min
99,9999 %	31,5 sec

Remarque

Un système ayant une disponibilité de 99,999 représente 5,25 minutes maximum d'arrêt par an. À noter que cette durée est très courte puisqu'elle représente moins que le temps de reboot d'un serveur physique !

1.3 Protection de l'infrastructure

La protection du système d'information peut être classée en deux catégories : la **disponibilité locale** sur un site et la **continuité d'activité** lorsqu'un incident majeur survient sur le site de production.



– La **disponibilité locale** a pour objet de supprimer les interruptions de service lorsqu'un composant tombe en panne, grâce à :
  – La mise en place de redondance **matérielle** pour éliminer les SPOF (*Single Point of Failure*).
  – La mise en place de systèmes de clustering pour remettre rapidement en production des **applications** en cas de crash de serveurs.

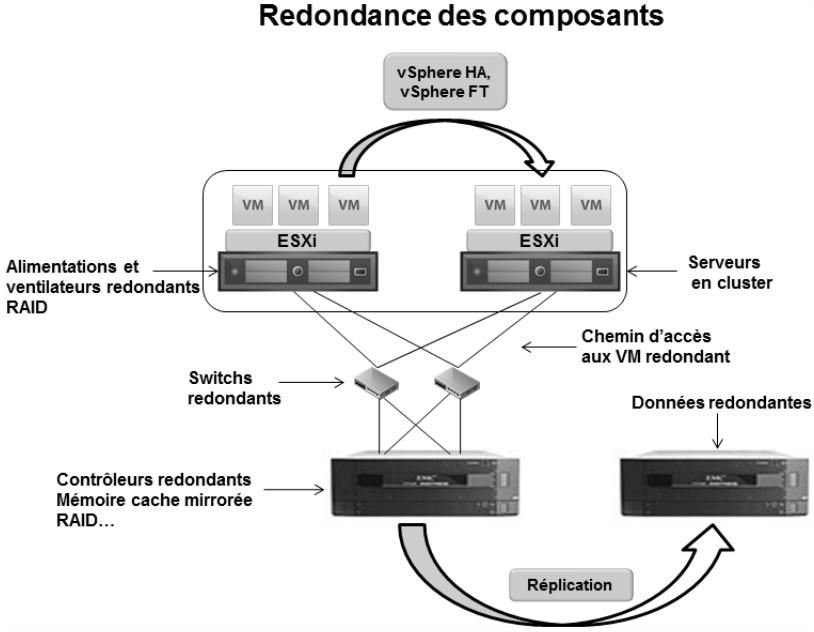
  - La sécurisation des **données** au travers de sauvegarde pour faire face à la perte de données ou à des mécanismes de réplication pour faire face à la perte d'une baie de stockage.
  - La mise en place de snapshots pour un retour arrière rapide vers un état sain lorsqu'un **applicatif est corrompu**.
- La **continuité d'activité** a pour objet de remettre en fonctionnement rapidement un site de production lorsqu'un événement majeur survient. Les notions de **PRA** (Plan de Reprise d'Activité), **PCA** (Plan de Continuité d'Activité) ou **PSI** (Plan de Secours Informatique) sur un site de secours permettent de faire face à ces événements survenant au niveau du Datacenter de production.

La sauvegarde faisant partie intégrante de la protection et étant un sujet important à traiter, un chapitre lui est consacré.

2. La disponibilité locale

2.1 Suppression de SPOF (Single Point of Failure)

La virtualisation de l'infrastructure engendre une consolidation sur un nombre réduit d'équipements. Ces équipements hébergeant un nombre important de VM, ils deviennent donc hautement critiques. Un arrêt d'un seul de ces équipements peut engendrer une interruption de plusieurs VM dont les conséquences pour le système d'information peuvent être dramatiques. Un **SPOF** représente un composant qui peut rendre indisponible le système d'information s'il tombe en panne. Plusieurs techniques permettent de se prémunir contre cette éventualité en mettant en place de la redondance matérielle. En environnement virtualisé, les bonnes pratiques préconisent de redonder tous les éléments matériels afin de réduire les interruptions de service.



Techniques permettant de supprimer les SPOF.

Les **disques durs** sont les composants les plus importants à protéger car ils contiennent les données et ils sont sollicités en permanence. Pour pallier des pannes de disques durs, il faut mettre des cartes **RAID**.

Les alimentations et ventilateurs sont susceptibles de chauffer et de tomber en panne. Pour pallier ces problèmes, il faut mettre des alimentations et ventilateurs redondants.

La **mémoire** peut être sécurisée grâce à des techniques de mirroring bien que cela soit peu répandu.

Les cartes réseau peuvent être sécurisées en suivant le protocole IEEE 802.3ad permettant d'agréger les liens.

Le processeur et la carte mère ne contiennent pas de mécaniques ils sont donc moins soumis à des dysfonctionnements. Cependant ces composants étant critiques, il est possible de les sécuriser au travers de solutions matérielles comme le **Fault Tolerant** de **NEC** ou **Stratus** dont l'architecture met en redondance la carte mère.