SafeKit
Logiciel de haute disponibilité
Réplication temps réel
Partage de charge
Reprise sur panne

Trusted partner for your **Digital Journey**

Sommaire

Le produit idéal pour un éditeur de logiciel

*« SafeKit est le logiciel de clustering d'application idéal pour un éditeur de logiciel. Nous avons actuellement déployé plus de **100 clusters SafeKit** dans le monde entier avec notre application cri tique de télédiffusion. »*

Le produit très simple à déployer pour un revendeur

*« SafeKit est une solution professionnelle facilitant la redondance du **système de vi-déosurveillance Milestone**. La solution est facile à déployer, facile à maintenir et peut être ajoutée à une installation exis tante. »*

Le produit qui fait gagner du temps à un intégrateur de systèmes

*« Grâce à la simplicité et la puissance du produit, nous avons gagné du temps dans l'intégration et la validation de nos projets critiques de supervision des **lignes de mé-tro à Paris** (PCC / Poste de Commande et de Contrôle). »*

Continuité d'activité, reprise sur sinistre, haute disponibilité

Quelle que soit leur importance, toutes les activités reposant sur un système informatique sont un jour ou l'autre confrontées au problème de la panne informatique. Et malheureusement, le jour où la panne survient, un petit problème peut se transformer en crise généralisée si aucune solution de haute disponibilité n'a été mise en œuvre.

Les 10 raisons de choisir le clustering logiciel SafeKit

1. Solution de haute disponibilité purement logicielle

SafeKit est une solution de haute disponibilité purement logicielle. Cette solution permet de sécuriser de manière simple et rapide le fonctionnement 24x7 de vos applications critiques.

Alors que les solutions de haute disponibilité traditionnelles sont focalisées sur la résistance aux pannes matérielles des serveurs physiques, SafeKit a fait le choix de s'occuper de la résistance aux pannes matérielles et logicielles des applications critiques.

2. Haute disponibilité qui cible toutes les pannes

L'indisponibilité d'une application est aujourd'hui liée à 3 types de problèmes :

- les pannes matérielles et surtout d'environnement du matériel : incluant la panne globale à toute la salle machine (20%) ;
- les pannes logicielles : régression sur évolution logicielle, indisponibilité par surcharge d'un service, bug logiciel (40%) ;
- les erreurs humaines : erreur d'administration et incapacité à redémarrer correctement un service critique (40%).

SafeKit adresse l'ensemble de ces problématiques, toutes essentielles pour la haute disponibilité d'une application critique.

3. Les 3 meilleurs cas d'utilisation de clustering logiciel

Après plus de 20 ans d'expérience dans le 24x7, SafeKit se révèle être la solution de clustering logicielle préférée sur le marché dans trois cas d'utilisation :

1. Un éditeur de logiciel peut ajouter SafeKit à son catalogue comme option logicielle OEM de haute disponibilité et de partage de charge.
2. Une entreprise distribuée peut déployer une solution de haute disponibilité sur du matériel standard sans besoin de compétence informatique spécifique.
3. Un datacenter peut rendre hautement disponibles ses applications avec une solution uniforme sur Windows ou Linux et avec partage de charge, réplication temps réel des données et reprise sur panne entre deux sites distants.

4. Procédé unique sur le marché : 3 produits en 1

Traditionnellement, trois produits différents sont nécessaires pour créer un cluster applicatif :

- les boîtiers réseau pour le partage de charge ;
- les baies de disques répliquées de manière synchrone sur un SAN pour la disponibilité des données ;
- les toolkits de haute disponibilité pour la reprise applicative sur panne.

SafeKit fournit dans le même logiciel les trois fonctions ci-dessus : partage de charge, réplication de donnée et reprise applicative.

Afin de réduire encore les coûts d'implémentation, SafeKit se met en œuvre sur vos serveurs physiques ou virtuels existants et fonctionne avec les éditions standards des OS et des bases de données : Windows, Linux, Microsoft SQL Server, Oracle, Firebird, MariaDB, PostgreSQL ou autres bases ou fichiers plats... et même avec les éditions Windows pour PCs !

5. Une solution adaptée aux environnements Cloud

La haute disponibilité des applications avec SafeKit peut être déployée dans les clouds AWS, Azure et Google ainsi que sur site sur des machines virtuelles ou physiques. La redondance des applications Docker est également supportée.

6. Réplication et reprise de machines virtuelles complètes

SafeKit propose également une réplication et une reprise sur panne de machines virtuelles complètes entre 2 serveurs physiques Hyper-V ou KVM actifs. La solution est simple et économique car elle ne nécessite aucun disque partagé.

7. Déploiement plug&play d'un cluster logiciel

Une fois un module de reprise configuré et testé pour une application, le déploiement d'un cluster logiciel ne nécessite pas de compétence informatique spécifique. Il suffit d'installer l'application, le logiciel SafeKit et le module de reprise sur deux serveurs standards Windows ou Linux .

8. Choix riche d'intégration d'une application dans un cluster logiciel

SafeKit propose plusieurs types de cluster logiciel. La configuration d'un cluster pour une application donnée est très riche et se fait au moyen d'un ou plusieurs modules applicatifs. SafeKit propose des modules miroirs (primaire/secondaire avec réplication et reprise), des modules fermes (partage de charge réseau et reprise), et des mixtes de plusieurs modules qui peuvent se mettre en œuvre sur le même cluster ou sur des clusters différents.

Un module se configure avec les adresses IP des serveurs pour les *« heartbeats »*, l'adresse IP virtuelle du cluster, les règles de partage de charge pour un module ferme, les répertoires de fichiers à répliquer pour un module miroir, les détecteurs de pannes matérielles et logicielles et les services à relancer en cas de panne.

9. Administration simple pour éviter les erreurs humaines

SafeKit fournit une console d'administration web centralisée. Un administrateur peut contrôler à distance l'état de ses applications sur plusieurs clusters et agir avec des boutons simples (start, stop) pour redémarrer l'application sur un autre serveur.

Vous avez la possibilité de tester gratuitement SafeKit. En moins d'1 heure, vous mettez en œuvre votre premier cluster logiciel sur deux machines virtuelles ou physiques grâce la console d'administration web.

10. Réplication synchrone pour les applications transactionnelles

La fonction de réplication synchrone et temps réel de SafeKit vient renforcer les capacités de haute disponibilité et de prévention contre les pertes de données. Avec ce mécanisme, une donnée commitée sur un disque par une application transactionnelle est retrouvée sur la machine secondaire.

Les serveurs applicatifs peuvent être écartés dans des salles machines géographiquement éloignées à travers un LAN étendu afin de résister au sinistre d'une salle complète.

Intégration – Déploiement - Architectures

Intégration via un module applicatif

Un module applicatif est une personnalisation de SafeKit pour une application. Il existe deux types de module : le module miroir avec réplication temps réel de données et reprise sur panne et le module ferme avec partage de charge et reprise sur panne.

Concrètement, un module applicatif est un fichier « .safe » de type zip incluant :

1. le fichier de configuration userconfig.xml qui contient :
   - les noms ou les adresses IP physiques des serveurs ;
   - le nom ou l'adresse IP virtuelle du cluster ;
   - les répertoires de fichiers à répliquer en temps réel (pour un module miroir) ;
   - les critères de partage de charge (pour un module ferme) ;
   - la configuration des détecteurs de pannes logicielles et matérielles.
2. les scripts de démarrage et d'arrêt de l'application.

Déploiement plug&play

Une fois un module applicatif configuré et testé, le déploiement ne nécessite pas de compétence informatique spécifique. Il faut :

1. Installer l'application sur 2 serveurs standards (physiques ou virtuels).
2. Installer le logiciel SafeKit sur les 2 serveurs.
3. Installer le module applicatif sur les 2 serveurs.

Architectures : les différents types de cluster

SafeKit offre deux clusters de base :

- le cluster miroir construit en déployant un module applicatif miroir sur 2 serveurs ;
- le cluster ferme construit en déployant un module applicatif ferme sur 2 serveurs ou plus.

Plusieurs modules applicatifs peuvent être déployés dans le même cluster. Ainsi, des architectures de clustering avancées peuvent être mises en œuvre :

- un cluster qui mixte ferme et miroir avec le déploiement d'un module ferme et d'un module miroir dans le même cluster ;
- un cluster actif/actif avec le déploiement de plusieurs modules miroirs sur 2 serveurs ;
- un cluster Hyper-V ou KVM avec réplication et reprise de machines virtuelles complètes entre 2 serveurs physiques actifs ;
- un cluster N-1 avec le déploiement de N modules miroirs sur N+1 serveurs.

Le cluster miroir de SafeKit

Haute disponibilité avec réplication temps réel de fichiers et reprise applicative sur panne

Le cluster logiciel miroir est une solution de haute disponibilité applicative de type primaire - secours. L'application est exécutée sur un serveur primaire et redémarrée automatiquement sur un serveur de secours si le serveur primaire est défaillant.

Le cluster miroir peut être configurée avec ou sans réplication de fichiers. Avec la réplication de fichiers, ce cluster est particulièrement adapté à la haute disponibilité des applications base de données avec des données critiques à protéger contre les pannes.

Microsoft SQL Server.safe, PostgreSQL.safe, Oracle.safe sont des exemples de modules applicatifs de type « miroir ». Vous pouvez écrire votre propre module miroir pour votre application à partir du module générique Mirror.safe.

Une démonstration d'un cluster miroir avec Microsoft SQL Server est présentée ici.

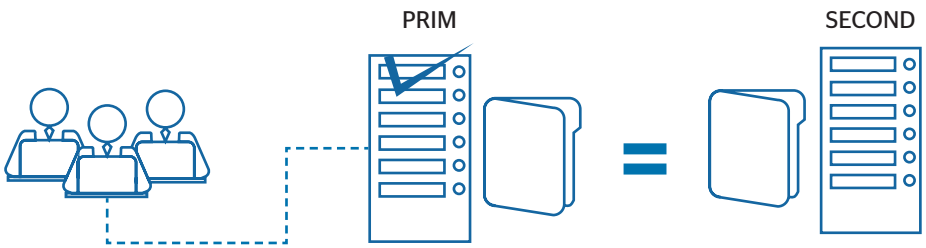
Le système de reprise d'un cluster logiciel miroir fonctionne de la façon suivante.

Etape 1. Etat normal d'un miroir

Seuls les noms des répertoires de fichiers à répliquer sont configurés dans SafeKit. Il n'y a pas de pré-requis sur l'organisation disque des deux serveurs. Les répertoires à répliquer peuvent être localisés dans le disque système.

Le serveur 1 (PRIM) exécute l'application.

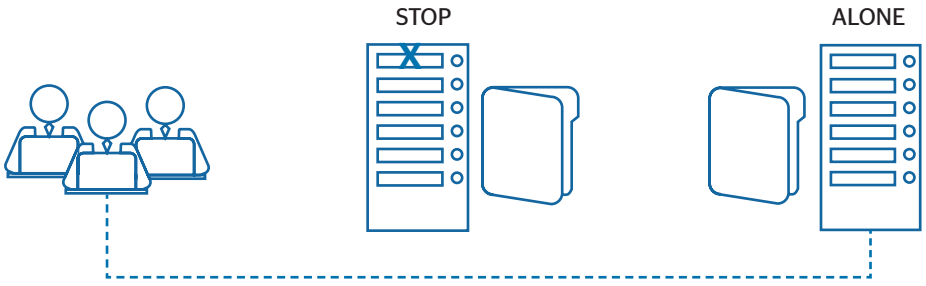
SafeKit réplique les fichiers ouverts par l'application. Seules les modifications faites par l'application à l'intérieur des fichiers sont répliquées en temps réel à travers le réseau limitant ainsi le trafic.



Etape 2. Reprise sur panne

Lorsque le serveur 1 est défaillant, SafeKit bascule l'adresse IP virtuelle du cluster sur le serveur 2 et redémarre automatiquement l'application. L'application retrouve les fichiers répliqués à jour grâce à la réplication synchrone réalisée par SafeKit entre le serveur 1 et le serveur 2. L'application continue son exécution sur le serveur 2 en modifiant localement ses fichiers qui ne sont plus répliqués vers le serveur 1.

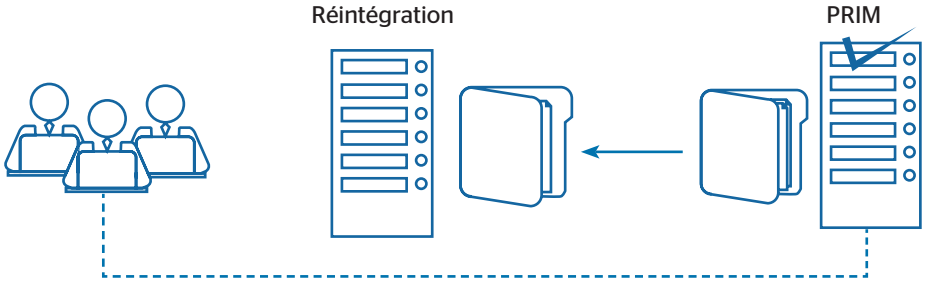
Le temps de basculement est égal au temps de détection de la panne (time-out configuré à 30 secondes par défaut) et au temps de relance de l'application. Sur la machine secondaire, il n'y a pas de temps lié au remontage du système de fichiers ou au passage des procédures de recovery du système de fichiers, comme avec les solutions de réplication de disques.



Etape 3. Réintégration après panne

A la reprise après panne du serveur 1 (réintégration du serveur 1), SafeKit resynchronise automatiquement les fichiers de ce serveur à partir de l'autre serveur. Seuls les fichiers modifiés sur le serveur 2 pendant l'inactivité du serveur 1 sont resynchronisés.

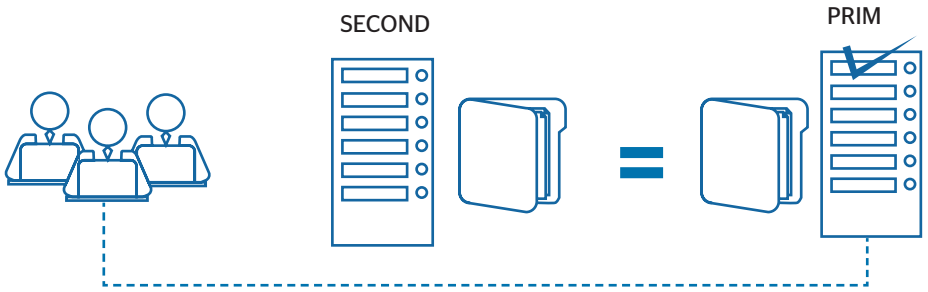
La réintégration du serveur 1 se fait sans arrêter l'exécution des applications sur le serveur 2. Cette propriété est un gros différentiateur du produit SafeKit par rapport à d'autres solutions qui nécessitent d'arrêter les applications sur le serveur 2 pour réintégrer le serveur 1.



Etape 4. Retour à la normale

Après la réintégration, les fichiers sont à nouveau en mode miroir comme à l'étape 1. Le système est en haute disponibilité avec l'application qui s'exécute sur le serveur 2 et avec comme secours le serveur 1. Les modifications de l'application dans les fichiers sont répliquées en temps réel du serveur 2 vers le serveur 1.

Si l'administrateur souhaite que son application s'exécute en priorité sur le serveur 1, il peut exécuter une commande de basculement, soit manuellement à un moment opportun, soit automatiquement. par configuration.



Solution de réplication synchrone versus réplication asynchrone

Il existe une grande différence entre réplication synchrone de données mise en œuvre par la solution miroir de SafeKit et réplication asynchrone de données telle qu'elle est traditionnellement mise en œuvre dans les solutions de réplication de fichiers.

Avec une réplication synchrone, lorsqu'une IO disque est réalisée par l'application ou le cache système sur le serveur primaire et sur un fichier répliqué, SafeKit attend l'acquittement de l'IO du disque local et du serveur secondaire avant d'envoyer l'acquittement à l'application ou au cache système. Ce mécanisme est indispensable pour la reprise d'applications transactionnelles.

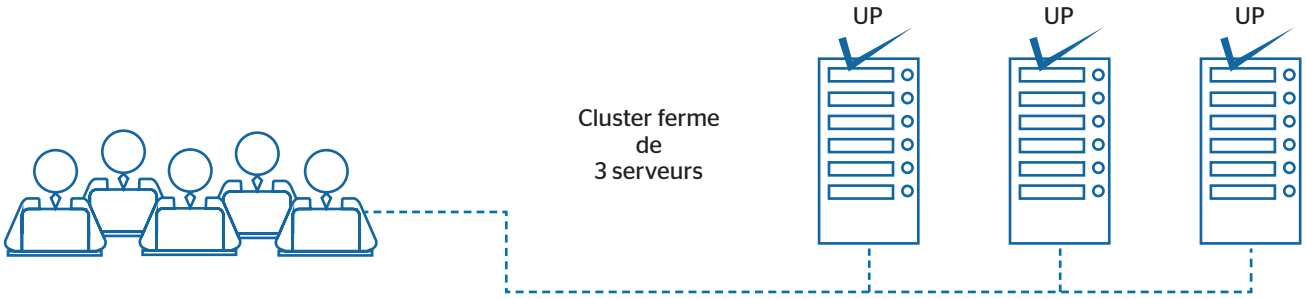
La bande passante d'un LAN entre les deux serveurs est nécessaire pour mettre en œuvre une réplication synchrone de données avec éventuellement un LAN étendu dans deux salles machines géographiquement éloignées.

Avec la réplication asynchrone mises en œuvre par d'autres solutions, les IOs sont mises dans une file sur le serveur primaire et les acquittements du serveur secondaire ne sont pas attendus. Donc, toutes les données qui n'ont pas eu le temps d'être recopiées à travers le réseau sur le second serveur sont perdues en cas de panne du premier serveur. Notamment, une application transactionnelle perd des données commitées en cas de panne. La réplication asynchrone est adaptée à la réplication de données à travers un réseau bas débit de type WAN pour réaliser un backup à distance.

SafeKit propose une solution semi-synchrone avec un asynchronisme non pas sur la machine primaire mais sur la machine secondaire. Dans cette solution, SafeKit attend toujours l'acquittement des deux machines avant d'envoyer l'acquittement à l'application ou au cache système. Mais sur la secondaire, il y a 2 options asynchrone ou synchrone. Dans le cas asynchrone, la secondaire envoie l'acquittement à la primaire dès réception de l'IO puis écrit sur disque. Dans le cas synchrone, la secondaire écrit l'IO sur disque puis envoie l'acquittement à la primaire. Le mode synchrone sur la secondaire est nécessaire si l'on considère une double panne électrique simultanée des deux serveurs avec impossibilité de redémarrer l'ex serveur primaire et obligation de redémarrer sur le secondaire.

Le cluster ferme de SafeKit

Montée en charge et haute disponibilité avec partage de charge réseau et reprise applicative sur panne



Le cluster logiciel ferme permet à la fois de réaliser le partage de charge réseau, à travers une distribution transparente du trafic réseau et une reprise sur panne matérielle et logicielle. Cette architecture fournit une solution simple au problème de la montée en charge. La même application s'exécute sur chacun des serveurs et la charge est distribuée par répartition de l'activité réseau sur les différents serveurs de la ferme. Le cluster ferme est adaptée aux applications frontales telles que les services web.

Apache_farm.safe, Microsoft IIS_farm.safe sont des exemples de modules applicatifs de type « ferme ». Vous pouvez écrire votre propre module ferme pour votre application à partir du module générique Farm.safe.

Une démonstration d'un cluster ferme avec Apache est présentée ici.

Principe d'une adresse IP virtuelle avec partage de charge réseau

L'adresse IP virtuelle est configurée localement sur chaque serveur de la ferme. Le trafic du réseau à destination de l'adresse IP virtuelle est distribué entre les serveurs grâce à un filtre chargé dans le système d'exploitation de chaque serveur.

L'algorithme de partage de charge dans le filtre est basé sur l'identité des paquets client (adresse IP client, port TCP client). Suivant l'identité du paquet client en entrée, seul un filtre dans un serveur accepte le paquet ; les autres filtres dans les autres serveurs le rejettent. Une fois un paquet accepté par le filtre sur un serveur, seul le CPU et la mémoire de ce serveur sont utilisés par l'application qui répond à la requête du client. Les messages de retour de l'application sont envoyés directement du serveur vers le client.

Lorsqu'un serveur est défaillant, le protocole de gestion du groupe des serveurs en vie reconfigure les filtres pour redistribuer le trafic vers les serveurs disponibles.

Critères de partage de charge pour les services web à état et sans état

Avec un service à état, il y a affinité de session. Le même client doit être connecté sur le même serveur sur plusieurs sessions TCP pour retrouver son contexte sur le serveur. Dans ce cas, la règle de load balancing SafeKit est configurée sur l'adresse IP des clients. Ainsi, le même client est toujours connecté sur le même serveur sur plusieurs sessions TCP. Et différents clients sont répartis sur les différents serveurs de la ferme. Cette configuration est à choisir pour les services web à état lorsqu'il y a affinité de session.

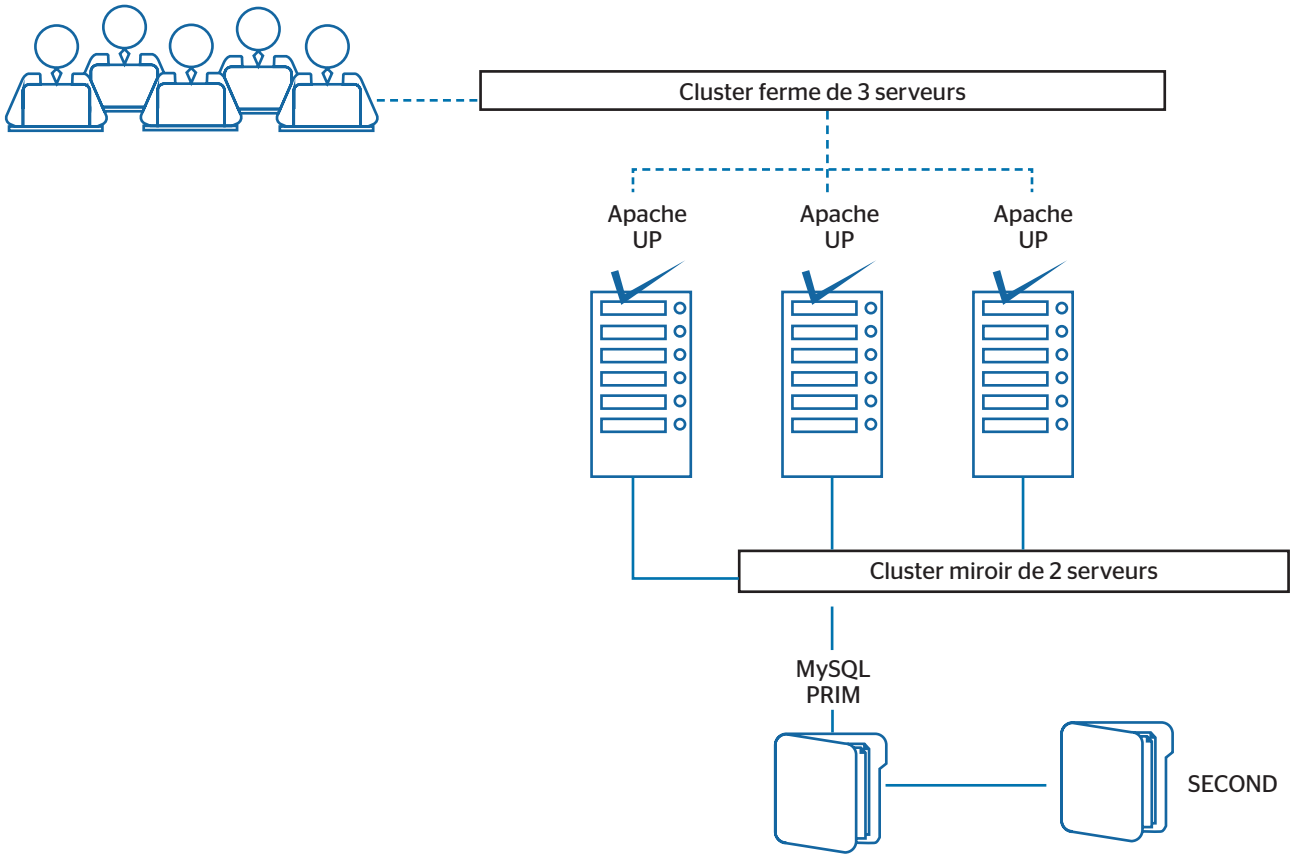
Avec un service web sans état, il n'y a pas d'affinité de session. Le même client peut être connecté sur des serveurs différents dans la ferme lors de sessions TCP successives. Dans ce cas, la règle de load balancing SafeKit est configurée sur l'identité de la session TCP du client. Cette configuration est celle qui répartit le mieux les sessions entre les serveurs mais elle requiert un service TCP sans affinité de session.

Le cluster ferme + miroir de SafeKit

Partage de charge réseau, réplication temps réel de fichiers et reprise applicative sur panne

Des modules applicatifs ferme et miroir peuvent être mixés sur des serveurs physiques communs.

Cette possibilité permet de mettre en œuvre une architecture applicative multi tiers telle que Apache_farm.safe (ferme avec partage de charge et reprise) et MySQL.safe (miroir avec réplication de fichiers et reprise) sur des serveurs applicatifs communs.

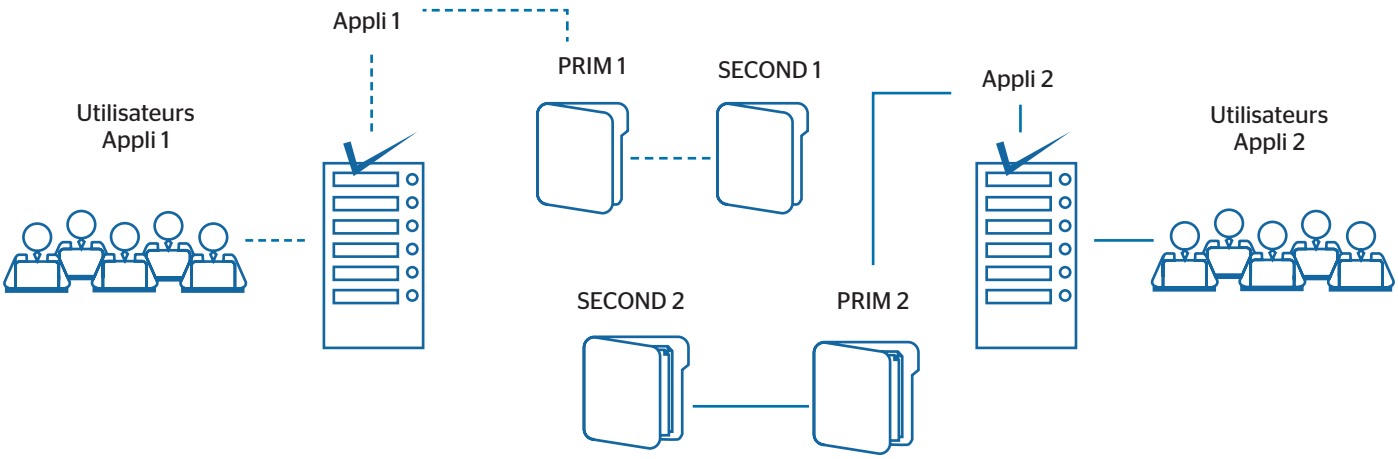


Ainsi, le partage de charge, la réplication de fichiers et la reprise sur panne sont mis en œuvre de manière cohérente sur les mêmes serveurs physiques. Ce type de cluster est propre à SafeKit et unique sur le marché !

Le cluster actif/actif de SafeKit

Réplication croisée et reprise mutuelle sur panne

Dans un cluster actif/actif, il y a deux serveurs et deux modules applicatifs miroirs en reprise mutuelle (Appli1.safe et Appli2.safe). Chaque serveur applicatif est secours de l'autre serveur applicatif.



Lorsqu'un serveur applicatif est défaillant, les deux applications sont actives sur le serveur applicatif restant. Et après le redémarrage du serveur défaillant, chaque application est de nouveau active sur son serveur primaire par défaut.

Un cluster en reprise mutuelle est une solution plus économique que deux clusters miroirs.
Il n'y a pas de serveur de reprise inactif passant son temps à attendre la panne du serveur primaire. Notez que dans une telle architecture, en cas de défaillance d'un serveur, le serveur restant doit supporter la charge des deux applications.

Il faut noter que :

- il faut installer les 2 applications Appli1 et Appli2 sur chacun des 2 serveurs pour la reprise applicative sur panne ;
- cette architecture n'est pas réduite à 2 applications : on peut déployer N modules applicatifs sur les 2 serveurs ;
- chaque module miroir aura sa propre adresse IP virtuelle, ses propres répertoires de fichiers répliqués et ses propres scripts de reprise.

Le cluster Hyper-V ou KVM de SafeKit

Partage de charge, réplication, reprise sur panne de machines virtuelles complètes

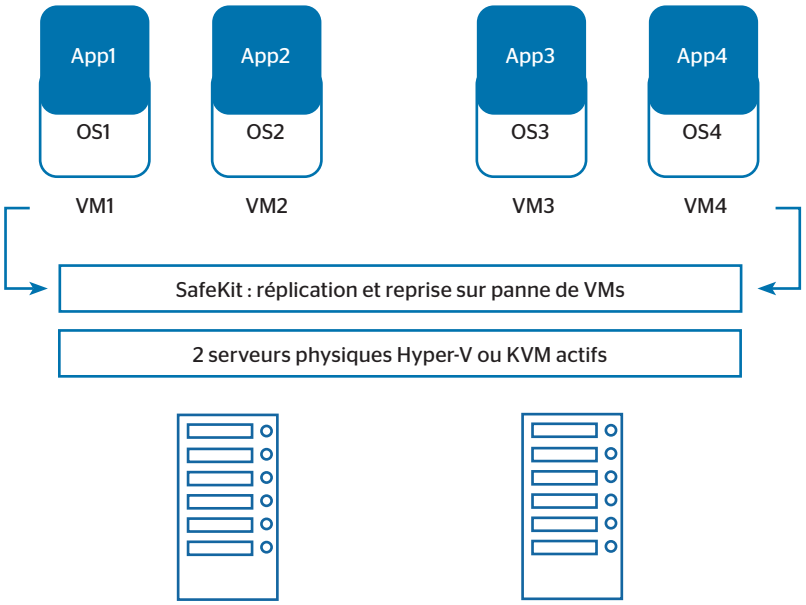
Le cluster Hyper-V ou KVM est un exemple d'un cluster actif-actif avec plusieurs modules miroirs. Chaque machine virtuelle est intégrée dans un module miroir distinct. La solution a les caractéristiques suivantes :

- une réplication temps réel synchrone d'une machine virtuelle complète avec reprise sur panne ;
- un partage de charge de charge des machines virtuelles entre les 2 serveurs Hyper-V ou KVM avec réplication croisée ;
- une console centralisée pour gérer le basculement des VMs ;
- une offre très intéressante pour un revendeur car elle ne nécessite aucune intégration avec les applications ;
- une architecture intéressante pour des solutions de haute disponibilité qui ne peuvent être réalisées au niveau applicatif.

Une démonstration du cluster Hyper-V de SafeKit est présentée ici.

Une démonstration du cluster KVM de SafeKit est présentée ici.

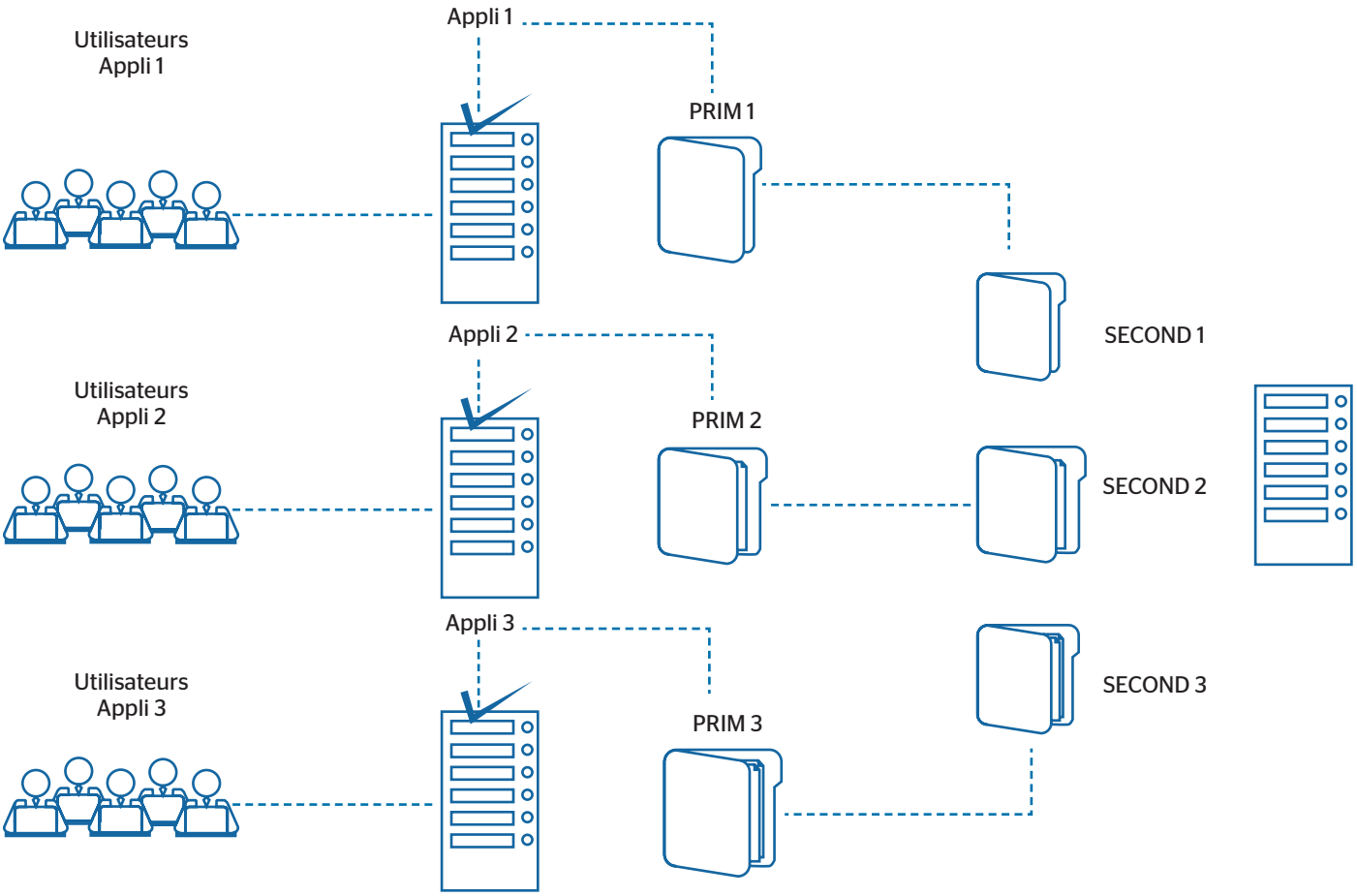
Exemple d'un cluster Hyper-V ou KVM avec 4 machines virtuelles



Le cluster N-1 de SafeKit

Réplication et reprise applicative entre N serveurs actifs et 1 serveur de secours

Dans le cluster N-1, il y a N modules applicatifs de type miroir mis en œuvre sur N serveurs primaires et un seul serveur de secours.



Si un des N serveurs applicatifs actifs est défaillant, le serveur de secours redémarre l'application qui tournait sur le serveur défaillant. Quand le serveur défaillant redémarre, l'application bascule du serveur de secours vers son serveur d'origine.

Dans le cas d'une panne, contrairement au cluster actif/actif, le serveur de secours n'est pas surchargé par l'exécution de plusieurs applications. Dans le cas particulier de plusieurs pannes simultanées, toutes les applications défaillantes sont redémarrées sur le serveur de secours.

Il faut noter que dans un cluster N-1 :

- toutes les applications (Appli 1, Appli 2, Appli 3) doivent être installées sur le serveur de secours unique pour la reprise applicative sur panne ;
- chaque module miroir aura sa propre adresse IP virtuelle, ses propres répertoires de fichiers répliqués et ses propres scripts de reprise.

À propos d'Eviden

Eviden IAM est le leader européen des logiciels de gestion des identités et des accès, avec une présence en pleine croissance en dehors du continent européen et notamment aux Etats-Unis et au Japon.

Plus de 5.000.000 d'utilisateurs dans plus de 900 organisations dans le monde entier se connectent tous les jours à leur entreprise et gèrent leurs droits d'accès avec les solutions de gestion des identités et des accès d'Eviden.

Pour plus d'information : site web SafeKit

CT-210324-JR-SAFEKIT-HIGH-AVAILABILITY-SOFTWARE-EVIDEN-FR