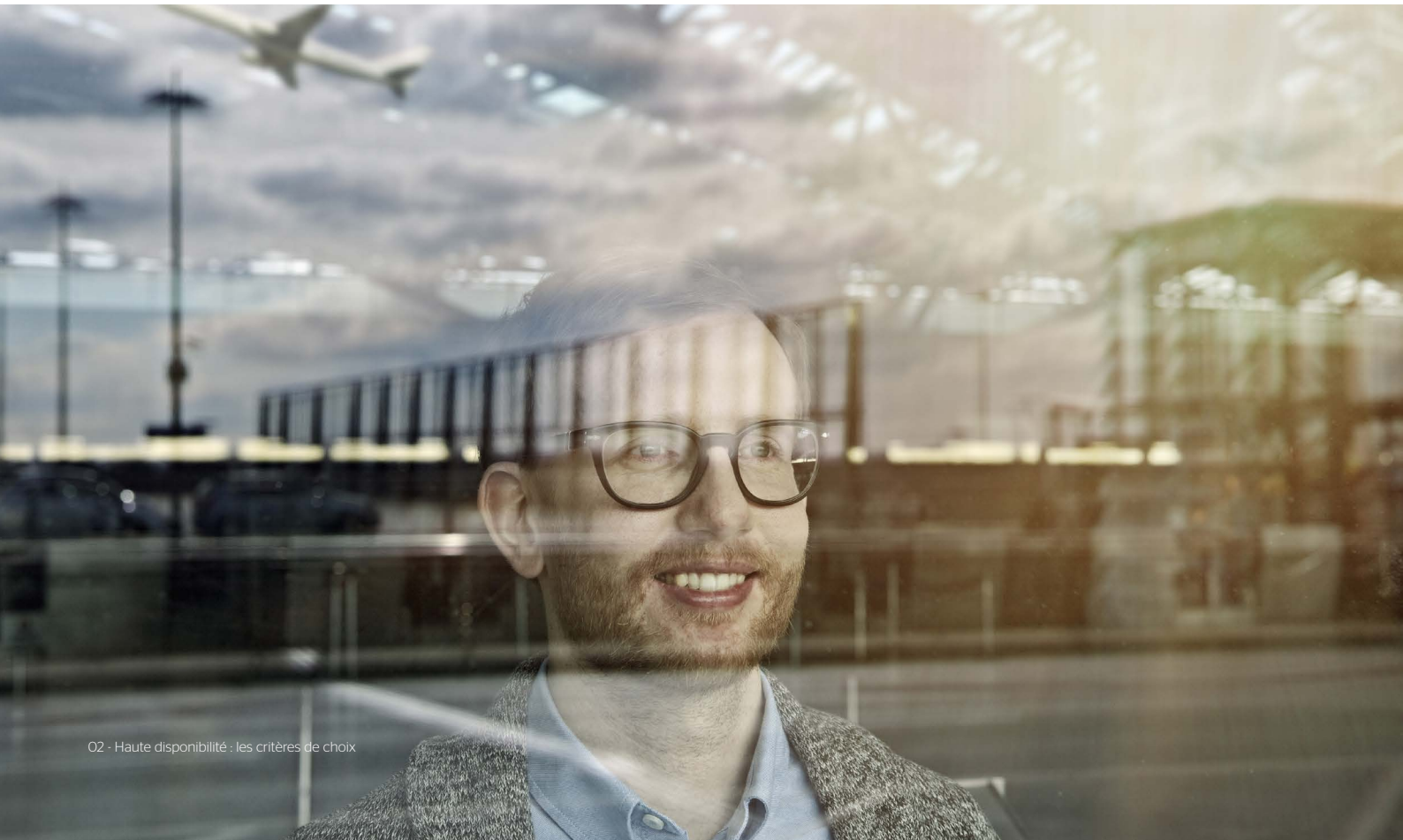
Haute disponibilité : les critères de choix

Trusted partner for your **Digital Journey**

Sommaire

Histoire d'une crise dans un aéroport. Comment choisir une solution de haute disponibilité ?



Histoire d'une crise dans un aéroport

Toutes les activités, petites ou grandes, 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 arrive, un petit problème peut se transformer en crise généralisée à cause d'une succession d'erreurs.

Ce fut le cas de l'histoire suivante vécue dans un aéroport pourtant équipé d'une solution redondante. Cette histoire va nous permettre de dégager les points fondamentaux qui font la qualité d'une solution de haute disponibilité.

La crise s'est déroulée dans un aéroport sur l'application de gestion des voyageurs.

Cette application affiche les informations sur les panneaux de l'aéroport permettant aux voyageurs de retrouver le lieu d'un embarquement ou l'endroit de récupération des bagages.

Une haute disponibilité basée sur la redondance

La base de données associée à la gestion des voyageurs n'est pas importante en terme de volumétrie. Cette base est par contre extrêmement sensible et doit résister au pire cas considéré dans un aéroport : le crash d'un avion sur une salle informatique.

La solution de redondance choisie a donc été deux serveurs éloignés dans deux salles informatiques distantes, chaque serveur disposant localement de la base de gestion des voyageurs. Un produit de réplication a été choisi pour assurer la redondance de la base entre le serveur principal et le serveur de secours.

L'incident

Pour entretenir la base avec les nouveaux vols d'une semaine, tous les dimanches, une opération de mise à jour de la base est réalisée avec les vols de la semaine suivante.

Un dimanche alors que l'opération de mise à jour des vols a lieu sur le serveur principal, la réplication est malencontreusement arrêtée sur le serveur de secours. A l'issue de la mise à jour, le serveur principal dispose donc des vols pour la semaine suivante, alors que le serveur de secours dispose des vols de la semaine précédente.

Le lundi, le serveur principal alimente correctement les panneaux de l'aéroport indiquant aux voyageurs les bons vols et leurs horaires. Pour le service informatique, la gestion de l'aéroport fonctionne parfaitement, malgré l'arrêt de la réplication sur le serveur de secours qui n'a pas été détecté.

La crise

En milieu de semaine, une erreur amène le serveur principal à rebooter automatiquement. Malheureusement, il reste coincé dans son boot et donc ne redémarre pas l'application de gestion des voyageurs. Les panneaux dans l'aéroport deviennent noirs et le service informatique est mis en alerte.

Le serveur principal étant coincé dans son boot, la décision est prise de redémarrer l'application sur le serveur de secours. Le redémarrage sur le serveur de secours est réalisé sans difficulté et quelques minutes plus tard, tous les panneaux de l'aéroport sont de nouveau actifs. Mais ils présentent aux voyageurs les vols de la semaine précédente !

L'alerte rouge au service informatique se transforme en alerte noire. L'application de gestion des voyageurs est immédiatement arrêtée sur le serveur de secours et la décision est prise de régler le problème de reboot du serveur principal. Pendant cette opération, l'application de gestion de l'aéroport est indisponible pour tous les voyageurs.

La situation s'aggrave encore

Les administrateurs parviennent au bout de quelques heures à régler le problème du serveur principal et à le rebooter. Mais, malheureusement, dans la phase de boot, le produit de réplication sur le serveur principal est lancé automatiquement. Il détecte que la réplication est déjà active sur le serveur de secours et il resynchronise la base locale du serveur principal à partir du serveur de secours. Les deux serveurs se retrouvent donc avec la base des vols de la semaine précédente !!!

L'aéroport a été perturbé une journée entière et seule l'opération spéciale du dimanche a permis de re-synchroniser correctement le serveur principal. Au bout du compte, l'aéroport a abandonné le produit de réplication au profit d'une solution de réplication et de haute disponibilité complète, sur la base des critères que nous développons maintenant.

Où sont les failles d'une solution de haute disponibilité ?

Le problème du service informatique de l'aéroport était lié à la solution de réplication choisie. La réplication fonctionnait mais le produit était totalement incomplet sur les mécanismes de haute disponibilité et de reprise en cas de panne. Pourtant, dans sa fiche de spécification technique, ce produit affiche des mécanismes de haute disponibilité avec des scripts de reprise ! Il est donc nécessaire de bien identifier les besoins en haute disponibilité au moment du choix d'un produit de réplication. Les besoins exprimés par l'équipe de production suite à cette crise dans l'aéroport ont été les suivants.

N'importe quel administrateur doit savoir que la réplication est arrêtée sur le serveur de secours

Le premier évènement qui a conduit à la crise dans l'histoire précédente est la mise à jour le dimanche des vols de la semaine sur le serveur principal alors que la réplication sur le serveur de secours était hors service.

Le lundi, lorsque l'équipe de production se retrouve en effectif complet, un simple coup d'œil sur la console d'administration du produit de réplication doit permettre de détecter l'arrêt de la réplication sur le serveur de secours. Le produit de réplication doit donc fournir une console d'administration simple qui sait se connecter à distance sur les serveurs et qui sait fournir un état synthétique d'une application en haute disponibilité sur deux serveurs.

Des possibilités d'envoi de mail et d'intégration dans les consoles d'administration du client en cas d'arrêt de la réplication doivent également exister.

N'importe quel administrateur doit pouvoir relancer la réplication par une opération très simple

Le lundi, dès que l'arrêt de la réplication sur le serveur de secours est détecté, n'importe quel administrateur du service informatique doit pouvoir relancer la réplication :

- soit par une opération clique bouton dans la console d'administration du produit de réplication,
- soit par une commande en ligne très simple offert par le produit de réplication sur le serveur de secours,
- soit par un simple reboot du serveur de secours.

En aucun cas, la relance ne doit être réservée à un expert du produit de réplication. En effet, le système doit être remis au plus vite en haute disponibilité et l'expert n'est pas toujours présent.

La resynchronisation du serveur de secours doit se faire alors que l'application est active sur le serveur principal

Le lundi, à la reprise du service informatique, l'application de gestion des voyageurs de l'aéroport est en cours d'exécution sur le serveur principal. L'opération de relance de la réplication sur le serveur de secours doit être réalisée au plus vite. La resynchronisation de la base du serveur de secours doit pouvoir se faire concurremment aux accès sur le serveur principal.

Il est à noter que des produits de réplication réputés ne savent pas resynchroniser un serveur de secours sans arrêter l'application sur le serveur principal ! Ces produits ne sont pas des produits de haute disponibilité

L'application ne doit pas être relancée sur un serveur dont les données ne sont pas à jour

Dans le cas de l'aéroport, l'alerte s'est transformée en crise à cause du manque de cette fonctionnalité. Le serveur de secours avec les vols de la semaine précédente n'était pas à jour et pourtant rien n'a empêché le démarrage de l'application sur ce serveur.

Plus tard, au redémarrage du serveur principal, la synchronisation des données s'est faite dans le mauvais sens en synchronisant les bases des deux serveurs sur les vols de la semaine précédente et a amené l'aéroport directement à la crise. Des mécanismes de contrôle de la reprise doivent assister l'administrateur pour éviter l'erreur humaine et le démarrage sur une base de données non à jour, ce que ne fournit pas un simple produit de réplication.

La réplication ne doit pas perdre les données collectées avant la panne

Cette réflexion de bon sens n'est pas assurée avec une réplication asynchrone que les produits de réplication mettent traditionnellement en œuvre ! Avant de choisir un produit, il faut vérifier que le produit réalise bien une réplication synchrone pour ne pas perdre de données suite à une panne.

En cas de panne avec une solution de réplication asynchrone, il faudra retrouver les voyageurs passés aux guichets avant la panne et enregistrés sur un vol, mais qui ne sont pas enregistrés dans la base du serveur de secours à cause de la réplication asynchrone. La réservation de ces passagers a été perdue suite à la panne et leurs places sont à nouveau libres dans le système de réservation !

La réplication des données sur le serveur de secours doit être synchrone pour assurer la haute disponibilité

Avec une solution de réplication synchrone, les données ne sont pas perdues en cas de panne. En effet, au guichet d'enregistrement, la procédure d'enregistrement d'un passager consiste à réserver une place dans l'avion pour le passager.

La demande de réservation est envoyée au serveur principal et l'application de gestion des voyageurs stocke l'information de réservation dans la base de données de manière permanente sur le disque local. Avec un mode de réplication synchrone, lorsqu'une information est stockée de manière permanente sur la base locale d'un serveur, elle est également stockée sur la base distante (ce qui n'est pas le cas avec une réplication asynchrone).

Ainsi, lorsque le guichet d'enregistrement reçoit l'acquittement de réservation et que l'hôtesse libère le passager en lui fournissant sa carte d'embarquement, la réservation est réalisée de manière permanente dans les bases des deux serveurs. En cas de panne du serveur principal, les passagers en cours d'enregistrement sont mis en attente car les hôtesses ne peuvent plus contacter l'application de réservation. Dès que l'application est relancée sur le serveur de secours, les hôtesses peuvent à nouveau enregistrer les passagers en attente. Mais les réservations des passagers passés avant la panne ne sont pas perdues et elles sont bien retrouvées dans la base du serveur de secours.

La haute disponibilité doit pouvoir se combiner avec la résistance aux désastres

La haute disponibilité nécessite d'avoir un système de réplication synchrone entre deux serveurs. Les deux serveurs doivent être placés dans un même LAN pour deux raisons. D'une part, la bande passante et la latence du LAN assure les performances de la réplication synchrone. D'autre part, il faut avoir deux serveurs dans le même LAN pour assurer le basculement de l'adresse IP de service lorsque l'application est relancée sur le serveur de secours.

Pour assurer la résistance au désastre et la haute disponibilité, un même LAN peut être très simplement étendu par fibre optique dans deux salles machines géographiquement éloignées. Il est alors possible d'assurer en même temps la haute disponibilité d'une application et la résistance au désastre avec deux serveurs dans deux salles machines et une solution de réplication des données temps réel à travers le réseau.

Lorsque des données doivent être répliquées à travers un WAN faible débit, la réplication des données doit être asynchrone. Mais le système de réplication asynchrone n'apporte pas la haute disponibilité : il perd des données en cas de panne. La réplication asynchrone doit être comparée à un système de backup à distance à travers le réseau et non pas à un système de haute disponibilité.

La solution de haute disponibilité résiste-t-elle au « split brain » sans corrompre les données ?

Le "split brain" se produit en situation d'isolation réseau entre deux serveurs d'un cluster. Chaque serveur devient primaire, croyant que l'autre est défaillant, et tourne l'application. En situation de "split brain", certaines solutions de haute disponibilité peuvent corrompre les bases de données avec deux applications actives sur la même base. Il faut éviter la double exécution en testant un équipement réseau externe agissant comme un témoin entre les deux serveurs.

Cette analyse sur l'exemple de l'aéroport démontre qu'une simple solution de réplication de données n'est pas une solution de haute disponibilité.

Nous avons vu les pièges en cas de panne et nous engageons le lecteur à vérifier qu'un produit de réplication répond bien aux critères de haute disponibilité que nous venons d'expliquer.

De nombreux produits se vantent de réaliser la réplication de données et la haute disponibilité des applications. Mais en fait, ils ne mettent en œuvre que la réplication de données et sont très incomplets du point de vue de la reprise sur panne.

Avec ce type de produit, de manière insidieuse, un service informatique croit disposer d'un système redondant en haute disponibilité. Et il apprend ses limites le jour où un problème comme un serveur coincé dans son boot, se transforme en crise généralisée avec un jour d'indisponibilité pour tout un aéroport !

SafeKit est un produit idéal pour la haute disponibilité des applications critiques. C'est un produit complet et simple. Il a été choisi à l'issue de la crise connue par l'aéroport et a remplacé avantageusement le produit concurrent qui amené à la situation critique décrite dans ce document.

Plus d'information sur notre site web

- Architectures de haute disponibilité et meilleures pratiques
- Comparaison cluster logiciel vs cluster matériel
- Cluster sans données partagées vs cluster avec disques partagés
- HA au niveau VM vs HA au niveau Application
- Réplication de fichiers au niveau octet vs réplication de disques au niveau bloc
- Réplication synchrone versus réplication asynchrone
- Cluster de haute disponibilité logicielle vs système fault-tolerant
- Comment mettre en œuvre des serveurs redondants avec un simple logiciel (Windows / Linux)?
- Heartbeat, failover et quorum dans des clusters Windows ou Linux
- Comment fonctionne une adresse IP virtuelle (Windows/Linux) ?
- Quel est le RTO / RPO d'un cluster de haute disponibilité SafeKit ?
- Microsoft NLB : alternative aux adresses multicast et unicast avec le logiciel SafeKit

Trois témoignages de partenaires

1. Le produit idéal pour un éditeur logiciel

Harmonic, Télédiffusion :

« SafeKit est le logiciel de clustering d'application idéal pour un éditeur logiciel qui cherche une solution de haute disponibilité simple et économique. Nous avons actuellement plus de 80 clusters SafeKit dans le monde entier sur Windows avec notre application critique de télédiffusion à travers la TNT, les satellites, le câble et les réseaux IP. SafeKit réalise la réplication temps réel et continue de notre base de données et la reprise automatique de notre application sur panne logicielle et matérielle. Sans modifier notre application, il a été possible pour nous de personnaliser l'installation de SafeKit. Depuis lors, le temps de préparation et de mise en œuvre a été considérablement réduit. »

2. Le produit très simple à déployer pour un revendeur

NOEMIS, distributeur à valeur ajoutée des solutions de vidéosurveillance Milestone :

« Eviden SafeKit est une solution professionnelle facilitant la redondance de Milestone Management Server, Event Server, Log Server. La solution est facile à déployer, facile à maintenir et peut être ajoutée à une installation existante. Nous avons aidé des intégrateurs à déployer la solution sur de nombreux projets tels que la surveillance urbaine, les data centers, les stades et autres infrastructures critiques. SafeKit est un excellent produit et Eviden fournit un excellent support. Heureux de vous aider si vous avez des questions. »

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

Atos, BU Transport :

« SafeKit est un produit simple et puissant pour la haute disponibilité des applications. Nous avons intégré SafeKit dans nos projets critiques de supervision des lignes de métro à Paris (dans le PCC / Poste de Commande et de Contrôle). Grâce à la simplicité du produit, nous avons gagné du temps dans l'intégration et la validation de la solution et nous avons eu également des réponses rapides à nos questions avec une équipe Eviden réactive. »

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 des 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 :

- Un éditeur de logiciel peut ajouter SafeKit à son catalogue comme option logicielle OEM de haute disponibilité et de partage de charge.
- Une entreprise distribuée peut déployer une solution de haute disponibilité sur du matériel standard sans besoin de compétence informatique spécifique.
- 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 2 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 3 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 versions Windows pour PC !

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 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.

À propos d'Eviden

Eviden IAM est la suite logicielle de gestion des identités et des accès (IAM), 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.

Plus d'information : **site web SafeKit**

CT-210325-JR-HIGH-AVAILABILITY-CHOOSING-SOLUTION-EVIDEN-FR