Descriptif de la solution

Zscaler Resilience™

Continuité des activités sans aucune interruption pendant les coupures de courant, les baisses de tension et les événements catastrophiques

©2023 Zscaler, Inc. Tous droits réservés.

La continuité des activités est une préoccupation majeure des responsables informatiques

La façon dont nous travaillons a changé, et avec ce changement, la continuité des activités est devenue une priorité absolue pour les responsables informatiques. Désormais, ils doivent se concentrer sur la prévention des interruptions des services stratégiques et veiller au maintien de la productivité habituelle. Avec les bons outils, processus et technologies, les équipes informatiques peuvent restaurer rapidement et facilement toutes les capacités opérationnelles de leur entreprise, même en cas de catastrophe.

La migration du stockage, de l'informatique et de la sécurité vers les services cloud a apporté aux entreprises des systèmes flexibles et évolutifs, une meilleure continuité des activités, une réduction des coûts informatiques et une diminution de la complexité. Même avec ces avantages, les entreprises cherchent à optimiser la continuité de leurs activités face à des désastres tels que des catastrophes naturelles, des attaques physiques ou des menaces d'États-nations.

Zscaler Resilience désigne un ensemble complet de fonctionnalités de résilience qui garantit aux clients une continuité des activités sans aucune interruption pendant les coupures, les baisses de tension ou les catastrophes. Cette solution s'appuie sur l'architecture avancée de Zscaler Zero Trust ExchangeTM et est renforcée par l'excellence opérationnelle afin de garantir en permanence une disponibilité et une capacité de service optimales aux clients. Les capacités de reprise après sinistre contrôlées par le client de Zscaler, associées à un ensemble robuste d'options de basculement, accompagnent les efforts de planification de la continuité des activités des clients pour tous les scénarios de défaillance. Cet ensemble complet de capacités de résilience confère au cloud de sécurité Zscaler la plus grande sécurité et la plus grande résilience du secteur.

La résilience cloud : pourquoi est-elle indispensable ?

Les chefs d'entreprise ont à cœur de fournir un environnement propice à une productivité maximale. Les équipes informatiques doivent assurer la continuité des activités et de la productivité même lorsque des problèmes de connectivité, des événements de mise à l'échelle ou des défaillances de service perturbent l'activité normale de l'entreprise.

Le trafic des utilisateurs vers les applications critiques (SaaS, internes et privées) doit constamment être assuré pour garantir la continuité des activités. Les interruptions peuvent résulter d'une panne du cloud ou de la connectivité aux applications. La résilience du cloud englobe à la fois la résilience du cloud et la résilience vers le cloud.

Résilience du cloud
La résilience du cloud garantit que le cloud lui-même repose sur une infrastructure performante et dispose de processus opérationnels solides pour les activités quotidiennes de l'entreprise. Zscaler Cloud gère de manière autonome de nombreuses défaillances mineures (pannes de nœud, problèmes de disque, etc.) sans aucune interaction avec le client, perte de connectivité ou baisse de performances. Nos systèmes matériels robustes et spécialement conçus, avec un surdimensionnement de la capacité de traitement et de la redondance, fournissent la base d'une résilience élevée.

Résilience vers le cloud
La résilience vers le cloud représente un aspect essentiel d'une solution complète de résilience cloud. La connectivité au cloud dépend de sa disponibilité et des moyens de connexion dont disposent les utilisateurs pour accéder aux applications ou aux données. En cas d'interruption de l'accès au cloud, il est indispensable de trouver un chemin alternatif et optimal vers les applications. Cette optimisation consiste en un ensemble d'actions manuelles ou autonomes qui peuvent être appliquées pour faire face à des défaillances telles qu'une baisse des performances du réseau ou des interruptions complètes. Zscaler Resilience désigne un ensemble complet de fonctionnalités qui garantit une continuité des activités sans aucune interruption pour tout type de défaillances allant des pannes mineures aux pannes catastrophiques.

©2023 Zscaler, Inc. Tous droits réservés.

Garantir la résilience du cloud à travers des scénarios de défaillance

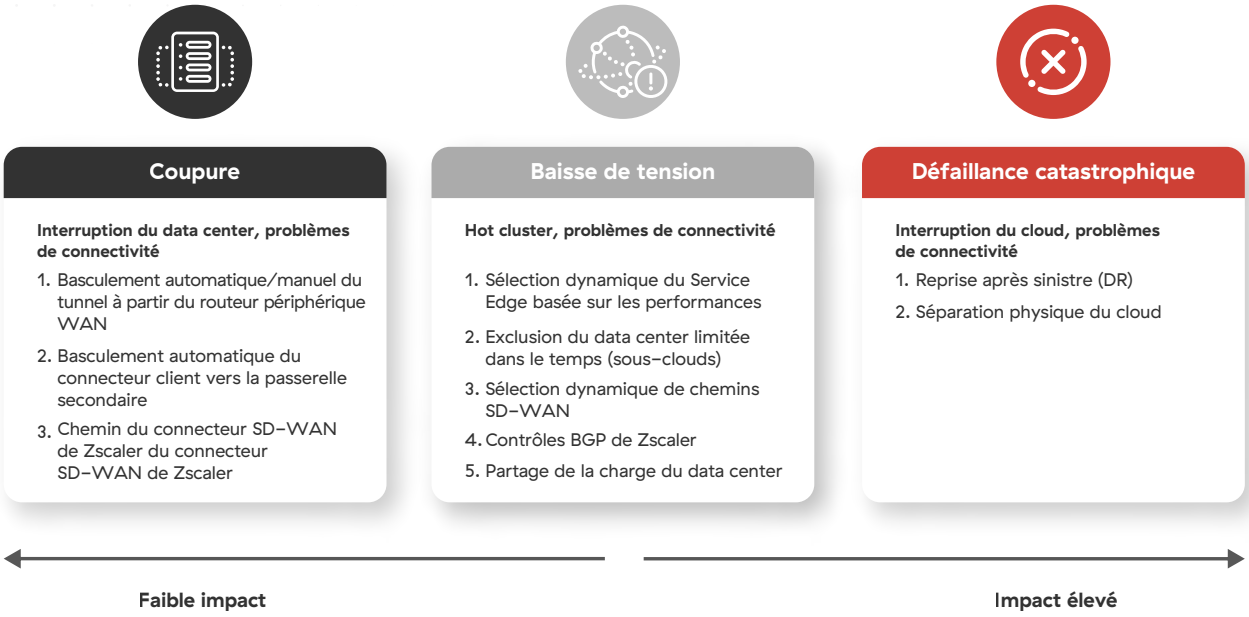

Illustration 1 : Plusieurs options de réponse aux scénarios de défaillance.

Défaillances mineures

Les défaillances mineures sont notamment les problèmes de performances, de compatibilité et de fonctionnement ou de qualité qui ne sont pas des défaillances graves ni critiques. Les pannes de nœuds ou les problèmes de disque peuvent constituer les principales raisons des défaillances isolées. Les défaillances mineures surviennent le plus fréquemment et passent souvent inaperçues. Ces défaillances peuvent être responsables de ralentissements, de problèmes opérationnels et de la frustration des utilisateurs. L'architecture cloud résiliente et l'excellence opérationnelle de Zscaler peuvent contribuer à les éviter. Les défaillances mineures sont gérées en arrière-plan avec un minimum d'interaction avec le client, tout en assurant la continuité de la productivité.

Principaux avantages de Zscaler Resilience

Continuité des activités avec une sécurité ininterrompue

Appliquer les politiques de sécurité critiques tout en accordant un accès Zero Trust à Internet, aux SaaS et aux applications privées, même en cas de catastrophe

Expérience sans faille pour tous les scénarios de défaillance

Gérer facilement les coupures d'électricité, les baisses de tension et les pannes catastrophiques en exploitant l'architecture de pointe et l'excellence opérationnelle de Zscaler Zero Trust Exchange

Diminution des coûts et de la complexité

Éviter les interruptions d'activité et les pertes de productivité causées par un manque d'accès aux applications critiques tout en éliminant les coûts de l'infrastructure de sauvegarde traditionnelle et les VPN sur site

©2023 Zscaler, Inc. Tous droits réservés.

Coupures

Les interruptions de service des data centers (par exemple, l'interruption de service en janvier 2022 du site d'Interxion de Londres) ou les graves problèmes de connectivité, tels que les interruptions de service des opérateurs/fournisseurs de transit, sont considérés comme des scénarios de coupure au cours desquels les entreprises ne peuvent pas transférer le trafic vers le data center Zscaler affecté. Notre architecture redondante (data centers indépendants des opérateurs avec de multiples fournisseurs et des échanges Internet) est particulièrement efficace pour minimiser les pannes en cas de perte d'un opérateur et d'autres problèmes de connectivité. Quel que soit le temps de rétablissement, nos clients sont dans l'impossibilité de bénéficier des services du data center touché.

Pour poursuivre leurs activités, ceux-ci doivent rediriger le trafic vers un centre de données Zscaler secondaire situé à proximité. Nous utilisons un mélange d'opérateurs et de fournisseurs de data centers pour atténuer efficacement les perturbations provenant de n'importe quel fournisseur donné, en garantissant que le data center secondaire sera disponible. Nous sur-provisionnons également et maintenons une capacité de réserve dans le data center afin de gérer une charge transitoire supplémentaire.

S'engager dans la continuité des activités consiste à concevoir et à planifier les différents scénarios de défaillance possibles. Zscaler dispose d'une infrastructure de classe mondiale, conçue pour assurer une disponibilité totale.

Trafic en provenance du bureau via un dispositif SD-WAN
Lorsqu'ils transmettent du trafic depuis un bureau via un dispositif de routage/SD-WAN, les clients doivent suivre les bonnes pratiques de déploiement de Zscaler et disposer d'un tunnel IPsec/GRE de secours prêt à fonctionner lorsque le tunnel principal est inaccessible. La procédure de déclenchement du basculement dépend des capacités du dispositif et de la conception du réseau. Par exemple, un SD-WAN doté de doubles circuits Internet pourrait basculer automatiquement vers le tunnel de secours sur un circuit secondaire lorsque le tunnel actif devient inaccessible ou dépasse un seuil de latence (avec des contrôles de santé L7 activés). Avec des appareils plus anciens, les clients doivent activer manuellement le tunnel de secours. Une fois le data center primaire rétabli, il incombe au client de rétablir la commutation.

Trafic utilisant Zscaler Client Connector
Lors de l'envoi de trafic à l'aide de Zscaler Client Connector, Zscaler contrôle les deux extrémités du tunnel et bascule automatiquement de la passerelle primaire à la passerelle secondaire en utilisant la logique du fichier PAC du profil d'application. Zscaler Client Connector (ZCC) revient à la passerelle primaire dès qu'elle est accessible. Dans certains cas, les clients peuvent choisir de modifier manuellement les fichiers PAC pour déclencher un basculement.

Baisses de tension

Une baisse involontaire ou inattendue de la qualité de service du réseau est un cas typique de baisse de tension. Une mauvaise gestion d'une baisse de tension peut s'avérer coûteuse, tant en termes de perte de revenus que de productivité : si les utilisateurs signalent une baisse de tension avant que l'équipe informatique ne la découvre et ne travaille à sa résolution, il peut en résulter une grande frustration des utilisateurs, ce qui aura pour effet de tout ralentir. Non content de fournir des moyens de résoudre les pannes, Zscaler aide à atténuer les baisses de tension par d'autres moyens évoqués ci-dessous.

©2023 Zscaler, Inc. Tous droits réservés.

Sélection dynamique de Zscaler du Service Edge basée sur les performances
Zscaler Client Connector choisit le chemin optimal entre le ZIA Service Edge principal et le ZIA Service Edge secondaire sans égard à la proximité géographique, en se basant plutôt sur la santé de chaque ZIA Service Edge, comme le montre l'illustration 2. Une connexion HTTP de bout en bout calcule la latence, en envoyant continuellement une requête aux deux passerelles à cette fin. Zscaler peut ainsi proposer une sélection de data centers basée sur la latence afin de répondre efficacement aux scénarios de baisse de tension.

Exclusion du data center contrôlée par le client
Une autre façon de maintenir la continuité des activités pendant les baisses de tension consiste à sélectionner un data center contrôlé par le client, comme le montre l'illustration 3. Lorsqu'un client rencontre des problèmes de capacité dans un data center, comme un problème de peering d'une application SaaS à LAX (dont la résolution pourrait prendre des heures), ce data center peut être exclu du sous-cloud dans le portail d'administration. Zscaler Client Connector récupère alors la nouvelle passerelle primaire et secondaire, et établit un Z-tunnel (tunnel Zscaler) vers un nouveau data center. Cette exclusion du data center contrôlée par le client est limitée dans le temps et revient à la sélection initiale du data center après un délai prédéterminé.

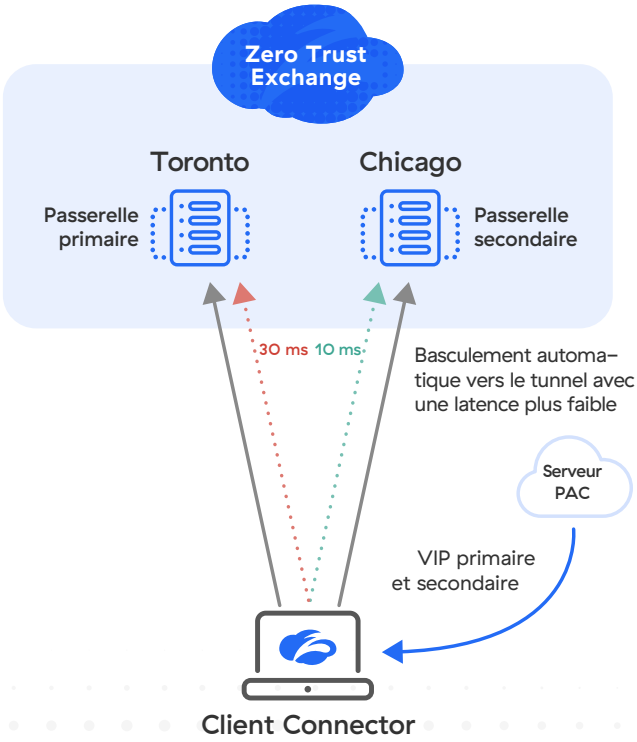

Illustration 2 : Sélection dynamique du Service Edge basée sur les performances.

Basculement du tunnel à partir de dispositifs de routage sensibles aux baisses de tension
Lors de l'envoi de trafic depuis un bureau via un dispositif de routage/SD-WAN sur lequel Zscaler n'a aucun contrôle direct, les options du client sont liées aux capacités du dispositif en périphérie. Par exemple, un routeur SD-WAN peut détecter la dégradation du service à l'aide d'algorithmes propriétaires basés sur les contrôles de santé L7 aux terminaux d'analyse Zscaler. Dès qu'une baisse de tension potentielle est détectée, le dispositif SD-WAN peut automatiquement basculer vers un tunnel de secours sur le même lien ou sur un lien secondaire. L'appareil revient au tunnel primaire lorsque les contrôles de santé font état de meilleurs résultats.

Contrôles BGP de Zscaler
Notre architecture redondante (data centers indépendants des opérateurs avec de multiples fournisseurs et des échanges Internet ou IX) est particulièrement efficace pour minimiser les baisses de tension, les congestions ou autres problèmes liés à des opérateurs uniques. Lorsque Zscaler CloudOps découvre qu'un FAI en amont fournit un routage sous-optimal, nous pouvons réacheminer le trafic via un FAI secondaire pendant que nous travaillons avec le FAI principal pour résoudre le problème.

Partage de la charge du data center par Zscaler
En cas de congestion du réseau ou d'autres problèmes de connectivité à un data center particulier, Zscaler peut rediriger de manière proactive les clients exécutant Zscaler Client Connector vers des data centers secondaires géographiquement proches sans recourir à une méthode statistique.

©2023 Zscaler, Inc. Tous droits réservés.

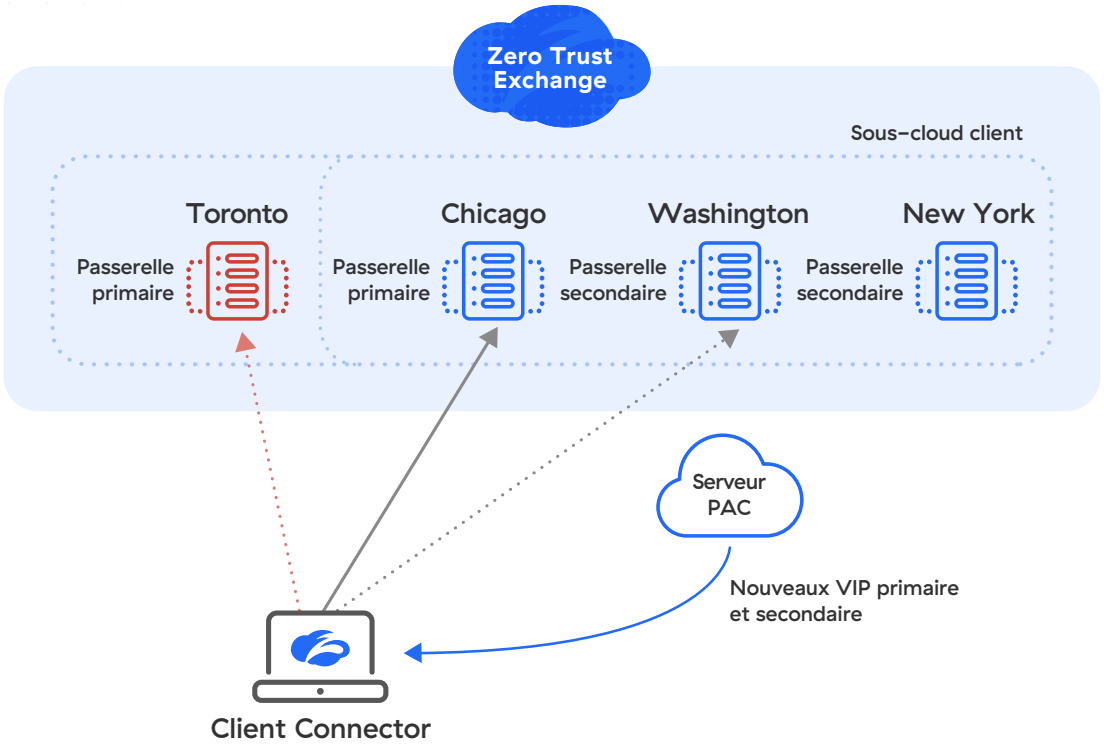

Illustration 3 : Exclusion du data center contrôlée par le client.

Défaillances catastrophiques

Capacité de reprise après sinistre de Zscaler pour ZIA/ZPA

La reprise après sinistre de Zscaler (Zscaler Disaster Recovery) pour le cloud assure aux utilisateurs un fonctionnement sans aucune interruption, garantissant qu'ils peuvent accéder aux applications critiques même pendant un événement catastrophique.

Zscaler Disaster Recovery désigne une solution de continuité des activités contrôlée par le client qui permet aux entreprises de rester opérationnelles même pendant un événement catastrophique susceptible d'affecter Zscaler Cloud.

Zscaler Disaster Recovery est initié par la mise à jour de l'enregistrement TXT du DNS. Lorsque le basculement de reprise après sinistre est initié, Zscaler Disaster Recovery fournit un chemin aux utilisateurs qui se connectent de n'importe quel emplacement, leur permettant d'accéder aux applications privées et SaaS critiques et à Internet, comme le montre l'illustration 4. Avec Zscaler Disaster Recovery, les clients ont le contrôle des applications privées ou SaaS critiques auxquelles les utilisateurs peuvent accéder pendant une panne mondiale de Zscaler Cloud.

Les utilisateurs se connectent aux applications privées critiques via Zscaler Private Access™ (ZPA™) Private Service Edge (une version de Zscaler Cloud déployée localement) et à Internet et aux applications SaaS critiques définis par des politiques enregistrées dans l'instance AWS S3. Tout client ayant installé Zscaler Client Connector peut utiliser Zscaler Disaster Recovery. Grâce au déclencheur de reprise après sinistre basé sur le DNS et initié par le client, ce dernier peut déterminer et contrôler quand activer la reprise après sinistre.

Pour un accès sécurisé aux applications privées, les administrateurs peuvent configurer la reprise après sinistre dans le portail d'administration Zscaler pour les segments d'applications critiques, les groupes App Connector et les groupes ZPA Private Service Edge afin de garantir la continuité des activités en cas de sinistre affectant l'infrastructure cloud ZPA mondiale.

©2023 Zscaler, Inc. Tous droits réservés.

Accès aux applications critiques identifiées par le client
Dans l'interface utilisateur de ZPA, les clients peuvent pré-identifier les applications critiques pour la continuité des activités en cas de sinistre afin de s'assurer que les utilisateurs ont accès à ces applications lors d'un événement de reprise après sinistre.

Pour un accès sécurisé aux applications sur Internet via Zscaler Internet Access™ (ZIA™), les administrateurs peuvent choisir parmi les options de reprise après sinistre suivantes (ces contrôles sont fournis via Zscaler Client Connector et configurés dans le portail Zscaler) :

- **Fail Open :** dans le cas peu probable d'une interruption de Zscaler Cloud, les utilisateurs se rendent directement sur Internet. Cela s'accompagne toutefois du risque de donner à tous les utilisateurs un accès illimité à n'importe quel site Web sur Internet, sans aucune restriction de sécurité.
- **Controlled Fail Open (accès à une liste de destinations Internet définie par Zscaler) :** les utilisateurs ont accès aux applications les plus courantes et les plus critiques sur le Web (Microsoft 365, Google Workspace, etc.). Zscaler maintient cette liste, hébergée sur AWS, afin qu'elle soit disponible pendant que Zscaler Cloud redémarre après une interruption. Les clients peuvent ajouter leur propre liste de sites Internet à cette liste, et tout site Internet ne figurant pas sur la liste est bloqué et appliqué au terminal de l'utilisateur via Zscaler Client Connector. Zscaler Client Connector télécharge périodiquement cette liste pour la maintenir à jour et exacte.
- **Fail Closed :** les clients qui sont très soucieux de la sécurité et qui ne souhaitent pas que les utilisateurs accèdent à quoi que ce soit sur Internet sans ZIA peuvent interrompre tout accès.

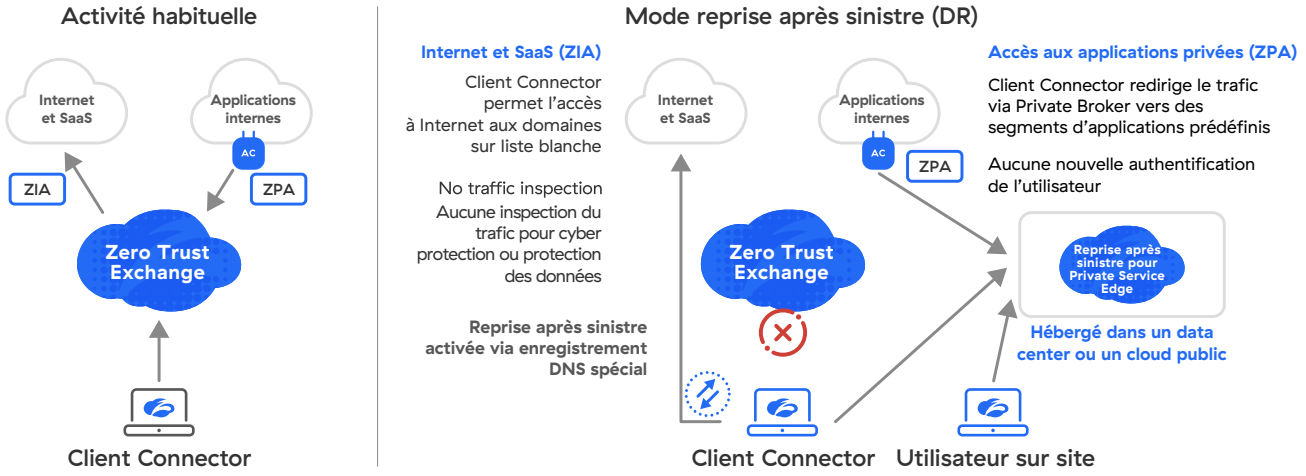

Illustration 4 : Reprise après sinistre pour le service critique de Zscaler.

©2023 Zscaler, Inc. Tous droits réservés.

Activer la reprise après sinistre garantit la continuité des activités en cas de scénario catastrophique ayant un impact sur l'infrastructure cloud mondiale de Zscaler. Cette mise en œuvre permet de maintenir un accès continu et fluide aux applications critiques pour les utilisateurs du monde entier.

Pendant les opérations normales, l'accès aux applications critiques est négocié via Zero Trust Exchange. En cas de sinistre, toutes les connexions aux applications privées sont assurées par le ZPA Private Service Edge, qui est installé localement dans le data center du client ou dans un cloud privé ; toutes les connexions à Internet et aux applications SaaS sont appliquées par le biais de politiques enregistrées dans le compartiment AWS S3. Cela garantit une expérience utilisateur homogène pendant un sinistre. Dès le rétablissement des fonctionnalités de Zscaler Cloud, le produit peut revenir à un fonctionnement normal et bénéficier pleinement de la sécurité et de la connectivité Zero Trust via Zero Trust Exchange. Zscaler Digital Experience détecte les défaillances mineures, les baisses de tension et les coupures de courant pour aider les clients à y remédier avant que cela n'affecte radicalement les utilisateurs. La plateforme Zscaler fournit une flexibilité absolue pour la continuité des activités assortie d'une sécurité inégalée et d'une expérience utilisateur sans faille.

Zscaler Resilience faisant partie de la plateforme globale, nos clients bénéficient d'une redondance au sein de celle-ci sans avoir besoin de recourir à des services externes supplémentaires. Zscaler s'engage à fournir une expérience continue et sans faille aux utilisateurs et aux équipes informatiques à la faveur d'investissements continus dans les solutions Zscaler Resilience.

Pour les dernières informations concernant Zscaler Resilience, rendez-vous sur zscaler.fr/resilience.

Principaux avantages de la reprise après sinistre de Zscaler

- Interruption minimale des opérations des clients lors d'un sinistre
- Accès aux applications stratégiques même pendant un événement catastrophique
  • Amélioration de la fiabilité de la solution pour l'accès aux applications avec Zscaler
- Économies de coûts grâce à une plateforme unique à gérer pour l'accès aux applications, aussi bien en fonctionnement normal qu'en cas de reprise après sinistre
- Économies potentielles en évitant les pertes de productivité dues aux interruptions pendant un sinistre

À propos de Zscaler
Zscaler (NASDAQ : ZS) accélère la transformation numérique de ses clients pour qu'ils gagnent en agilité, en efficacité, en résilience et en sécurité. La plateforme Zscaler Zero Trust Exchange protège des milliers de clients contre les cyberattaques et la perte des données en connectant de manière sécurisée les utilisateurs, les dispositifs et les applications indépendamment de l'emplacement. Distribué à travers plus de 150 data centers dans le monde, Zero Trust Exchange, basée sur le SASE, est la plus grande plateforme de sécurité cloud opérant en mode inline. Pour en savoir plus, rendez-vous sur zscaler.fr ou suivez-nous sur Twitter **@zscaler**.

© 2023 Zscaler, Inc. Tous droits réservés. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™, Zscaler Digital Experience, and ZDX™, et les autres marques commerciales répertoriées sur zscaler.fr/legal/trademarks sont soit 1) des marques déposées ou des marques de service, soit 2) des marques déposées ou des marques de service de Zscaler, Inc. aux États-Unis et/ou dans d'autres pays. Toutes les autres marques commerciales sont la propriété de leurs détenteurs respectifs.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.fr