



Utilisation d'Amazon Web Services pour la reprise après sinistre

Octobre 2014

Glen Robinson, Attila Narin et Chris Elleman

Table des matières

Introduction	3
Objectif de délai de reprise et objectif de point de reprise.....	4
Méthodes traditionnelles de reprise après sinistre.....	4
Services et fonctions AWS élémentaires pour la reprise après sinistre	5
Exemples de scénarios de reprise après sinistre avec AWS	9
Sauvegarde et restauration	9
Veilleuse pour une récupération rapide sur AWS	11
Solution de secours « à chaud » dans AWS	14
Solution multi-site déployée sur AWS et sur site	16
Production AWS vers une solution de reprise après sinistre AWS via plusieurs régions AWS.....	18
Réplication des données	18
Se remettre d'un sinistre	19
Amélioration de votre plan de reprise après sinistre	20
Licences de logiciel et reprise après sinistre.....	21
Conclusion.....	21
Suggestions de lecture	22
Révisions de documents	22

Résumé

En cas de sinistre, vous pouvez lancer rapidement des ressources dans Amazon Web Services (AWS) afin de garantir la continuité des activités. Ce livre blanc met en évidence les services et fonctions AWS que vous pouvez mettre à profit pour vos processus de reprise après sinistre afin de réduire considérablement l'impact sur le fonctionnement de votre entreprise, votre système et vos données. Il comprend également des scénarios qui décrivent progressivement comment améliorer votre stratégie de reprise après sinistre et comment exploiter le plein potentiel du cloud AWS dans ce cas de figure.

Introduction

La reprise après sinistre consiste à vous préparer aux sinistres éventuels et à rétablir vos systèmes. Tout événement ayant un impact négatif sur la continuité des activités d'une entreprise ou sur ses finances peut être considéré comme sinistre. Il peut s'agir d'une défaillance matérielle ou logicielle, d'une indisponibilité du réseau, d'une panne de courant, de dégâts physiques subis par un bâtiment (incendie, inondations, etc.), d'une erreur humaine ou de tout autre événement important.

Pour minimiser l'impact d'un sinistre, les entreprises investissent du temps et des ressources pour planifier et préparer, pour former les employés, ainsi que pour documenter ou mettre à jour les processus. L'investissement nécessaire pour la planification de la reprise après sinistre d'un système spécifique peut varier énormément en fonction du coût d'une panne potentielle. Les sociétés dont les environnements physiques sont traditionnels doivent généralement dupliquer leur infrastructure afin d'assurer la disponibilité de la capacité inutilisée en cas de catastrophe. L'infrastructure doit être achetée, installée et gérée de sorte à prendre en charge les exigences de capacité anticipée. En situation normale, l'infrastructure est souvent sous-utilisée ou surprovisionnée.

Avec Amazon Web Services (AWS), votre entreprise peut ajuster la capacité de son infrastructure en fonction des besoins sur la base d'un paiement à l'utilisation. Vous avez accès à la même infrastructure hautement évolutive, fiable et rapide que celle exploitée par Amazon pour faire fonctionner son propre réseau mondial de sites Web. AWS vous offre également la liberté de remplacer et d'optimiser rapidement les ressources pendant un événement de reprise après sinistre, ce qui peut entraîner d'importantes économies.

Ce livre blanc met en avant les bonnes pratiques recommandées pour améliorer vos processus de reprise après sinistre, allant d'un investissement minime à une disponibilité et une tolérance aux pannes à grande échelle. Il vous explique comment utiliser les services AWS pour réduire les coûts et assurer la continuité des activités en cas de sinistre.

Objectif de délai de reprise et objectif de point de reprise

Ce livre blanc utilise deux termes standards pour la planification des sinistres :

Objectif de délai de reprise (RTO)¹: délai de restauration d'un processus métier à son niveau de service après une interruption, tel que défini par l'accord sur les niveaux opérationnels. Par exemple, si un sinistre a lieu à midi et si le RTO est de huit heures, le processus de reprise après sinistre doit restaurer le processus métier à son niveau de service acceptable avant 20 h.

Objectif de point de reprise (RPO)²: volume acceptable de données perdues mesuré en heures. Par exemple, si un sinistre a lieu à midi et que le RPO est d'une heure, le système doit récupérer toutes les données qui se trouvaient dans le système avant 11 h. La perte de données dure seulement une heure, entre 11 h et midi.

Une entreprise détermine généralement un RTO et un RPO acceptables en fonction de l'impact financier de l'indisponibilité des systèmes sur l'entreprise. Pour déterminer l'impact financier, elle tient compte de plusieurs facteurs, tels que la perte d'activité et l'effet néfaste sur sa réputation en raison du temps d'arrêt et de l'indisponibilité des systèmes.

Les organisations informatiques prévoient ensuite des solutions afin d'assurer une récupération économique des systèmes en fonction du RPO, conformément au délai et au niveau de service défini par le RTO.

Méthodes traditionnelles de reprise après sinistre

Une approche de reprise après sinistre traditionnelle implique différents niveaux de duplication hors site des données et de l'infrastructure. Les services métier critiques sont installés et gérés sur cette infrastructure. Ils sont également testés à intervalles réguliers. L'environnement de reprise après sinistre et l'infrastructure source doivent être physiquement assez éloignés l'un de l'autre pour s'assurer que l'environnement de reprise après sinistre est bien isolé des défaillances susceptibles d'affecter le site source.

Au minimum, l'infrastructure nécessaire pour prendre en charge l'environnement dupliqué doit inclure les éléments suivants :

- Equipements permettant d'héberger l'infrastructure, y compris l'électricité et les stations de refroidissement.
- Sécurité pour garantir la protection physique des ressources.
- Capacité adaptée à la mise à l'échelle de l'environnement.
- Prise en charge des réparations, des remplacements et de l'actualisation de l'infrastructure.
- Accords contractuels avec un fournisseur de service Internet (ISP) qui offre une connectivité Internet pouvant supporter une utilisation de la bande passante dans l'environnement sous une charge totale.
- Infrastructure réseau de type pare-feu, routeurs, commutateurs et équilibreurs de charge.
- Capacité de serveur suffisante pour exécuter tous les services vitaux, y compris des appareils de stockage pour les données connexes, des serveurs permettant d'exécuter des applications et des services backend tels que l'authentification de l'utilisateur, le système de noms de domaine (DNS), le protocole DHCP, la surveillance et l'alerte.

¹ Source http://en.wikipedia.org/wiki/Recovery_time_objective

² Source http://en.wikipedia.org/wiki/Recovery_point_objective

Services et fonctions AWS élémentaires pour la reprise après sinistre

Avant d'aborder les différentes méthodes de reprise après sinistre, il est utile d'examiner les services et fonctions AWS essentiels à celle-ci. Cette section fournit un récapitulatif.

Lors de la préparation à la reprise après sinistre, vous devez prendre en compte les services et fonctions qui prennent en charge la migration des données et le stockage durable, car ils permettent de restaurer les données sauvegardées vers AWS en cas de sinistre. Dans les scénarios qui impliquent une diminution du déploiement ou un déploiement entièrement déployé de votre système dans AWS, des ressources de calcul sont également requises.

Lorsque vous devez réagir à un sinistre, vous devez rapidement indiquer aux ressources de calcul d'exécuter le système sur AWS ou d'orchestrer le basculement vers des ressources s'exécutant déjà sur AWS. Les éléments d'infrastructure essentiels incluent le serveur DNS, les fonctionnalités de mise en réseau, ainsi que les fonctions [Amazon Elastic Compute Cloud](#) (Amazon EC2) que nous décrivons plus bas dans cette section.

Régions

Amazon Web Services est disponible dans de nombreuses régions à travers le monde. Cette présence internationale vous permet de sélectionner l'emplacement le mieux adapté pour votre site de reprise après sinistre, en plus du site sur lequel votre système est entièrement déployé. AWS propose plusieurs régions à usage général dans les zones Amériques, EMEA et Asie-Pacifique, auxquelles les détenteurs d'un compte AWS peuvent accéder. Des régions à usage spécial sont également disponibles pour les agences gouvernementales et pour la Chine. Pour consulter la liste complète des régions disponibles, [cliquez ici](#).

Stockage

[Amazon Simple Storage Service](#) (Amazon S3) offre une infrastructure de stockage hautement durable, conçue pour le stockage des données principales et stratégiques. Les objets sont stockés de manière redondante sur plusieurs appareils dans plusieurs installations au sein d'une région, l'objectif étant d'atteindre une durabilité de 99,999999999 % (11 9s). AWS assure une protection supplémentaire pour la rétention et l'archivage des données via la gestion des versions dans Amazon S3, AWS Multi-Factor Authentication (AWS MFA), les stratégies de compartiment et AWS [Identity and Access Management \(IAM\)](#).

[Amazon Glacier](#) offre un stockage à coût réduit pour l'archivage et la sauvegarde des données. Les objets (ou archives, tels qu'ils sont dénommés dans Amazon Glacier) sont optimisés pour les accès occasionnels, dont le délai d'extraction peut être de plusieurs heures. Amazon Glacier a été conçu pour offrir la même durabilité qu'Amazon S3.

[Amazon Elastic Block Store](#) (Amazon EBS) permet de créer des instantanés ponctuels des volumes de données. Vous pouvez utiliser les instantanés comme point de départ pour les nouveaux volumes Amazon EBS, et vous pouvez protéger vos données pour une durabilité à long terme, car ils sont stockés dans Amazon S3. Une fois que vous avez créé un volume, vous pouvez l'attacher à une instance Amazon EC2 en cours d'exécution. Les volumes Amazon EBS fournissent un stockage hors instance qui perdure indépendamment de la durée de vie d'une instance et qui est répliqué sur plusieurs serveurs dans une zone de disponibilité afin de prévenir la perte de données en cas de panne d'un composant.

[AWS Import/Export](#) accélère le transfert de grandes quantités de données vers et hors d'AWS en utilisant des périphériques de stockage portables pour le transfert. AWS Import/Export contourne Internet et transfère les données directement sur les périphériques de stockage via le réseau à grande vitesse d'Amazon. Pour les ensembles de données volumineux, AWS Import/Export se révèle souvent plus rapide qu'un transfert via Internet et plus économique que la mise à niveau de votre connectivité. Vous pouvez utiliser AWS Import/Export pour migrer les données vers et hors des compartiments Amazon S3 et des coffres Amazon Glacier ou dans les instantanés Amazon EBS.

Le service [AWS Storage Gateway](#) connecte l'appliance logicielle sur site à une unité de stockage basée sur le cloud afin de fournir une intégration continue et sécurisée entre l'environnement informatique et l'infrastructure de stockage AWS.



AWS Storage Gateway prend en charge trois configurations différentes :

Volumes mis en cache sur Gateway : vous pouvez stocker les données primaires dans Amazon S3 et conserver en local les données fréquemment consultées. Les volumes mis en cache sur Gateway vous permettent de réaliser d'importantes économies sur le stockage des données primaires, puisque vous n'avez plus forcément besoin d'ajuster la capacité de stockage sur site. De plus, vous conservez un accès à faible latence aux données fréquemment consultées.

Volumes stockés sur Gateway : si vous avez besoin d'un accès à faible latence à l'ensemble de vos données, vous pouvez configurer la passerelle de façon à stocker les données primaires en local, puis sauvegarder de manière asynchrone des instantanés ponctuels de ces données dans Amazon S3. Les volumes stockés offrent des sauvegardes hors site durables et économiques que vous pouvez récupérer localement ou à partir d'Amazon EC2 si, par exemple, vous avez besoin de capacité de remplacement pour la reprise après sinistre.

Gateway-Virtual Tape Library (Gateway-VTL) : avec Gateway-VTL, vous disposez d'une collection presque illimitée de bandes virtuelles. Vous pouvez stocker chaque bande virtuelle dans une bibliothèque de bandes virtuelles (Virtual Tape Library ou VTL) sauvegardée par Amazon S3 ou une étagère de bandes virtuelles (Virtual Tape Shelf ou VTS) sauvegardée par Amazon Glacier. La bibliothèque de bandes virtuelles présente une interface iSCSI standard, qui fournit à votre application de sauvegarde un accès en ligne aux bandes virtuelles. Dès lors que vous n'avez plus besoin d'un accès fréquent ou immédiat aux données contenues dans une bande virtuelle, vous pouvez utiliser votre application de sauvegarde pour déplacer cette bande de sa bibliothèque de bandes virtuelles vers votre étagère de bandes virtuelles, afin de réduire davantage les coûts de stockage.

Calcul

[Amazon Elastic Compute Cloud \(Amazon EC2\)](#) : offre une capacité de calcul redimensionnable dans le cloud. En l'espace de quelques minutes, vous pouvez créer des instances Amazon EC2, qui sont des machines virtuelles que vous contrôlez entièrement. En matière de reprise après sinistre, il est essentiel de pouvoir créer rapidement des machines virtuelles que vous pouvez contrôler. Ce document n'a pas pour objectif de décrire toutes les fonctions d'Amazon EC2. Il se concentre sur les aspects Amazon EC2 les plus pertinents pour la reprise après sinistre.

Les AMI (Amazon Machine Image) sont préconfigurées avec les systèmes d'exploitation. Certaines incluent même des piles d'applications. Vous pouvez également configurer vos propres AMI. Pour la reprise d'activité, nous vous recommandons vivement de configurer et d'identifier vos propres AMI, pour que leur lancement soit conforme à votre procédure de reprise. Préconfigurez ces AMI avec le système d'exploitation de votre choix, ainsi qu'avec les éléments appropriés de la pile d'applications.

Les zones de disponibilité sont des emplacements distincts conçus pour être isolés des défaillances dans d'autres zones de disponibilité. Elles fournissent également une connectivité réseau économique à faible latence aux autres zones de disponibilité de la même région. En lançant des instances dans des zones de disponibilité distinctes, vous protégez vos applications contre la défaillance d'un seul emplacement. Les régions sont constituées d'une ou de plusieurs zones de disponibilité.

L'application virtuelle [Amazon EC2 VM Import Connector](#) vous permet d'importer des images de machines virtuelles depuis leur environnement existant vers des instances Amazon EC2.

Mise en réseau

En cas de sinistre, il est très probable que vous deviez modifier les paramètres réseau, car le système bascule sur un autre site. AWS propose plusieurs services et fonctions qui vous permettent de gérer et de modifier les paramètres réseau.

[Amazon Route 53](#) est un service Web de système de noms de domaine (DNS) hautement disponible et évolutif. Cette solution fiable et économique permet aux développeurs et aux entreprises d'acheminer les utilisateurs vers les applications Internet. Amazon Route 53 inclut plusieurs fonctionnalités globales d'équilibrage de charge (qui peuvent être utiles dans les scénarios de reprise après sinistre, tels que la vérification de l'état des points de terminaison), ainsi que la possibilité d'effectuer le basculement entre différents points de terminaison, voire entre des sites Web statiques hébergés dans Amazon S3.



Une adresse IP Elastic est une adresse IP statique conçue pour le cloud computing dynamique. Toutefois, contrairement aux adresses IP statiques traditionnelles, les adresses IP Elastic permettent de masquer les défaillances de l'instance ou de la zone de disponibilité en remappant par programmation les adresses IP publiques avec les instances de votre compte dans une région spécifique. Pour la reprise d'activité, vous pouvez également allouer des adresses IP aux systèmes les plus stratégiques au préalable afin qu'elles soient connues avant qu'une catastrophe ne survienne. Cette approche permet de simplifier l'exécution du plan de reprise après sinistre.

[Elastic Load Balancing](#) répartit automatiquement le trafic applicatif entrant sur plusieurs instances Amazon EC2. Il vous permet d'atteindre une tolérance aux pannes encore plus élevée dans vos applications, en fournissant la capacité d'équilibrage de charge nécessaire pour répondre au trafic entrant des applications. Comme avec les adresses IP Elastic, vous pouvez allouer l'équilibrEUR de charge au préalable pour que son nom DNS soit connu, ce qui permet de simplifier l'exécution du plan de reprise après sinistre.

[Amazon Virtual Private Cloud](#) (Amazon VPC) vous permet de mettre en service une section privée et isolée du cloud AWS à partir de laquelle vous pouvez lancer des ressources AWS dans un réseau virtuel que vous définissez. Vous conservez la totale maîtrise de votre environnement réseau virtuel, y compris la sélection de votre propre plage d'adresses IP, la création de sous-réseaux et la configuration de tables de routage et de passerelles réseau. Vous pouvez ainsi établir une connexion VPN entre votre centre de données d'entreprise et votre VPC, et profiter du cloud AWS comme d'une extension de votre centre de données. Pour la reprise après sinistre, vous pouvez utiliser Amazon VPC afin d'étendre la topologie du réseau au cloud, ce qui est particulièrement pratique lors de la récupération des applications professionnelles qui se trouvent généralement sur le réseau interne.

[Amazon Direct Connect](#) facilite la configuration d'une connexion réseau dédiée depuis vos locaux vers AWS. Dans de nombreux cas, cela permet de réduire les coûts réseau, d'augmenter le débit de la bande passante et d'offrir une expérience réseau plus régulière que les connexions basées sur Internet.

Bases de données

Pour répondre à vos besoins en matière de bases de données, pensez à utiliser ces services AWS :

[Amazon Relational Database Service](#) (Amazon RDS) facilite l'installation, l'exploitation et le dimensionnement d'une base de données relationnelle dans le cloud. Vous pouvez utiliser Amazon RDS soit lors de la phase de préparation de la reprise après sinistre (pour conserver les données critiques dans une base de données active), soit lors de la phase de récupération (afin d'exécuter la base de données de production). Lorsque vous souhaitez analyser plusieurs régions, Amazon RDS vous permet de créer un instantané des données d'une région afin de la transmettre à une autre, et d'exécuter un réplica en lecture dans une autre région.

[Amazon DynamoDB](#) est un service de base de données NoSQL rapide et entièrement géré, qui permet, de façon simple et économique, de stocker et d'extraire n'importe quelle quantité de données et de traiter n'importe quel niveau de trafic de demandes. Outre la fiabilité de son débit fiable, il offre une latence moyenne inférieure à 10 millisecondes. Vous pouvez également l'utiliser lors de la phase de préparation, afin de copier les données DynamoDB dans une autre région ou dans Amazon S3. Lors de la phase de récupération de la reprise après sinistre, vous pouvez facilement ajuster la capacité à la hausse en quelques minutes. Un seul clic ou un appel d'API suffit.

[Amazon Redshift](#) est un service d'entrepôt de données dans le cloud rapide et puissant. Entièrement géré, il est doté d'une capacité de plusieurs péta-octets. Il permet d'analyser de manière simple et rentable toutes vos données grâce à vos outils d'informatique décisionnelle existants. Vous pouvez utiliser Amazon Redshift lors de la phase de préparation, afin de créer un instantané de votre entrepôt de données et de le stocker de manière durable dans la même région d'Amazon S3 ou de le copier dans une autre région. Lors de la phase de récupération de la reprise après sinistre, vous pouvez restaurer rapidement votre entrepôt de données dans la même région ou au sein d'une autre région AWS.

Vous pouvez également installer et exécuter votre logiciel de base de données de prédilection sur Amazon EC2, et avez le choix parmi un large éventail de systèmes de bases de données de premier ordre.

Pour plus d'informations sur les options de base de données sur AWS, consultez la page [Exécution de bases de données sur AWS](#).



Orchestration du déploiement

Les processus et outils d'automatisation du déploiement et d'installation ou de configuration des logiciels après le démarrage peuvent être utilisés dans Amazon EC2. Nous vous recommandons vivement d'investir dans ce domaine. Ces processus et outils, qui vous permettent de créer le jeu de ressources requis de manière automatisée, peuvent être très utiles lors de la phase de récupération.

[AWS CloudFormation](#) permet aux développeurs et aux administrateurs système de créer et de gérer facilement un ensemble de ressources AWS liées entre elles et de les mettre en service de manière ordonnée et prévisible. Vous pouvez créer des modèles pour vos environnements et déployer les ensembles de ressources associés (ou piles) à votre convenance.

[AWS Elastic Beanstalk](#) est un service de déploiement et d'évolutivité des applications et services Web développés avec Java, .NET, PHP, Node.js, Python, Ruby et Docker. Il vous suffit de déployer le code applicatif et AWS Elastic Beanstalk se charge de mettre en service l'environnement d'exploitation de vos applications.

[AWS OpsWorks](#) est un service de gestion d'applications qui facilite le déploiement et l'exploitation d'applications de toutes tailles et de tous les types. Vous pouvez définir votre environnement tel une série de couches et configurer chacune de ces couches comme niveau de votre application. AWS OpsWorks assure le remplacement automatique des hôtes. Autrement dit, en cas de défaillance d'une instance, celle-ci est remplacée automatiquement. Vous pouvez utiliser AWS OpsWorks lors de la phase de préparation, afin de créer un modèle de l'environnement, puis le combiner avec AWS CloudFormation lors de la phase de récupération. Vous pouvez rapidement mettre en service une nouvelle pile à partir de la configuration stockée qui prend en charge le RTO défini.

Sécurité et conformité

Tous les services AWS incluent de nombreuses fonctions liées à la sécurité. Nous vous conseillons de lire le livre blanc sur les [bonnes pratiques en matière de sécurité](#). AWS fournit également des informations sur les risques et la conformité dans le [Centre de sécurité AWS](#). Sachez que ce livre blanc n'aborde que partiellement la question de la sécurité.

Exemples de scénarios de reprise après sinistre avec AWS

Cette section décrit quatre scénarios de reprise après sinistre qui illustrent l'utilisation d'AWS et le compare aux méthodes de reprise après sinistre traditionnelles. La figure ci-dessous représente le spectre de ces quatre scénarios, organisé selon la rapidité avec laquelle les utilisateurs parviennent de nouveau à accéder à un système suite à un événement de reprise après sinistre.

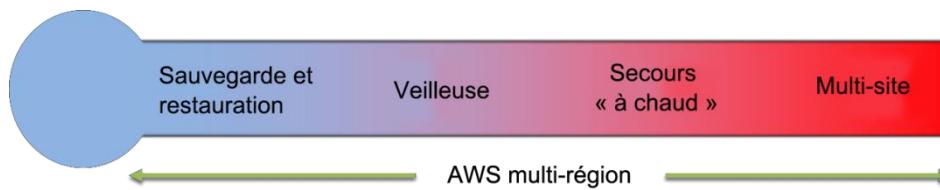


Figure 1 : Spectre des options de reprise après sinistre

AWS vous permet de gérer chacune de ces stratégies de reprise après sinistre à moindre coût. Notez qu'il s'agit uniquement d'exemples d'approches envisageables. Des variations, ainsi que diverses combinaisons sont possibles. Si l'application est déjà exécutée sur AWS, les mêmes stratégies de reprise après sinistre s'appliquent, même si vous utilisez plusieurs régions.

Sauvegarde et restauration

Dans la plupart des environnements traditionnels, les données sont généralement sauvegardées sur des bandes, puis envoyées hors site. Cette méthode implique un délai de restauration du système très long en cas de perturbation ou de catastrophe. Amazon S3 est une destination parfaite pour les données de sauvegarde qui doivent être disponibles rapidement afin de procéder à la restauration. Les échanges de données avec Amazon S3 ont normalement lieu via le réseau. Les données sont donc accessibles à partir de n'importe quel emplacement. Les solutions de sauvegarde commerciales et Open Source compatibles avec Amazon S3 sont nombreuses. Vous pouvez utiliser le service AWS Import/Export pour transférer des ensembles de données très volumineux en transmettant des périphériques de stockage directement à AWS. Amazon Glacier, qui offre le même modèle de durabilité qu'Amazon S3, convient parfaitement au stockage des données à long terme, dont le délai d'extraction peut être de plusieurs heures. Amazon Glacier est une alternative économique dont le prix mensuel commence à 0,01 USD/Go. Amazon Glacier et Amazon S3 peuvent être combinés afin de disposer d'une solution de sauvegarde à plusieurs niveaux.

AWS Storage Gateway permet de créer des instantanés de vos volumes de données sur site afin de les copier de manière transparente et de les sauvegarder dans Amazon S3. Vous pouvez ensuite créer des volumes locaux ou volumes Amazon EBS à partir de ces instantanés.

Les volumes mis en cache vous permettent de stocker les données primaires dans Amazon S3 tout en conservant en local les données fréquemment consultées afin d'assurer un accès à faible latence. Comme avec AWS Storage Gateway, vous pouvez créer des instantanés des volumes de données pour une sauvegarde hautement durable. En cas de reprise après sinistre, vous pouvez restaurer les volumes mis en cache sur un deuxième site exécutant une passerelle de stockage ou sur Amazon EC2.

Vous pouvez utiliser la configuration Gateway-VTL d'AWS Storage Gateway comme destination de sauvegarde de votre logiciel de gestion des sauvegardes. Cette méthode permet de remplacer la sauvegarde traditionnelle sur bande magnétique.

Pour les systèmes exécutés sur AWS, vous pouvez également sauvegarder les données dans Amazon S3. Il est possible de stocker des instantanés des volumes Amazon EBS, des bases de données Amazon RDS et des entrepôts de données Amazon Redshift dans Amazon S3. Vous pouvez également copier des fichiers directement dans Amazon S3 ou créer des fichiers de sauvegarde et les copier dans Amazon S3. Les solutions de sauvegarde qui permettent de stocker les données directement dans Amazon S3 sont nombreuses. Par ailleurs, vous pouvez aussi les utiliser à partir des systèmes Amazon EC2.



La figure ci-dessous illustre les options de sauvegarde de données dans Amazon S3 à partir d'une infrastructure sur site ou d'AWS.

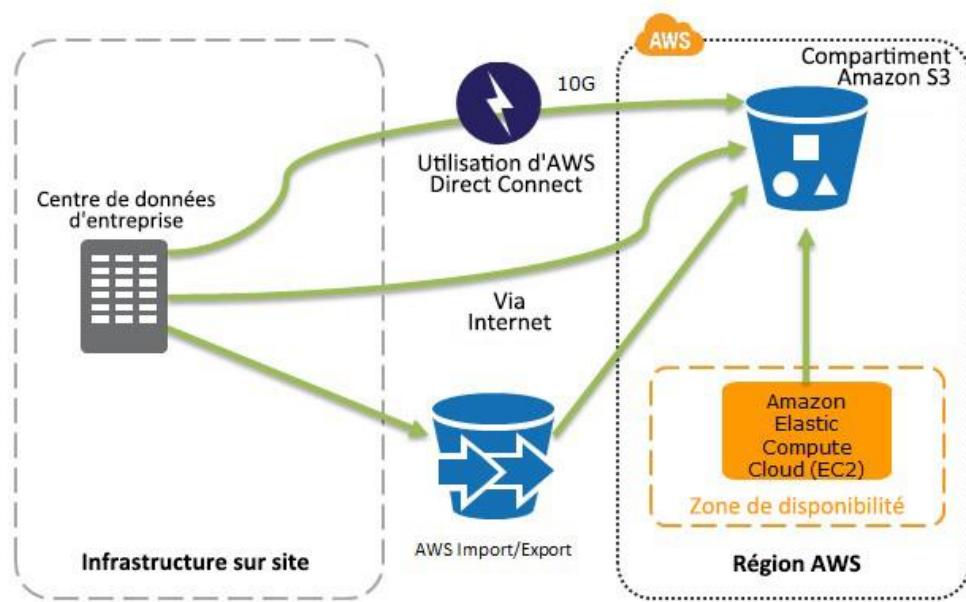


Figure 2 : Options de sauvegarde de données dans Amazon S3 à partir d'une infrastructure sur site ou d'AWS

La sauvegarde de vos données n'est que la partie émergée de l'iceberg. En cas de catastrophe, vous devez récupérer vos données rapidement, avec une fiabilité optimale. Vous devez vérifier que vos systèmes sont configurés pour conserver et sécuriser vos données, de même que vous devez tester les processus de récupération.

Le diagramme suivant illustre la rapidité avec laquelle vous pouvez restaurer un système à partir des sauvegardes Amazon S3 vers Amazon EC2.

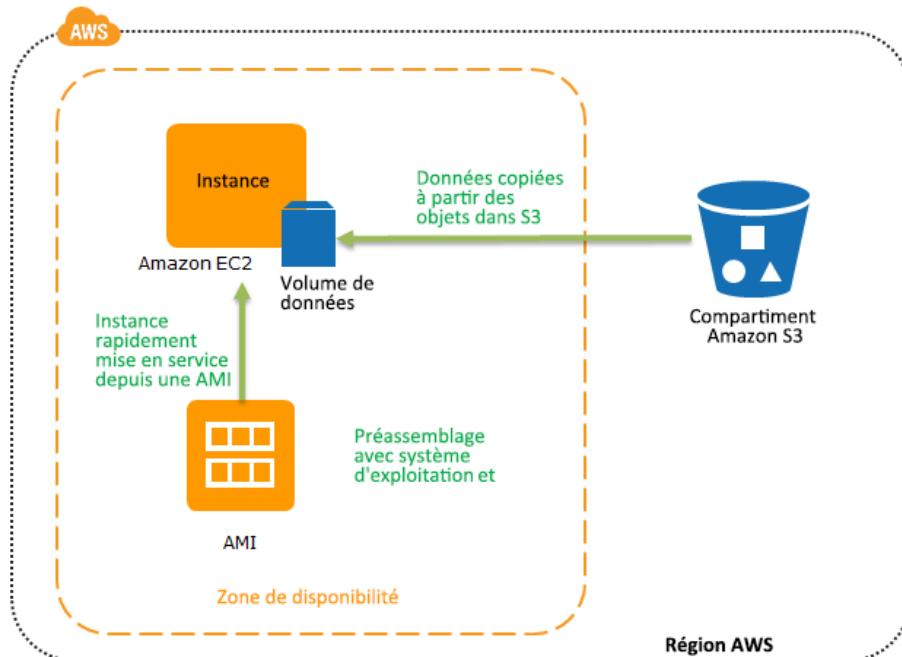


Figure 3 : Restauration d'un système à partir des sauvegardes Amazon S3 vers Amazon EC2

Principales étapes de sauvegarde et restauration :

1. Sélectionnez une méthode ou un outil approprié pour sauvegarder vos données dans AWS.
2. Assurez-vous de disposer d'une stratégie de rétention appropriée pour ces données.
3. Veillez à ce que des mesures de sécurité adéquates s'appliquent à ces données, telles que des stratégies de chiffrement et d'accès.
4. Testez régulièrement la récupération de ces données et la restauration de votre système.

Veilleuse pour une récupération rapide sur AWS

Le terme *veilleuse* est souvent utilisé pour décrire un scénario de reprise après sinistre dans lequel la version minimale d'un environnement s'exécute toujours dans le cloud. Le concept de veilleuse est une analogie qui provient des systèmes de chauffage au gaz. Dans un système de chauffage au gaz, une petite flamme toujours allumée peut rapidement déclencher toute la chaudière pour chauffer une maison.

Cela est similaire à un scénario de sauvegarde et de restauration. Par exemple, avec AWS, la veilleuse est assurée par la configuration et l'exécution des principaux éléments de votre système dans AWS. A l'heure de procéder à la récupération, vous pouvez rapidement mettre en service un environnement de production entièrement déployé autour du noyau critique.

Les éléments d'infrastructure pour la veilleuse incluent généralement les serveurs de base de données, qui répliquent les données vers Amazon EC2 ou Amazon RDS. Selon le système, il est parfois nécessaire de répliquer sur AWS d'autres données critiques qui se trouvent en dehors de la base de données. C'est le noyau critique du système (veilleuse) autour duquel tous les autres éléments de l'infrastructure AWS peuvent être rapidement mis en service (autres composants de la chaudière) pour restaurer l'intégralité du système.

Pour mettre en service le reste de l'infrastructure et restaurer ainsi les services stratégiques, des serveurs préconfigurés sont généralement regroupés sous forme d'AMI (Amazon Machine Image), que vous pouvez lancer en un instant. Lors du lancement de la récupération, les instances de ces AMI entrent en jeu rapidement avec leur rôle prédéfini (par exemple, serveur Web ou serveur d'applications) au sein du déploiement autour de la veilleuse. Du point de vue de la mise en réseau, deux options principales s'offrent à vous pour la mise en service :

- Associez des adresses IP Elastic, que vous pouvez allouer au préalable et identifier lors de la phase de préparation de la reprise après sinistre, à vos instances. Notez que pour les licences logicielles basées sur des adresses MAC, vous pouvez utiliser des interfaces ENI (Elastic Network Interface) dont l'adresse MAC peut également être préalablement affectée pour la mise en service des licences. Comme avec les adresses IP Elastic, vous pouvez les associer à vos instances.
- Utilisez la fonction Elastic Load Balancing (ELB) pour répartir le trafic entre plusieurs instances. Mettez ensuite à jour les enregistrements DNS pour qu'ils renvoient vers l'instance Amazon EC2 ou vers l'équilibreur de charge via un CNAME. Nous conseillons cette option pour les applications Web traditionnelles.

Pour les systèmes dont la priorité est secondaire, assurez-vous que tous les packages d'installation et toutes les informations de configuration sont disponibles dans AWS (sous forme d'instantané Amazon EBS, par exemple). La configuration du serveur d'applications sera ainsi accélérée, car vous pourrez créer rapidement plusieurs volumes dans différentes zones de disponibilité et les relier aux instances Amazon EC2. Vous pourrez ensuite procéder à l'installation et à la configuration en conséquence (par exemple, via la méthode de sauvegarde et de restauration).

La méthode de la veilleuse offre un délai de reprise plus court que la sauvegarde et la restauration, car les principaux éléments du système sont déjà en cours d'exécution et sont continuellement maintenus à jour. AWS permet d'automatiser la mise en service et la configuration des ressources d'infrastructure. Vous gagnez ainsi du temps tout en vous protégeant contre les erreurs humaines. Toutefois, vous devez tout de même effectuer certaines tâches d'installation et de configuration pour restaurer entièrement les applications.



Phase de préparation

La figure suivante illustre la phase de préparation, au cours de laquelle les données qui changent régulièrement doivent être répliquées vers la veilleuse, système central autour duquel l'environnement complet sera lancé lors de la phase de récupération. Les données mises à jour moins fréquemment, telles que les systèmes d'exploitation et les applications, peuvent être mises à jour périodiquement et stockées sous forme d'AMI.

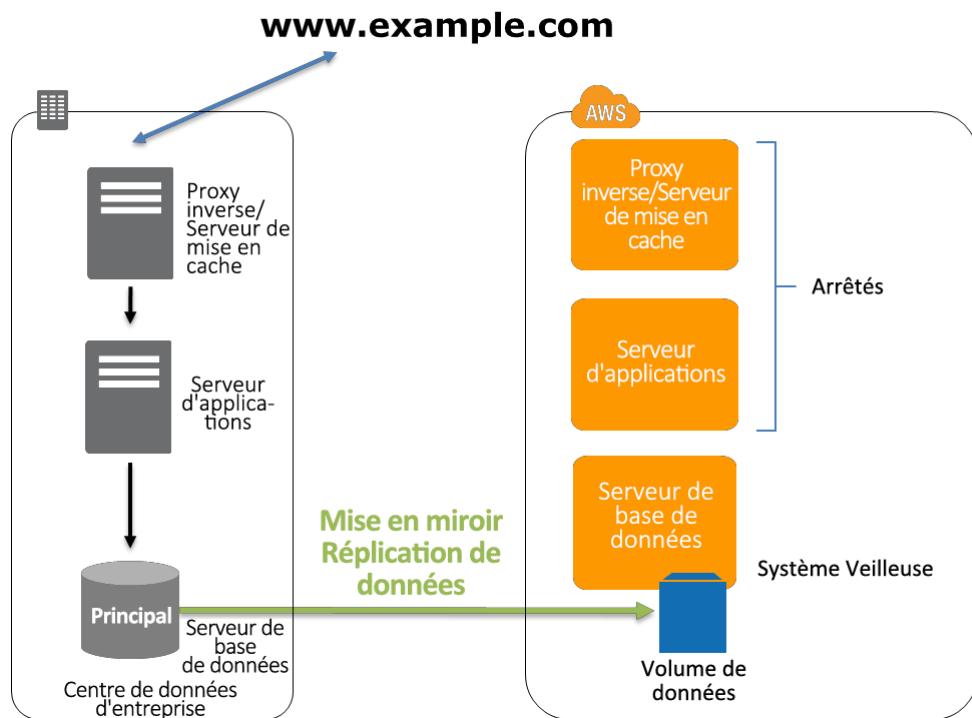


Figure 4 : Phase de préparation du scénario de la veilleuse

Principales étapes de préparation :

1. Configurez les instances Amazon EC2 pour effectuer la réPLICATION ou la mise en miroir des données.
2. Vérifiez que tous les packages de logiciels personnalisés requis sont disponibles dans AWS.
3. Créez et gérez le AMI des serveurs principaux sur lesquels une récupération rapide est nécessaire.
4. Exécutez régulièrement ces serveurs, testez-les et appliquez les mises à jour logicielles et les modifications de configuration.
5. Envisagez d'automatiser la mise en service des ressources AWS.

Phase de récupération

Pour récupérer le reste de l'environnement autour de la veilleuse, vous pouvez démarrer les systèmes à partir des AMI en quelques minutes sur les types d'instances appropriés. Pour les serveurs de données dynamiques, vous pouvez les redimensionner afin de traiter les volumes de production requis ou augmenter la capacité en conséquence. Le dimensionnement horizontal est souvent l'approche la plus économique et la plus évolutive pour accroître la capacité d'un système. Par exemple, vous pouvez ajouter davantage de serveurs Web lors des pics d'activité. Toutefois, vous pouvez également choisir des types d'instances Amazon EC2 plus grands et procéder ainsi à un dimensionnement vertical pour des applications comme les bases de données relationnelles. Du point de vue de la mise en réseau, toutes les mises à jour nécessaires du DNS peuvent être effectuées en parallèle.

Après la récupération, assurez-vous que la redondance est restaurée au plus vite. Il est peu probable que votre environnement de reprise après sinistre tombe en panne juste après votre environnement de production, mais le risque existe. Continuez de procéder à des sauvegardes régulières du système et envisagez d'élargir la redondance au niveau de la couche de données.

La figure suivante illustre la phase de récupération du scénario de la veilleuse.

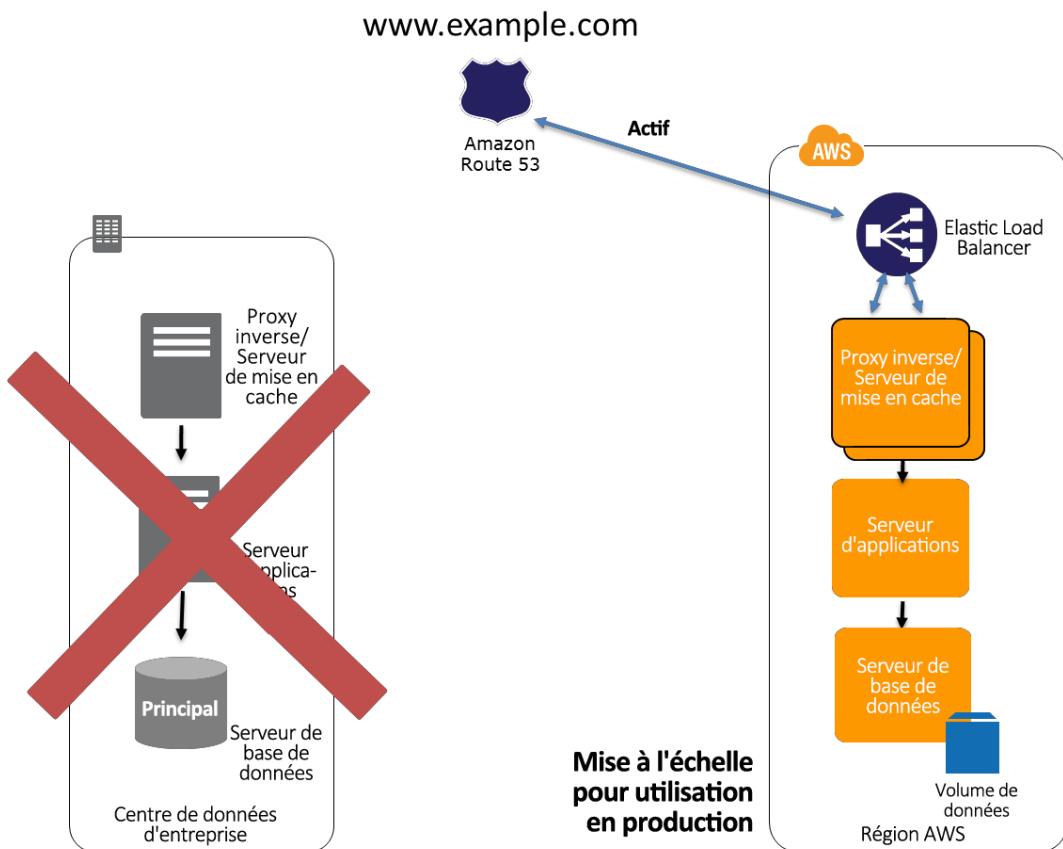


Figure 5 : Phase de récupération du scénario de la veilleuse

Principales étapes de récupération :

1. Démarrez les instances applicatives Amazon EC2 à partir des AMI personnalisées.
2. Redimensionnez les instances de stockage des données/bases de données afin de prendre en charge l'augmentation du trafic.
3. Ajoutez d'autres instances de stockage des données/bases de données afin d'assurer la résilience du site de reprise après sinistre au niveau des données. Si vous utilisez Amazon RDS, activez plusieurs zones de disponibilité pour améliorer la résilience.
4. Modifiez le DNS pour pointer vers les serveurs Amazon EC2.
5. Installez et configurez les systèmes non basés sur des AMI, idéalement de manière automatique.

Solution de secours « à chaud » dans AWS

Le terme *secours à chaud* est utilisé pour décrire un scénario de reprise après sinistre dans lequel la version minimale d'un environnement entièrement fonctionnel s'exécute toujours dans le cloud. Une solution de secours « à chaud » prolonge les éléments de la veilleuse et la préparation. Elle permet également de raccourcir davantage le temps de récupération, car certains services sont exécutés en permanence. En identifiant vos systèmes stratégiques, vous pouvez dupliquer entièrement ces systèmes sur AWS pour qu'ils soient toujours actifs.

Ces serveurs peuvent être exécutés sur une flotte d'instances Amazon EC2 de taille minimum. Cette solution n'est pas dimensionnée pour traiter une charge de production complète, mais elle est très pratique. Elle est utile pour les tâches autres que la production, notamment les tests, l'assurance qualité et l'utilisation interne.

Lors d'un sinistre, la capacité du système est rapidement ajustée pour pouvoir traiter la charge de production. Pour ce faire, dans AWS, il suffit d'ajouter des instances à l'équilibrage de charge et de redimensionner les serveurs à faible capacité pour qu'ils s'exécutent sur des types d'instances Amazon EC2 plus grands. Comme nous l'avons décrit dans la section précédente, un dimensionnement horizontal est préférable à un dimensionnement vertical.

Phase de préparation

La figure suivante illustre la phase de préparation d'une solution de secours « à chaud », dans laquelle une solution sur site et une solution AWS sont exécutées côté à côté.

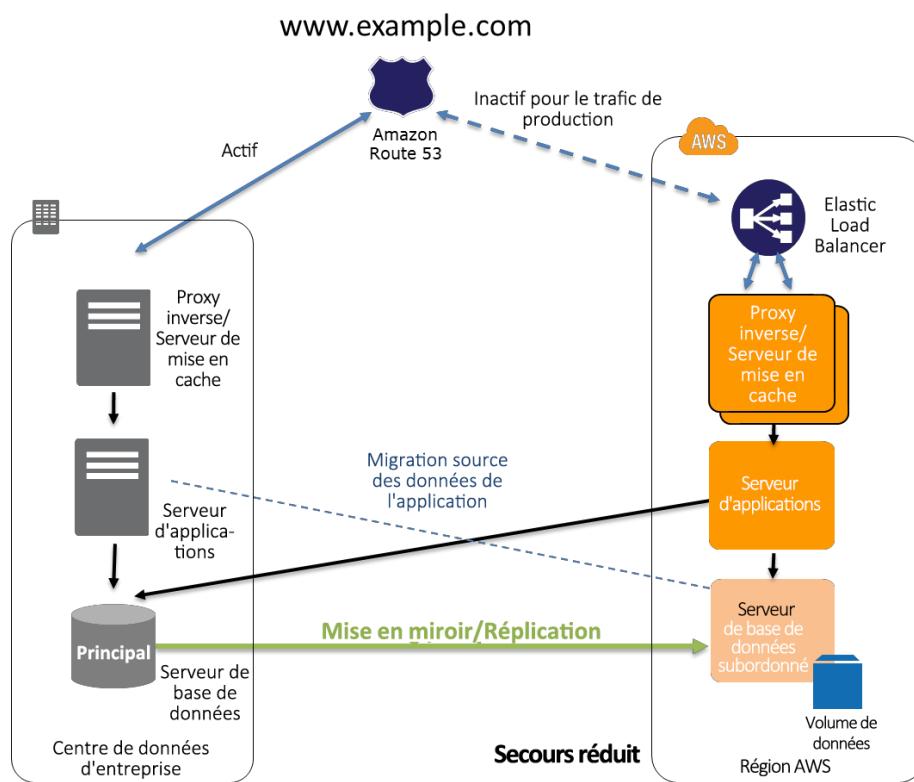


Figure 6 : Phase de préparation du scénario de secours « à chaud »

Principales étapes de préparation :

1. Configurez les instances Amazon EC2 pour effectuer la réplication ou la mise en miroir des données.
2. Créez des AMI et gérez-les.
3. Exécutez votre application avec des instances Amazon EC2 ou une infrastructure AWS à encombrement minime.
4. Appliquez les correctifs et les mises à jour aux logiciels et aux fichiers de configuration en accord avec votre environnement en direct.

Phase de récupération

En cas de défaillance du système de production, l'environnement de secours est ajusté en fonction de la charge de production et les enregistrements DNS sont modifiés pour acheminer l'ensemble du trafic vers AWS.

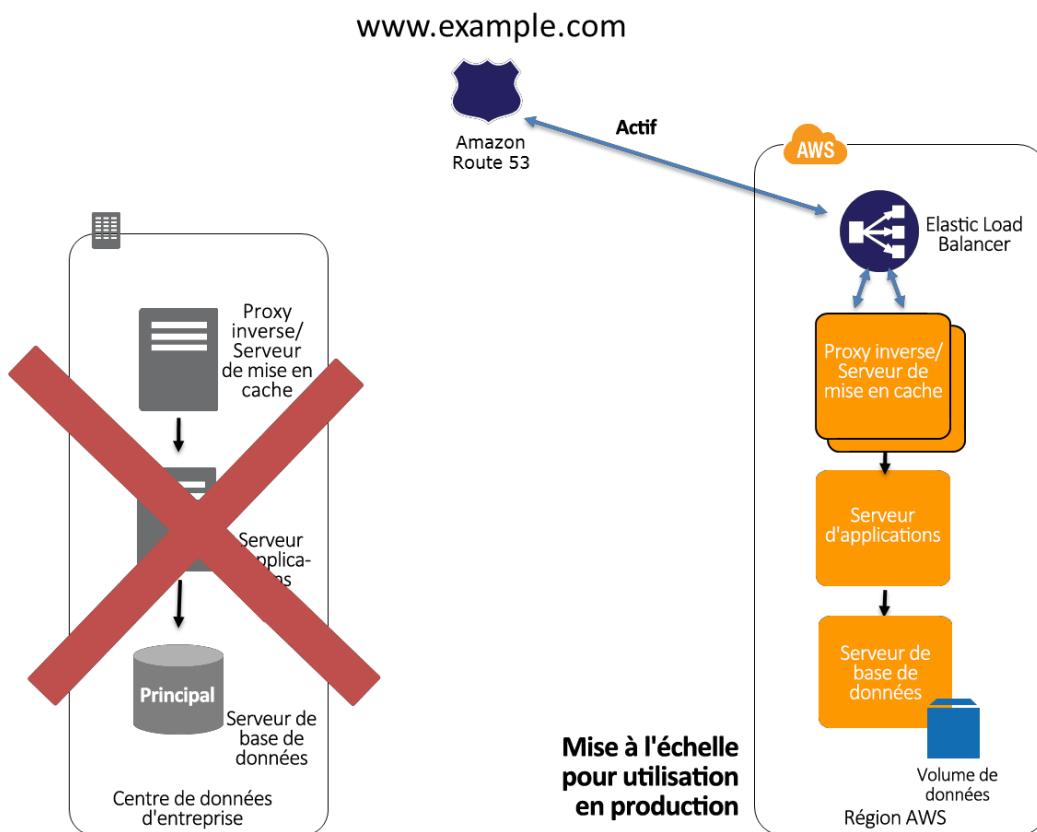


Figure 7 : Phase de récupération du scénario de secours « à chaud »

Principales étapes de récupération :

1. Augmentez la taille des flottes Amazon EC2 en service avec l'équilibrEUR de charge (dimensionnement horizontal).
2. Au besoin, démarrez les applications sur des types d'instances Amazon EC2 plus grandes (dimensionnement vertical).
3. Modifiez manuellement les enregistrements DNS ou utilisez les vérifications de l'état d'Amazon Route 53 pour que l'ensemble du trafic soit acheminé vers l'environnement AWS.
4. Envisagez de recourir à la fonction Auto Scaling pour dimensionner correctement la flotte ou pour répondre aux besoins liés à l'accroissement de la charge.
5. Augmentez la résilience ou la capacité de votre base de données.



Solution multi-site déployée sur AWS et sur site

Une solution multi-site fonctionne sur AWS, ainsi que sur l'infrastructure sur site, selon une configuration active/active. La méthode de réplication des données que vous utilisez dépend du point de reprise que vous choisissez. Pour plus d'informations sur les options de point de reprise, reportez-vous à la section [Objectif de délai de reprise et objectif de point de reprise](#) de ce livre blanc.

Outre les options de point de reprise, il existe plusieurs méthodes de réplication, telles que les méthodes synchrone et asynchrone. Pour plus d'informations, consultez la section [Réplication des données](#) de ce livre blanc.

Vous pouvez utiliser un service DNS compatible avec le routage du trafic pondéré, comme Amazon Route 53, pour acheminer le trafic de production vers les différents sites qui fournissent la même application ou le même service. Une proportion du trafic sera envoyée à votre infrastructure dans AWS, tandis que le reste sera transmis à votre infrastructure sur site.

En cas de catastrophe sur site, vous pouvez ajuster la pondération DNS et envoyer tout le trafic aux serveurs AWS. La capacité du service AWS peut être augmentée rapidement pour gérer la charge de production complète. Vous pouvez utiliser Amazon EC2 Auto Scaling pour automatiser ce processus. Vous aurez peut-être besoin d'une logique d'application pour détecter la défaillance des services de la base de données principale et pour les migrer vers les services de base de données parallèle exécutés sur AWS.

Le coût de ce scénario est déterminé par la proportion du trafic de production géré par AWS pendant le fonctionnement normal. Lors de la phase de récupération, vous payez uniquement les ressources utilisées au cours de la période pendant laquelle l'environnement de reprise après sinistre est le plus sollicité. Pour réduire davantage les coûts, vous pouvez acheter des instances réservées Amazon EC2 pour les serveurs AWS « toujours actifs ».

Phase de préparation

La figure suivante illustre comment vous pouvez utiliser la stratégie de routage pondéré du DNS Amazon Route 53 pour acheminer une portion du trafic vers le site AWS. L'application sur AWS accède parfois à des sources de données dans le système de production sur site. Les données sont répliquées ou mises en miroir sur l'infrastructure AWS.

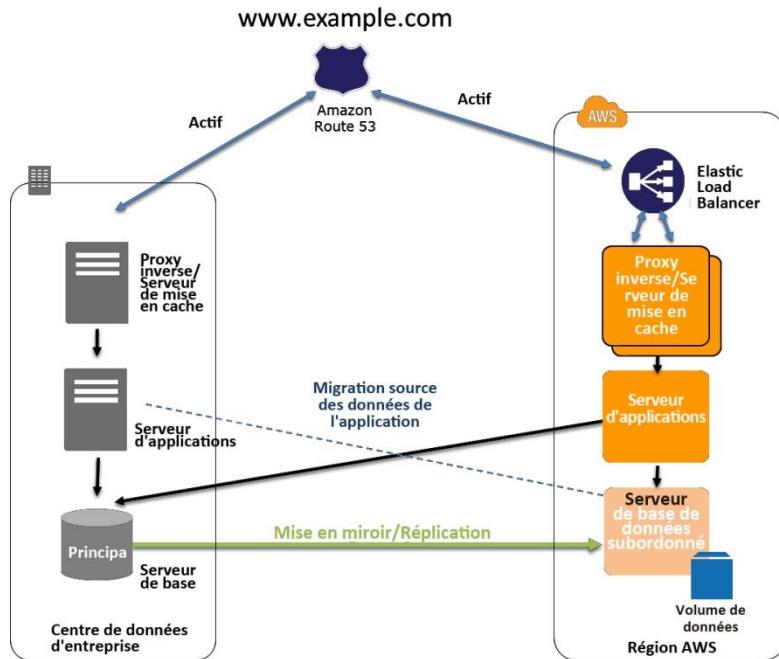


Figure 8 : Phase de préparation du scénario multi-site

Principales étapes de préparation :

1. Configurez l'environnement AWS pour dupliquer votre environnement de production.
2. Configurez la pondération DNS ou une technologie de routage du trafic similaire pour distribuer les demandes entrantes aux deux sites. Configurez le basculement automatique pour réacheminer le trafic à partir du site affecté.

Phase de récupération

La figure suivante illustre le changement de routage du trafic en cas de catastrophe sur site. Le trafic est envoyé à l'infrastructure AWS en mettant à jour le service DNS, et toutes les requêtes liées au trafic et aux données associées sont prises en charge par l'infrastructure AWS.

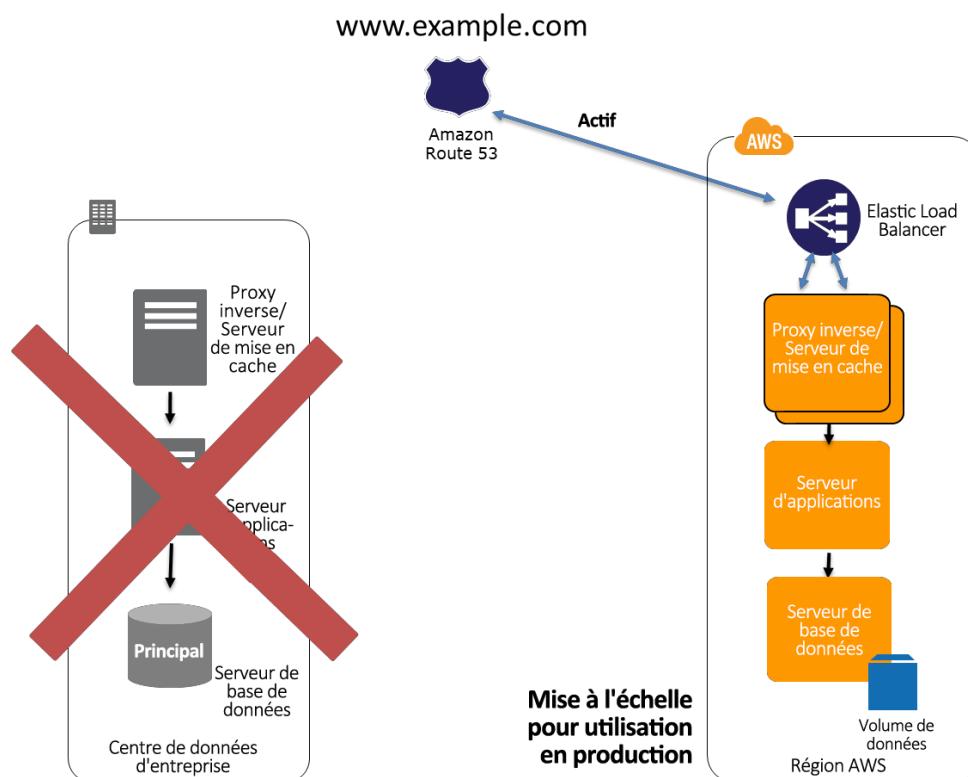


Figure 9 : Phase de récupération du scénario multi-site impliquant l'infrastructure sur site et l'infrastructure AWS

Principales étapes de récupération :

1. Modifiez, manuellement ou via le basculement DNS, la pondération DNS de sorte que toutes les demandes soient envoyées au site AWS.
2. Assurez-vous que la logique de l'application pour le basculement utilise les serveurs de base de données AWS locaux pour toutes les requêtes.
3. Pensez à utiliser Auto Scaling pour dimensionner automatiquement la flotte AWS.

Pour accroître davantage la disponibilité de votre solution multi-site, concevez des architectures à plusieurs zones de disponibilité. Pour plus d'informations sur la méthode de conception d'applications couvrant plusieurs zones de disponibilité, reportez-vous au livre blanc [Création d'applications tolérantes sur AWS](#).

Production AWS vers une solution de reprise après sinistre AWS via plusieurs régions AWS

Grâce à plusieurs zones de disponibilité, les applications déployées sur AWS ont une fonctionnalité multi-site. Ces zones sont des emplacements géographiques distincts conçus pour être isolés les uns des autres. Elles fournissent une connectivité réseau économique et à faible latence au sein de la même région.

Certaines applications nécessitent en plus le déploiement de leurs composants à l'aide de plusieurs régions. Cette exigence peut être réglementaire ou spécifique à l'entreprise elle-même.

Tous les scénarios précédents dans ce livre blanc peuvent être déployés à l'aide de régions AWS distinctes. Les avantages pour les scénarios de production et de reprise après sinistre sont les suivants :

- Vous n'avez pas besoin de négocier des contrats avec un autre fournisseur dans une autre région.
- Vous pouvez utiliser les mêmes technologies AWS sous-jacentes dans toutes les régions.
- Vous pouvez utiliser les mêmes outils ou API.

Pour plus d'informations, reportez-vous au livre blanc [Migration des ressources AWS vers une nouvelle région](#).

RéPLICATION DES DONNÉES

Lorsque vous répliquez des données sur un site distant, prenez en considération ces facteurs :

- **Distance entre les sites** : les longues distances impliquent généralement une latence ou une instabilité supérieure.
- **Bandé passante disponible** : étendue et variabilité des interconnexions.
- **Débit de données requis par votre application** : le débit de données doit être inférieur à la bande passante disponible.
- **Technologie de réPLICATION** : la technologie de réPLICATION doit être parallèle (de sorte à utiliser le réseau efficacement).

Il existe deux approches principales pour la réPLICATION des données : synchrone et asynchrone.

RéPLICATION SYNCHRONE

Les données sont toutes mises à jour à plusieurs emplacements. Cette approche implique une dépendance en matière de disponibilité et de performances du réseau. Dans AWS, les zones de disponibilité au sein d'une région sont bien connectées, mais physiquement séparées. Par exemple, dans un déploiement à plusieurs zones de disponibilité, Amazon RDS utilise la réPLICATION synchrone pour dupliquer les données dans une deuxième zone de disponibilité. De cette manière, les données ne sont pas perdues si la zone de disponibilité principale n'est pas disponible.

RéPLICATION ASYNCHRONE

Les données ne sont pas toutes mises à jour à plusieurs emplacements. Elles sont transférées dans la mesure où la disponibilité et les performances du réseau le permettent, et l'application continue d'écrire de données qui ne sont pas toujours entièrement répliquées.

Nombreux sont les systèmes de bases de données qui prennent en charge la réPLICATION des données asynchrone. Le réplica de base de données peut se trouver à distance et n'a pas besoin d'être complètement synchronisé avec le serveur de base de données principal. Cette approche est acceptable dans de nombreux scénarios, par exemple, en tant que source de sauvegarde ou dans les cas d'utilisation de création de rapports/en lecture seule. Outre les systèmes de bases de données, vous pouvez également l'appliquer aux systèmes de fichiers réseau et aux volumes de données.

Nous vous conseillons de bien connaître la technologie de réPLICATION utilisée dans votre solution logicielle. L'analyse détaillée des technologies de réPLICATION va au-delà du propos de ce livre blanc.



Les régions AWS sont totalement indépendantes les uns des autres, mais la procédure est la même pour y accéder et les utiliser. Vous pouvez ainsi créer des processus de reprise après sinistre qui couvrent des distances continentales, sans les problématiques ou les coûts que cela entraînerait normalement. Vous pouvez sauvegarder les données et les systèmes sur deux régions AWS ou plus, afin de permettre la restauration du service même en cas de catastrophes à très grande échelle. Vous pouvez également utiliser les régions AWS pour répondre aux besoins des utilisateurs à travers le monde avec une complexité des processus opérationnels relativement faible.

Se remettre d'un sinistre

Une fois que vous avez rétabli l'état de fonctionnement du site principal, vous devez restaurer le service normal. Selon votre stratégie de reprise après sinistre, cette procédure implique généralement l'inversion du flux de réPLICATION des données de sorte que toutes les mises à jour apportées aux données alors que le site principal était inaccessible puissent être répliquées, sans aucune perte de données. Les étapes suivantes décrivent les différentes approches de restauration :

Sauvegarde et restauration

1. Gelez toute modification des données sur le site de reprise après sinistre.
2. Procédez à une sauvegarde.
3. Restaurez la sauvegarde sur le site principal.
4. Redirigez les utilisateurs vers le site principal.
5. Annulez le gel des modifications.

Veilleuse, secours « à chaud » et multi-site

1. Effectuez la réPLICATION ou la mise en miroir inverse depuis le site de reprise après sinistre vers le site principal, une fois que ce dernier contient toutes les modifications.
2. Gelez toute modification des données sur le site de reprise après sinistre.
3. Redirigez les utilisateurs vers le site principal.
4. Annulez le gel des modifications.

Amélioration de votre plan de reprise après sinistre

Cette section décrit les étapes importantes à suivre afin de définir un plan de reprise après sinistre solide.

Test

Après la mise en place d'une solution de reprise après sinistre, vous devez la tester. Vous pouvez la tester fréquemment, ce qui est l'un des principaux avantages du déploiement sur AWS. L'expression « Game Day » désigne un basculement vers l'environnement de reprise après sinistre, en veillant à ce que la documentation soit suffisante pour faciliter le processus en cas de reprise après sinistre réelle. La mise en place d'un environnement dupliqué pour tester les scénarios Game Day est rapide et économique sur AWS. En général, vous n'avez pas à modifier votre environnement de production. Vous pouvez utiliser [AWS CloudFormation](#) pour déployer des environnements complets sur AWS. Cette approche utilise un modèle pour décrire les ressources AWS, ainsi que les dépendances ou paramètres d'exécution associés nécessaires à la création d'un environnement complet.

Il est essentiel de différencier les tests pour vous assurer que vous êtes bien protégé contre divers types de catastrophes. Voici des exemples de scénarios Game Day possibles :

- Coupure de courant au niveau d'un site ou d'un ensemble de serveurs
- Perte de connectivité réseau au niveau d'un seul site
- Virus qui se propage aux principaux services métier et qui affecte plusieurs sites
- Erreur d'un utilisateur, qui entraîne la perte de données et qui nécessite une restauration à un instant dans le passé

Surveillance et alertes

Il est important de mener des contrôles réguliers et de disposer d'un système de surveillance suffisant pour être averti lorsque l'environnement de reprise après sinistre est affecté par une panne de serveur, des problèmes de connectivité ou des erreurs d'applications. [Amazon CloudWatch](#) met à votre disposition des métriques sur les ressources AWS, ainsi que des métriques personnalisées qui peuvent être axées sur les applications, voire sur l'activité de l'entreprise elle-même. Vous pouvez configurer des alarmes basées sur des seuils définis au niveau de n'importe quelle métrique. De plus, le cas échéant, vous pouvez configurer Amazon SNS pour envoyer des alertes en cas de comportement inattendu.

Vous pouvez utiliser n'importe quelle solution de surveillance sur AWS, tout comme vous pouvez continuer d'utiliser les outils de surveillance et d'alerte auxquels votre société a recours pour surveiller les métriques de vos instances, ainsi que l'état des applications et les mesures liées aux systèmes d'exploitation invités.

Sauvegardes

Une fois que l'environnement de reprise après sinistre est en fonction, continuez à effectuer des sauvegardes régulières. En effet, il est essentiel de tester la sauvegarde et la restauration comme solution de secours.

AWS vous laisse la liberté de procéder à des tests fréquents et économiques de la reprise après sinistre sans que l'infrastructure correspondante n'ait besoin d'être toujours active.

Accès utilisateur

Pour sécuriser l'accès aux services et ressources dans l'environnement de reprise après sinistre, utilisez [AWS Identity and Access Management](#) (IAM). Avec IAM, vous pouvez créer des stratégies de sécurité qui isolent les responsabilités des utilisateurs et qui restreignent leur accès à certes ressources et tâches de cet environnement.



Accès au système

Vous pouvez également créer des rôles pour les ressources Amazon EC2, de sorte que seuls les utilisateurs associés à des rôles spécifiques puissent effectuer des actions définies dans votre environnement de reprise après sinistre, telles que l'accès à un compartiment Amazon S3 ou la redirection d'une adresse IP Elastic.

Automatisation

Vous pouvez automatiser le déploiement des applications sur les serveurs AWS et vos serveurs sur site via des logiciels de gestion des configurations ou d'orchestration. Cela vous permet de gérer facilement les modifications apportées aux applications ou à la configuration sur les deux environnements. Plusieurs logiciels d'orchestration connus s'offrent à vous. Pour obtenir une liste des prestataires de solution, consultez l'[annuaire des partenaires AWS](#).³

[AWS CloudFormation](#) s'associe à plusieurs outils pour mettre en service automatiquement les services d'infrastructure. Des niveaux supérieurs d'abstraction sont également disponibles avec [AWS OpsWorks](#) ou [AWS Elastic Beanstalk](#). L'objectif ultime est d'automatiser les instances autant que possible. Pour plus d'informations, consultez le livre blanc [Architecture du cloud : bonnes pratiques AWS](#).

Vous pouvez utiliser la fonction [Auto Scaling](#) afin de vous assurer que le pool d'instances est correctement dimensionné pour répondre aux besoins en fonction des métriques définies dans AWS CloudWatch. Autrement dit, en cas de reprise après sinistre, la solution s'adapte dynamiquement pour répondre à la demande plus élevée des utilisateurs à mesure qu'ils utilisent l'environnement. Lorsque l'événement de reprise après sinistre prend fin, si l'utilisation diminue, la solution s'adapte de sorte à utiliser un niveau minimal de serveurs.

Licences de logiciel et reprise après sinistre

Il est tout aussi important de vous assurer que vous disposez des licences appropriées pour votre environnement AWS que pour n'importe quel autre environnement. Pour faciliter la gestion des licences, AWS met à votre disposition différents modèles. Par exemple, le modèle « Bring Your Own License » (Licence à fournir) est possible pour plusieurs composants logiciels ou systèmes d'exploitation. Il existe également une gamme de logiciels pour lesquels le coût des licences est inclus dans le tarif horaire. Il s'agit du modèle « Licence incluse ».

Le modèle « Bring your Own License » vous permet d'utiliser vos logiciels existants en cas de catastrophe. Le modèle « Licence incluse » réduit les coûts de licence initiaux d'un site de reprise après sinistre qui ne sert pas tous les jours.

En cas de questions ou de doutes sur vos licences ou sur leur mode d'application dans AWS, veuillez contacter le revendeur des licences concernées.

Conclusion

Il existe de nombreuses options et variations pour la reprise après sinistre. Ce livre blanc décrit certains des scénarios les plus courants, allant d'une simple opération de sauvegarde et de restauration à des solutions multi-sites tolérantes aux pannes. AWS vous offre un contrôle granulaire et de nombreux composants afin de vous permettre de créer la solution de reprise après sinistre qui vous convient, conformément à votre budget, ainsi qu'à vos objectifs RTO et RPO. Les services AWS sont disponibles à la demande, et vous ne payez que ce que vous utilisez. Cette approche est idéale pour la reprise après sinistre, qui nécessite la mise à disposition d'une infrastructure significative très rapidement, mais seulement en cas de catastrophe.

Ce livre blanc vous a décrit dans quelle mesure AWS offre des solutions d'infrastructure flexibles et économiques vous permettant d'optimiser l'efficacité de vos plans de reprise après sinistre.

³ La liste des prestataires de solution est disponible sur <http://aws.amazon.com/solutions/solution-providers/>

Suggestions de lecture

- *Guide de démarrage d'Amazon S3* : <http://docs.amazonwebservices.com/AmazonS3/latest/gsg/>
- *Guide de démarrage d'Amazon EC2* :
<http://docs.amazonwebservices.com/AWSEC2/latest/GettingStartedGuide/>
- Annuaire des partenaires AWS (pour une liste des prestataires de solution) :
<http://aws.amazon.com/solutions/solution-providers/>
- Centre de sécurité et de conformité AWS : <http://aws.amazon.com/security/>
- Centre d'architecture AWS : <http://aws.amazon.com/architecture>
- Livre blanc : [Conception d'applications tolérantes aux pannes dans le Cloud AWS](#)
- Autres livres blancs techniques AWS : <http://aws.amazon.com/whitepapers>

Révisions de documents

Nous avons apporté les modifications ci-dessous à ce livre blanc depuis sa publication initiale en janvier 2012 :

- Mise à jour des informations sur les régions AWS
- Ajout d'informations sur les nouveaux services : Amazon Glacier, Amazon Redshift, AWS OpsWorks, AWS Elastic Beanstalk et Amazon DynamoDB
- Ajout d'informations sur les interfaces réseau Elastic
- Ajout d'informations sur diverses fonctions des services AWS pour les scénarios de reprise après sinistre incluant plusieurs régions AWS
- Ajout d'informations sur les bibliothèques de bandes virtuelles AWS Storage Gateway (VTL)