Engineer

# Reprise après sinistre

rétablir le service après une perte grave avec un plan testé

## Ce que c’est

La reprise après sinistre est la partie de la planification des mesures d’urgence qui couvre le pire cas : le lieu d’exploitation d’un système est perdu ou reste inaccessible longtemps, et le système doit être reconstruit ailleurs à partir de copies. Le guide de planification des mesures d’urgence pour les systèmes d’information fédéraux du NIST, SP 800-34 révision 1 de 2010, définit le plan de reprise après sinistre comme un plan écrit permettant de rétablir un ou plusieurs systèmes d’information sur un autre site après une panne matérielle ou logicielle majeure ou la destruction des installations. Son périmètre est étroit. Le guide le réserve aux perturbations majeures, généralement physiques, qui interdisent durablement l’accès au site principal ; il ne couvre que celles qui imposent une relocalisation.

Ce périmètre le distingue des plans voisins. Dans le vocabulaire du guide, un plan de secours d’un système d’information rétablit un système unique là où il se trouve, après la panne d’un disque ou la corruption d’une base, par exemple. Le plan de reprise après sinistre est lié à un site : il déplace l’exploitation vers le site de repli, où chaque système est remis en service selon son propre plan de secours. Le plan d’une base et celui de la perte de tout un centre de données, d’une région cloud ou d’un compte fournisseur sont des documents distincts, avec des responsables distincts. Les confondre conduit une entreprise à ne disposer ni de l’un ni de l’autre.

Trois mesures transforment une intention en plan vérifiable. La durée maximale d’interruption tolérable, MTD, est la durée totale de panne que le responsable du système accepte. L’objectif de délai de reprise, RTO, est la durée maximale d’indisponibilité d’une ressource avant que les dommages aux autres systèmes et à l’activité deviennent inacceptables. Comme le travail interrompu doit ensuite être retraité, le guide indique que le RTO doit normalement être inférieur à la MTD. L’objectif de point de reprise, RPO, regarde en arrière : c’est l’instant

antérieur à la panne auquel les données peuvent être rétablies depuis la copie de sauvegarde la plus récente. Il exprime la quantité de données perdues que l'entreprise peut accepter. En termes simples, le RTO est la durée d'interruption, et le RPO la quantité de travail perdue.

Les sites de repli se répartissent en plusieurs catégories. Un site froid ne fournit que l'espace et l'infrastructure ; un site tiède est partiellement équipé ; un site chaud est entièrement équipé et doté de personnel. Le guide ajoute les sites mobiles, qui peuvent souvent être livrés sous 24 heures avant le début de leur installation, et les sites en miroir, l'option la plus coûteuse à laquelle il attribue « pratiquement 100 % de disponibilité ». Les sites froids sont les moins chers à maintenir, mais leur équipement peut prendre beaucoup de temps. Pour la plupart des logiciels actuels, une seconde région cloud ou un second fournisseur joue le même rôle. L'arbitrage entre ce qui est prêt et le coût de ce maintien en état de disponibilité reste le même.

Utilisez le concept pour prendre une décision

Utilisez « Qu'est-ce que la reprise après sinistre ? » pour éclairer une décision réelle. Nous pouvons vous aider à relier ce concept au système que vous construisez ou achetez. Des sauvegardes testées plutôt que supposées fiables, et un plan écrit pour le matin où un serveur ne redémarre pas.

**Découvrir nos prestations** Contactez-nous →

Vérifiez les hypothèses derrière le terme

Appuyez-vous sur l'explication et les réalisations liées pour formuler les questions de votre projet. Nous pouvons examiner les hypothèses avec vous avant le choix d'un outil. 100 sauvegardes critiques automatisées : Barman — 100 sauvegardes critiques automatisées dans les bases

**100 sauvegardes critiques automatisées : Barman** Contactez-nous →

## Pourquoi c'est important

Une sauvegarde est une copie, et une copie seule ne fait rien fonctionner. Passer de la copie à un système opérationnel exige aussi le logiciel qui la lit, les clés qui la déchiffrent, des serveurs et un réseau pour l'exécuter, la configuration qui les relie et une personne qui connaît l'ordre des opérations. Tout élément qui n'existait que sur le site perdu a disparu avec lui. La reprise après sinistre consiste à s'assurer que tous survivent au même événement et que le chemin de la copie au service a déjà été parcouru avant que quelqu'un en ait besoin.

Les données récupérables ne sont pas plus récentes que la dernière copie effectivement restaurable, quel que soit le RPO que le calendrier des sauvegardes doit respecter. Une tâche nocturne échouant silencieusement depuis une semaine met en péril les données d'une semaine, quoi qu'annonce la politique écrite. Le guide du NIST fait la même remarque pour les bandes : il

recommande des tests réguliers pour confirmer le stockage correct des données et la récupération des fichiers sans erreur ni perte. Un voyant vert sur une tâche de sauvegarde prouve que quelque chose a été écrit. Seule une restauration prouve qu'on peut le relire.

Le plan se dégrade aussi. Des personnes partent, des serveurs sont remplacés, les fournisseurs refont leurs consoles et les mots de passe du guide d'exploitation expirent. Parmi les sept étapes de planification du NIST, les deux dernières sont les tests, la formation et les exercices, puis la maintenance du plan. Le guide demande un document vivant, révisé au moins chaque année et lorsque le système ou les ressources de reprise changent sensiblement. Un plan jamais mis à l'épreuve échoue souvent sur des détails que personne n'a pensé à écrire : l'ordre de démarrage des services, un enregistrement DNS dont la durée de vie en cache est d'une journée, l'unique identifiant d'accès conservé sur la machine disparue.

Pour les équipes logicielles, le sinistre touche souvent un compte plutôt qu'un bâtiment. Projet cloud supprimé, accès administrateur compromis, compte fournisseur suspendu ou commande destructrice lancée en production : chacun retire l'accès au système aussi complètement qu'une inondation. Des serveurs de secours ne protègent pas contre le dernier cas ; ils appliquent un `DROP TABLE` erroné en quelques instants, aussi fidèlement que toute autre modification.

## À quoi cela ressemble en pratique

Pour PostgreSQL, une fenêtre de perte de données bien plus courte que l'intervalle entre deux sauvegardes est possible grâce à l'archivage continu du journal d'écriture anticipée, WAL, en complément d'une sauvegarde de base. Le serveur copie chaque segment WAL terminé vers un endroit sûr. La restauration rejoue ensuite ces segments sur la sauvegarde de base jusqu'à tout instant choisi depuis sa réalisation :

```
# postgresql.conf on the protected server
wal_level = replica
archive_mode = on
archive_command = 'test ! -f /mnt/archive/%f && cp %p /mnt/archive/%f'
```

Pour restaurer, on extrait une sauvegarde de base dans un répertoire de données neuf, on y place un fichier vide nommé `recovery.signal` et les paramètres de reprise indiquent où se trouve l'archive et où s'arrêter :

```
restore_command = 'cp /mnt/archive/%f %p'
recovery_target_time = '2026-03-10 17:14:00+01'
recovery_target_action = 'pause'
```

La documentation PostgreSQL raconte le cas auquel répondent ces paramètres : une personne supprime une table essentielle un mardi soir à 17 h 15, s'en aperçoit le mercredi à midi et restaure à 17 h 14. La pause est l'action préconfigurée une fois la cible atteinte, pour que des requêtes confirment le bon instant avant que le serveur soit promu pour accepter les connexions. Sinon, le serveur est arrêté, reçoit une cible ultérieure et redémarre. L'instant de reprise doit être postérieur à la fin de la sauvegarde de base. La documentation conseille de configurer et de tester l'archivage avant la première sauvegarde de base. Une fois la reprise terminée, le serveur supprime `recovery.signal` pour ne pas recommencer accidentellement en mode reprise.

Engineer ApS propose une prestation de sauvegarde et de reprise après sinistre, présentée comme des sauvegardes testées plutôt que présumées bonnes et un plan écrit pour le matin où un serveur ne redémarre pas. Deux pages du portfolio l'illustrent. Dans les sauvegardes et la reprise après sinistre sous forme de code, travail réalisé dans le cadre d'un poste occupé depuis 2025, la conservation des sauvegardes était définie dans Bicep à côté de la base. La restauration à un instant donné fait ainsi partie du modèle plutôt que d'un paramètre activé un jour dans un portail. L'environnement de la base était lui aussi défini par le code : une base restaurée dans un environnement reconstruit de mémoire est à peine rétablie. La situation de reprise a ensuite été auditée et consignée, lacunes comprises : géoredondance désactivée et objectif de délai de reprise proposé plutôt que mesuré, puisqu'aucun exercice n'avait eu lieu.

L'automatisation des sauvegardes et des tests de restauration de l'entreprise était conçue pour étendre la reprise au-delà d'un instantané fournisseur. Un rôle Ansible installe des scripts restic et des unités systemd pour exporter la base lorsque cette option est configurée, produire des instantanés chiffrés et dédupliqués vers le stockage d'un autre fournisseur par SFTP, purger les sauvegardes selon la politique de conservation et vérifier l'intégrité. Un processus mensuel distinct restaure un fichier connu dans un emplacement temporaire et compare ses octets. Sauvegarde et restauration ont des signaux

de réussite séparés ; la phrase secrète provient d'un fichier protégé et les temporisateurs dépendent d'un dépôt configuré. Ces contrôles sont implémentés ; une reprise réelle reste un livrable distinct. Le dossier d'implémentation du 2026-10-27 indique que les temporisateurs étaient désactivés faute de dépôt et ne consigne aucune restauration réelle terminée. Il étaye donc le travail d'automatisation, pas un engagement de délai de reprise ni l'affirmation que l'entreprise pourrait déjà perdre son hôte sans risque.

## Où les problèmes surviennent

**La sauvegarde n'a jamais été restaurée.** Une tâche annonçant un succès chaque nuit ne dit pas si sa sortie peut être lue, déchiffrée et chargée. La première restauration réelle est un mauvais moment pour le découvrir. Planifiez les restaurations comme les sauvegardes : un contrôle automatisé extrait et compare des données connues, et une restauration complète dans un environnement propre est réalisée assez souvent pour que sa durée soit mesurée.

**La copie partage le sort de l'original.** Un instantané dans le même compte cloud, un disque de sauvegarde dans le même rack ou un bucket d'archives derrière le même accès administrateur disparaît avec ce qui frappe le primaire. Le guide du NIST demande de choisir le stockage hors site et les sites de repli selon leur faible probabilité d'être touchés par le même sinistre. Conservez au moins une copie chez un autre fournisseur ou dans un autre compte avec des identifiants distincts. Gardez les clés de déchiffrement à un endroit qui ne dépend pas des systèmes qu'elles protègent.

**Seules les données ont été prévues.** Restaurer une base n'est qu'une petite partie de la remise en service si serveurs, règles de pare-feu, DNS, certificats et secrets doivent être recréés de mémoire. Définissez l'environnement dans du code d'infrastructure suivi en gestion de versions et intégrez sa reconstruction à l'exercice, au-delà du simple chargement des données.

**Les objectifs sont des suppositions.** Un RTO écrit sans exercice pour l'étayer est une proposition ; un RPO supposant la réussite de chaque sauvegarde est optimiste. Mesurez les deux en exercice. Le NIST distingue les exercices sur table, limités à la discussion sans déployer d'équipement, des exercices fonctionnels simulant l'exploitation, jusqu'aux exercices à pleine échelle couvrant chaque élément du plan. Les chiffres viennent du second type.

**Un serveur de secours compte comme sauvegarde.** Un serveur de secours ou une base géorépliquée protège contre la perte de matériel, mais copie les suppressions, la corruption et les fichiers chiffrés par rançongiciel aussi fidèlement que les écritures correctes. Gardez des copies à des instants donnés qu'une erreur sur le primaire ne peut atteindre et conservez-les plus longtemps qu'il ne faut habituellement pour remarquer une erreur.

**Le plan décrit le système de l'an dernier.** Un guide d'exploitation énumérant des serveurs retirés, des personnes parties et des mots de passe inutilisables ralentit la reprise au lieu de la guider. Révisez le plan après chaque changement important et chaque exercice, consignez les erreurs révélées par l'exercice et réexaminez encore plus souvent les parties les plus changeantes, comme les listes de contacts, ainsi que le recommande aussi le NIST.

## Pour aller plus loin

- SP 800-34 révision 1 : guide de planification des mesures d'urgence pour les systèmes d'information fédéraux — le guide complet : définition et périmètre du plan de reprise après sinistre, sept étapes, MTD, RTO et RPO, sites de repli et types d'exercices, avec des modèles de plans.
- Archivage continu et restauration à un instant donné (PITR) — le chapitre de PostgreSQL 18 sur l'archivage WAL, les sauvegardes de base et la restauration à un instant choisi.
- Journal d'écriture anticipée — la référence de configuration pour `archive_command` , `restore_command` et les paramètres de cible de reprise.

Glossaire

Choisissez selon vos contraintes réelles

Présentez le parcours de déploiement, les risques opérationnels et les personnes d'astreinte. Nous pouvons définir un changement avec des vérifications, une procédure de reprise et une responsabilité claire.

**Consulter les tarifs** Contactez-nous →

# Rendez la terminologie concrète

Demandez comment « Qu'est-ce que la reprise après sinistre ? » s'applique à votre organisation. Un exemple concret tiré de votre système actuel suffit pour engager la discussion.

Découvrir nos prestations

welcome@engineer.company +45 50 10 61 84 Copenhague, Danemark

Emportez cette page avec vous

Fiche de contact

Créé avec soin et amour par D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Droit d'auteur © 2025 – aujourd'hui · Engineer ApS · Tous droits réservés.

Imprimé depuis https://engineer.company/fr/glossary/disaster-recovery/