Instances - Modèle de responsabilité partagée

Sur cette page, nous décrivons les rôles et responsabilités liés à la maintenance et à la sécurisation de vos instances virtuelles et GPU. Notre modèle de responsabilité partagée clarifie la répartition des tâches entre Scaleway et nos utilisateurs, garantissant ainsi une gestion claire de la disponibilité, des sauvegardes, des configurations et des mesures de sécurité des instances. En comprenant cette responsabilité partagée, vous pouvez optimiser les performances, la fiabilité et la sécurité de vos services d'instances CPU et GPU Scaleway.

Présentation du modèle « Sécurité du cloud vs sécurité dans le cloud »

Chez Scaleway, la sécurité de vos données et applications est primordiale. Afin de garantir un environnement robuste et sécurisé, nous fonctionnons selon un modèle de responsabilité partagée, qui distingue clairement les obligations de Scaleway de celles de nos utilisateurs. Ce modèle est souvent conceptualisé sous les termes « sécurité du cloud » et « sécurité dans le cloud ».

Sécurité *du* Cloud (responsabilité de Scaleway)

Scaleway est responsable de la sécurité du Cloud. Cela signifie que nous nous engageons à protéger l'ensemble de l'infrastructure qui fait fonctionner tous les services proposés dans le Cloud Scaleway. Nos responsabilités comprennent :

- Sécurité physique des centres de données : protection des installations, contrôle d'accès, surveillance.
- Sécurité de l'infrastructure réseau : protection des réseaux, des plateformes et des systèmes d'exploitation qui sous-tendent nos services.
- La sécurité de la virtualisation : isolation des ressources, hyperviseurs et gestion des environnements virtuels.
- La maintenance et les mises à jour de l'infrastructure : application des correctifs de sécurité et des mises à jour pour les composants gérés par Scaleway.
- La conformité et les certifications : maintien de nos propres certifications (par exemple, ISO 27001, HDS) et respect des réglementations applicables à notre rôle de fournisseur de services cloud.

En d'autres termes, Scaleway est responsable de la protection de l'environnement dans lequel résident vos instances.

Sécurité *dans le* cloud (responsabilité de l'utilisateur)

L'utilisateur est responsable de la sécurité dans le cloud. Une fois que les ressources sont mises à votre disposition, vous êtes responsable de la sécurité de tout ce que vous déployez, configurez et gérez dans cet environnement. Vos responsabilités comprennent :

- Gestion des instances : configuration du système d'exploitation, applications, middleware, correctifs et mises à jour logicielles pour vos instances.
- Gestion des données : chiffrement des données (au repos et en transit), gestion des sauvegardes, intégrité et confidentialité de vos informations.
- Gestion des identités et des accès (IAM) : configuration des autorisations, des rôles, des clés SSH, de l'authentification multifactorielle (MFA) et du principe du moindre privilège pour accéder à vos ressources.
- Sécurité réseau de vos instances : configuration des pare-feu, des groupes de sécurité et de l'accès réseau pour vos instances.
- Sécurité des applications : protection de vos applications contre les vulnérabilités, gestion des dépendances et surveillance des journaux d'application.
- Conformité de vos charges de travail : garantie que vos applications et vos données sont conformes aux réglementations du secteur et à vos propres politiques de sécurité internes.

Ce modèle de responsabilité partagée est essentiel pour une approche globale et efficace de la sécurité. Il vous permet de tirer parti de la robustesse de l'infrastructure Scaleway tout en conservant la flexibilité et le contrôle nécessaires pour sécuriser vos propres charges de travail. Une compréhension claire de ces rôles garantit que tous les aspects de la sécurité sont pris en compte.

Résilience des produits

Disponibilité

Les mesures et garanties détaillées des SLA sont disponibles dans l'accord de niveau de service pour les services Scaleway Instances.
Une fois que la ressource est entre vos mains, nous n'avons plus accès à la machine et ne pouvons donc plus surveiller son fonctionnement. En cas de problème opérationnel, nous vous invitons à consulter notre documentation ou à créer un ticket auprès de notre équipe d'assistance. Nous ferons alors tout notre possible pour que vous puissiez retrouver l'accès à vos ressources dans les plus brefs délais.

Sauvegardes et instantanés

Vous êtes entièrement responsable de la gestion de votre machine virtuelle et de ses données.
Il vous appartient d'assurer la redondance des données si nécessaire, en vous appuyant sur des sauvegardes ou des instantanés d'instance.

Il vous appartient de définir les mesures de redondance nécessaires en fonction de la nature et du niveau de criticité de vos données. Nous vous rappelons qu'un instantané ne constitue en aucun cas une sauvegarde permanente de vos données, mais seulement une copie « instantanée » de l'instance.

Les volumes de stockage en bloc sont répliqués trois fois afin d'offrir une disponibilité de redondance de stockage de 99,99 %.

Toutefois, lorsque vous utilisez le stockage local et le stockage temporaire et en cas de panne de disque ou de matériel sur l'hyperviseur sous-jacent, nous ne pouvons garantir que vous retrouverez l'accès à votre machine virtuelle et à vos données sur le stockage local. La panne peut nécessiter le remplacement complet de la machine virtuelle. Il est donc de votre responsabilité de vous assurer à l'avance que vous disposez d'une sauvegarde ou d'une redondance de vos données sur une autre instance ou un autre moyen de stockage. Nous ne pouvons être tenus responsables de la perte de vos données.
Les sauvegardes et les snapshots doivent être configurés et gérés par vos soins. Veuillez vous reporter à notre documentation pour obtenir de l'aide sur la configuration des sauvegardes pour les instances via l'interface CLI/API ou la console Scaleway . La restauration des snapshots ou des sauvegardes doit être déclenchée par vos soins.

Performances du stockage en bloc et bande passante des instances

Les volumes de stockage en bloc sont disponibles avec 5 000 ou 15 000 IOPS (opérations d'entrée/sortie par seconde). Les performances de stockage réelles sont déterminées par la bande passante de blocs disponible pour chaque type d'instance. Tous les types d'instances compatibles avec le stockage en bloc prennent en charge les deux types de volumes de stockage en bloc, mais les performances peuvent varier en fonction de la bande passante de blocs disponible.
Reportez-vous à la présentation de la bande passante Internet et du stockage en bloc des instances Scaleway pour les instances virtuelles et à la présentation de la bande passante Internet et du stockage en bloc des instances GPU Scaleway pour les instances GPU.

Configuration et gestion des versions

Installation et configuration

Nous proposons une gamme de distributions Linux et Windows pour l'installation automatique d'images depuis la console Scaleway. Ces distributions sont fournies avec une configuration par défaut conçue pour des cas d'utilisation standard, garantissant sécurité, efficacité d'utilisation et fiabilité. Lors de la configuration de votre machine, vous pouvez modifier et personnaliser cette configuration initiale. Cependant, vous êtes responsable de tout impact sur la disponibilité, la sécurité ou les performances de votre instance.
Si vous utilisez une image personnalisée, il vous incombe de garantir une configuration fiable et sécurisée de votre machine. Une image personnalisée est une image disque créée par l'utilisateur

avec un système d'exploitation, des logiciels ou des paramètres préconfigurés. Elle permet aux utilisateurs de déployer de nouvelles instances avec leur environnement déjà configuré, au lieu d'utiliser une image standard ou InstantApp.

Mises à jour et gestion des versions

Nous fournissons régulièrement des mises à jour de la version du système d'exploitation, vous permettant ainsi de mettre à niveau votre environnement si vous le souhaitez. Il est de votre responsabilité de mettre à jour votre machine vers la version souhaitée et ainsi de maintenir sa compatibilité avec toutes les ressources internes et externes de Scaleway.
Si vous effectuez des mises à niveau manuelles sans réinstaller votre machine à partir d'une image fournie par Scaleway, il est de votre responsabilité de garantir la fiabilité et la stabilité de la configuration de votre machine.

Mises à niveau de l'API/CLI Scaleway et changements majeurs

Dans le cadre de nos efforts continus pour améliorer et renforcer les fonctionnalités des instances Scaleway, nous pouvons publier des mises à jour de notre API susceptibles d'introduire des changements majeurs. Ces changements peuvent affecter la compatibilité des anciennes versions de notre interface de ligne de commande (CLI), des scripts, des automatisations ou des outils de développement (devtools) utilisés par nos utilisateurs.
Il incombe à l'utilisateur de surveiller activement les mises à niveau potentielles et de s'assurer que sa version de l'interface CLI, ainsi que tous les scripts, automatisations ou outils de développement qu'il utilise pour interagir avec l'API des instances Scaleway, sont régulièrement mis à jour vers la dernière version disponible. Cela inclut, sans s'y limiter :

- Maintenir l'interface CLI à jour avec les dernières versions
- Mettre à jour les scripts et automatisations personnalisés afin qu'ils soient compatibles avec les dernières versions de l'API
- S'assurer que tous les outils de développement ou intégrations tiers tels que Terraform ou Packer sont compatibles avec les dernières versions de l'API publiées par Scaleway.

Conformité d'utilisation

Vous êtes responsable de l'utilisation correcte de vos ressources. À cet égard, vous êtes tenu de veiller à ce que l'utilisation de vos instances soit conforme à la politique de conformité et aux conditions d'utilisation de Scaleway, ainsi qu'à celles des différents systèmes d'exploitation que vous utilisez.
Important
Il vous incombe de vous informer au préalable des cas d'utilisation autorisés et interdits pour vos instances et de vous y conformer tout au long de votre utilisation.

Protection des données

Chiffrement en transit

Les instances (CPU et GPU) prennent en charge les connexions SSH afin de sécuriser vos communications avec elles. Vous restez responsable de la configuration des clés SSH.

Chiffrement des données

Vous êtes responsable du chiffrement des volumes sur votre instance. Nous ne sommes pas responsables du chiffrement des données, en particulier dans le cas d'applications sensibles ou d'exigences de sécurité supplémentaires.
Pour plus d'informations, consultez notre documentation sur le chiffrement des volumes pour les données sensibles.

Suppression des données

Stockage local : lorsque vous supprimez votre instance, nous sommes responsables de la suppression de toutes vos données sur le stockage local de l'instance.
Stockage temporaire : la clé de chiffrement du stockage temporaire de votre instance est supprimée et ne peut pas être restaurée après la suppression. Les données du disque sont donc rendues indisponibles lors de la suppression.
Stockage en bloc : les volumes de stockage en bloc restent, par défaut, attachés à votre compte avec les données qui y sont stockées. Pour supprimer des volumes de stockage en bloc, vous pouvez demander explicitement la suppression des volumes lors de la suppression de l'instance. S'ils ne sont pas supprimés, les volumes restent dans votre compte pour une utilisation ultérieure (réattribution à une instance nouvelle ou existante) ou jusqu'à ce que vous demandiez leur suppression.

Accès Scaleway

Nous n'avons pas la capacité technique d'accéder à votre machine virtuelle une fois qu'elle est installée, ni aux données qui y sont stockées. Nous n'avons aucune visibilité sur votre utilisation de l'instance et sa configuration. Il vous appartient donc d'assurer la sécurité de votre machine virtuelle et de vos données.

Gestion des identités et des accès

Les instances virtuelles (CPU et GPU) fournissent des ensembles d'autorisations IAM qui autorisent ou restreignent certaines actions qu'un utilisateur ou une application peut effectuer, telles que la création ou la suppression d'instances. Vous restez responsable de l'attribution de ces autorisations aux utilisateurs ou applications concernés et de la vérification fréquente de ces accès.
La gestion des accès et des autorisations pour la création, la modification, l'utilisation et la suppression d'une ressource reste dans tous les cas votre responsabilité.

Sécurité de la plateforme

Nos garanties en matière de sécurité sont disponibles à l'adresse https://www.scaleway.com/en/security-and-resilience/, et nos certifications et engagements sont disponibles dans notre Centre de confiance.

Meilleures pratiques en matière de sécurité

Pour une sécurité optimale, nous vous recommandons :

- d'utiliser une clé SSH ED25519 pour accéder à votre machine, plutôt que l'authentification par nom d'utilisateur et mot de passe,
- de vérifier et de mettre à jour le pare-feu et les règles de filtrage si nécessaire (en suivant le principe du moindre privilège : « Tout refuser par défaut, autoriser par exception »),
- configurer des groupes de sécurité pour vos instances afin de limiter leur exposition sur Internet,
- mettre régulièrement à jour le système d'exploitation afin de bénéficier des mises à jour de configuration et des correctifs de sécurité,
- consulter régulièrement notre journal des modifications et notre documentation pour connaître les mises à jour des modifications de l'API et mettre à jour régulièrement les outils d'automatisation et l'interface CLI afin d'éviter les modifications importantes passées inaperçues.

HDS (Hébergement de Données de Santé) - Documentation complète

Cette section regroupe toutes les informations et exigences spécifiques à l'HDS en matière de conformité de l'hébergement des données de santé.

Résidence des données HDS

- Instances HDS : limitées à la France. Les données ne doivent pas être transférées en dehors du périmètre autorisé.
- Responsabilité de Scaleway : garantir techniquement que les données restent dans les datacenters parisiens autorisés et ne pas modifier la localisation choisie par le client lors de l'allocation des ressources.
- Responsabilité du client : ne pas configurer de transfert vers d'autres régions. Ne pas utiliser ni créer d'instances dans des régions non HDS pour votre infrastructure HDS, ni d'instances non HDS.

Exigences de conformité HDS

En tant qu'utilisateur d'instances HDS, vous êtes tenu de :

- Signer le contrat HDS de Scaleway,
- Veiller à ce que l'accès soit réservé au personnel autorisé,
- Respecter les offres d'instances autorisées, y compris les exigences en matière de stockage.
- Utiliser Audit Trail à des fins de provisionnement des journaux.

Responsabilité de Scaleway : fournir une infrastructure certifiée HDS et faire tout son possible pour maintenir la certification. La perte du certificat peut entraîner la résiliation de notre relation commerciale avec le client HDS. Ces éléments sont inclus dans le contrat HDS.

Chiffrement HDS

En tant qu'utilisateur d'instances HDS, vous êtes responsable de :

- Mettre en œuvre les mesures techniques et organisationnelles appropriées en fonction de vos politiques de sécurité associées
- Chiffrer vos données au repos et en transit sur les réseaux publics et privés
- Vous assurer que les services que vous utilisez sont compatibles avec les solutions de chiffrement que vous prévoyez d'utiliser.

Offres d’instances HDS

Offres d'instances autorisées

Configuration Type	Eligible for HDS purposes ?	Authorized type of storage
Autres instances SLO (DEV1, GP1, PLAY2, PRO2, COPARM1, ENT1)	Non	N/A
Instances Development	Oui	Block storage (i.e. aucun stockage local autorisé) Local storage (responsabilité du Client de chiffrer)

Instances Shared General Purpose	Oui	Block storage (i.e. aucun stockage local autorisé) Local storage (responsabilité du Client de chiffrer)
Instances Dedicated General Purpose	Oui	Block storage (i.e. aucun stockage local autorisé) Local storage (responsabilité du Client de chiffrer)
Instances Specialized	Oui	Block storage (i.e. aucun stockage local autorisé) Local storage (responsabilité du Client de chiffrer)
Instances GPU	Oui	Block storage Scratch storage Local storage (responsabilité du Client de chiffrer)

Responsabilités :

Client : Veiller à ce que seules les offres éligibles soient utilisées et comprendre les obligations relatives aux options de stockage.

Suppression de données HDS

Lorsque vous supprimez une instance HDS, les volumes de blocs restent, par défaut, associés à votre compte. Pour supprimer des volumes de stockage en blocs, vous pouvez demander explicitement la suppression des volumes lors de la suppression de l'instance.

Client : demandez explicitement la suppression des volumes de stockage en blocs lors de la suppression d'une instance HDS.

Sauvegardes et reproduction HDS

Vous êtes responsable de la gestion de vos besoins en matière de sauvegarde et de reproduction, tout en respectant la résidence des données (France uniquement) sur vos services Scaleway HDS. **Remarque importante :** les instantanés ne sont pas disponibles sur le stockage temporaire.