Modèle de responsabilité partagée : Services Kubernetes gérés par Scaleway (Kapsule et Kosmos)

Les services Kubernetes managés de Scaleway, Kapsule et Kosmos, fournissent un plan de contrôle entièrement géré et les composants d'écosystème associés nécessaires à l'exécution de clusters Kubernetes. Scaleway simplifie de nombreuses tâches opérationnelles afin d'alléger la charge de travail de ses clients, qui restent toutefois responsables de la sécurité, de la configuration et de l'exploitation de leurs charges de travail et de leurs clusters.

Ce modèle clarifie les responsabilités dans les catégories suivantes :

- **"Sécurité du Cloud"**: responsabilité de Scaleway
- **"Sécurité dans le Cloud"**: responsabilité du client
- **Responsabilités spécifiques aux services Kapsule et Kosmos**
- **Dispositions spécifiques pour HDS** (Health Data Hosting)

Les responsabilités varient en fonction de la configuration du cluster et de la présence de fournisseurs de nœuds externes dans Kosmos.

> **Principe général**
> Scaleway garantit la sécurité et la fiabilité de la plateforme.Le client garantit la sécurité et la conformité de ses applicatifs et de ses configurations.

Qu'est-ce qu'un service Kubernetes managé ?

Chez Scaleway, un service Kubernetes managé désigne les produits Kapsule et Kosmos. Scaleway assure la gestion et la maintenance du plan de contrôle (control-plane) Kubernetes, ainsi que de tous les composants essentiels au bon fonctionnement du cluster Kubernetes.

Quels composants de Kubernetes sont gérés par Scaleway ?

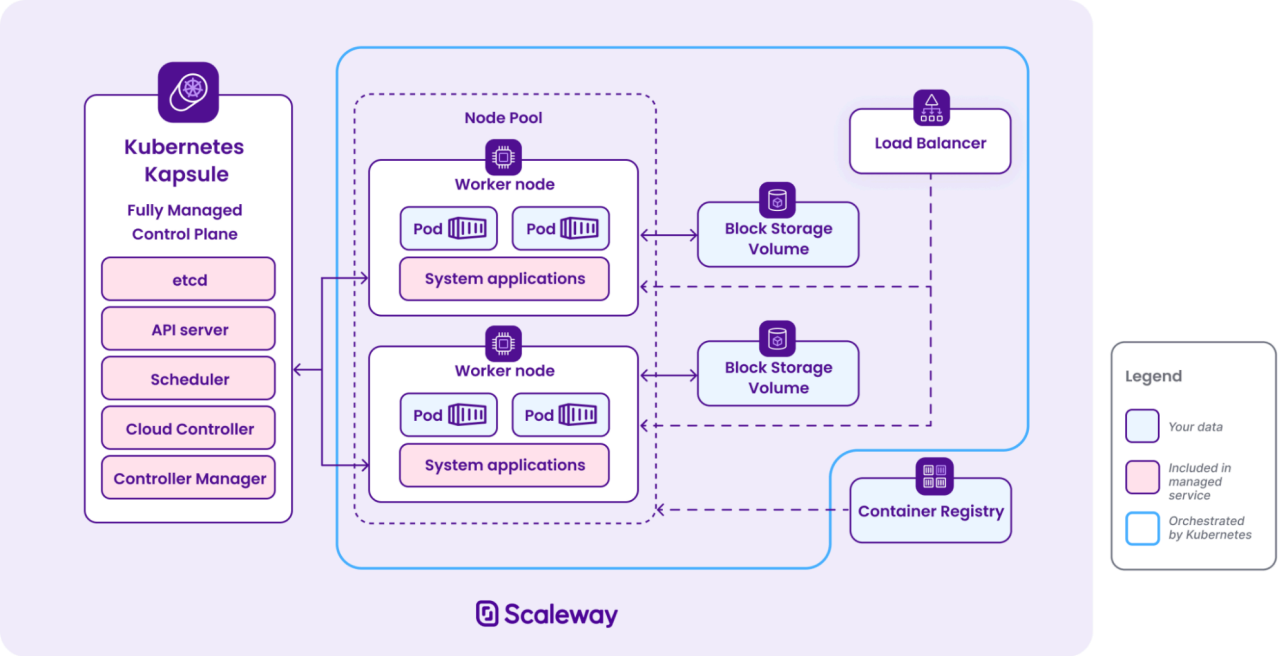
Scaleway gère le plan de contrôle Kubernetes (Kapsule ou Kosmos), composé de différents éléments assurant la gestion et la maintenance du cluster et de son état. Parmi ces éléments figurent notamment le plan de contrôle lui-même : *etcd*, l'*apiserver*, le *scheduler*, le *cloud controller manager*, et le *controller manager*.

Scaleway prend en charge les applications système Kubernetes telles que CoreDNS, kube-proxy, CNI (Container Networking Interface) et CSI (Container Storage Interface), indispensables au bon fonctionnement du cluster Kubernetes et de ses ressources associées.

Scaleway assure également le provisionnement des nœuds et la mise à jour des images système de ces nœuds.

Scaleway propose les dernières mises à jour mineures et correctifs, permettant ainsi à l'utilisateur de les installer régulièrement sur son cluster via notre API, notre interface de ligne de commande (CLI), la console web ou encore le fournisseur Terraform.

De plus, Scaleway fournit des informations et des rappels lorsque les anciennes versions ne sont plus prises en charge (EOL), garantissant ainsi que les utilisateurs restent informés et mettent à niveau leurs clusters régulièrement.



Composants et fonctionnalités gérés par Scaleway

Component	Responsibility
Control plane	etcd, API Server, Scheduler, Controller Manager, Cloud Controller Manager
Add-ons système (présents sur chaque nœud worker)	CoreDNS, kube-proxy, CNI, CSI
Image des nœuds	Publié, corrigé et maintenu par Scaleway pour les pools de nœuds gérés.

Component	Responsibility
Haute disponibilité du control-plane	Options de déploiement multi-AZ, basculement automatique
Intégration de l'infrastructure scw	VPC, Load Balancers, Block Storage, IAM APIs
Management des patches & versions	Notifications, planification de la fin de vie, prise en charge de la mise à niveau automatique des correctifs

Sécurité du cloud (responsabilité de Scaleway)

Opérations d'infrastructure et de plateforme

Scaleway est responsable de la mise à disposition et de la maintenance :

- **Sécurité physique des centres de données**, y compris les installations, le contrôle d'accès et la protection de l'environnement
- **Infrastructure du réseau**, y compris les réseaux physiques et virtuels sous-jacents : Stack de virtualisation, API sous-jacentes et plans de contrôle d'infrastructure utilisés pour le provisionnement des clusters
- **Plans de contrôle Kubernetes gérés**, y compris la haute disponibilité et la redondance des serveurs API et des données d'état du cluster
- **Fonctionnalités fournies par Scaleway et intégrées à la plateforme** (par exemple Load Balancers, VPC, IAM APIs)
- **Images de nœuds Kubernetes fournies par Scaleway** et automatisation du cycle de vie des pools de nœuds

Résilience et disponibilité du service

Scaleway est responsable de :

- Garantir que le control-plane Kubernetes géré atteigne les objectifs de disponibilité et de résilience définis dans la documentation produit.
- Proposer des options de plan de contrôle multi-AZ (zones de disponibilité) le cas échéant.
- Assurer la redondance de l'infrastructure sous-jacente.
- Publier des SLA documentés pour les plans de contrôle dédiés.

Intégration avec les autres services Scaleway

Scaleway assure l'intégration avec les VPC managés, IAM, les équilibreurs de charge, le stockage en mode bloc et d'autres services d'infrastructure utilisés par les clusters Kubernetes, y compris le provisionnement de ressources via les API Kubernetes.

Sécurité et mises à jour de la plateforme

Scaleway gère:

- Application de correctifs de sécurité aux composants d'infrastructure et aux composants du plan de contrôle géré
- Gestion continue des vulnérabilités pour les services sous le contrôle de Scaleway
- Paramètres par défaut sécurisés et pertinents pour les fonctionnalités et intégrations Scaleway
- Les clients sont avertis lorsque les versions approchent de leur fin de vie.

Sécurité dans le cloud (responsabilité de l'utilisateur)

Les utilisateurs sont responsables de tous les aspects de la configuration et des applicatifs du cluster Kubernetes, de façon non-exhaustive :

Configuration du cluster Kubernetes

Les utilisateurs sont responsables de :

- Configuration des ressources Kubernetes (Déploiements, Services, ConfigMaps, Secrets, CRD)
- RBAC (Contrôle d'accès basé sur les rôles) et permissions d'accès utilisateur
- Contrôles d'admission et gouvernance des espaces de noms (“namespaces”)
- Politiques de sécurité des pods (“PSP”) et configurations appliquées via l'API Kubernetes
- “Network Policies” au sein du cluster
- Configuration de “l'audit log” (pour les offres dédiées), de la conservation des journaux et de l'observabilité

Pools de nœuds, images et applicatifs

Lors de l'utilisation des pools de nœuds gérés par Scaleway :

- Les utilisateurs définissent la taille du pool de nœuds, les types d'instances et les politiques de mise à l'échelle.
- Ils choisissent le moment de déclencher les mises à niveau des nœuds ou les mises à jour progressives des images.
- Ils sont responsables de la compatibilité des charges de travail.

Pour les nœuds personnalisés ou externes (par exemple, dans un cluster Kosmos qui attache des ressources de calcul externes non-Scaleway) :

- Les utilisateurs sont responsables du provisionnement et du cycle de vie des nœuds.
- Ils doivent garantir la sécurité, les correctifs et le “hardening” du système d'exploitation.
- Ils doivent gérer la connectivité réseau, les règles de pare-feu et la configuration de d'initialisation (“bootstrap”) des nœuds.

Sécurité des réseaux et des VPC

L'utilisateur est responsable de :

- Conception de la segmentation VPC et des sous-réseaux
- Configuration des règles de pare-feu (ACL) et des groupes de sécurité
- Gestion de l'exposition publique des services sur internet
- Configuration des certificats TLS, des règles “d’ingress” et du DNS

Identité, gestion des accès et identifiants

L'utilisateur est responsable de :

- Politiques IAM au sein de leur compte/projet
- Authentification et autorisation d'accès au cluster
- Stockage sécurisé et rotation des identifiants, “tokens” et clés API Kubernetes
- Gestion des accès avec privilèges minimaux systématiques pour les utilisateurs et les applications

Sécurité des applicatifs et protection des données

L'utilisateur doit s'assurer que :

- Les images de conteneurs sont analysées, sécurisées et fiables.
- Chiffrement au niveau applicatif en transit et au repos lorsque nécessaire.
- Stratégies de sauvegarde et de restauration des données applicatives et des charges de travail avec état (“stateful workload”).
- La journalisation et l’observabilité sont configurées pour répondre aux exigences de conformité et d'audit.

Add-ons

Scaleway est responsable de :

- Provisionner des modules complémentaires gérés (par exemple, pilotes CSI, composants CNI par défaut, CoreDNS ou opérateur GPU NVIDIA).

L'utilisateur est responsable de :

- Configurer ces modules complémentaires en fonction de ses besoins spécifiques, le cas échéant.
- Surveiller et maintenir la compatibilité avec les charges de travail du cluster.
- Évaluer les modules complémentaires tiers ou les extensions personnalisées non fournies par Scaleway.

Important
Lorsque les utilisateurs modifient ou remplacent des composants préinstallés (par exemple, en modifiant les configurations kubelet, le réseau des nœuds), la responsabilité de ces composants est transférée au client.

Offre mutualisée et offre dédiée

Le plan de contrôle (“control-plane”) Kapsule varie selon qu'il s'agit d'un environnement partagé ou dédié, et selon les ressources dédiées spécifiques que vous choisissez.

Veuillez consulter cette documentation pour comprendre les différences entre les offres dédiées et mutualisées.

Options de Cluster: Kapsule vs Kosmos

Kapsule

Dans les clusters Kapsule, le control-plane et les pools de nœuds gérés sont exploités par Scaleway.
Les utilisateurs définissent la configuration des ressources du cluster
Des images Kubernetes gérées et l'automatisation des pools de nœuds sont fournies.

Kosmos

Kosmos étend Kubernetes géré pour prendre en charge plusieurs sources d'infrastructure :

Nœuds hébergés par Scaleway

- Comportement similaire aux nœuds Kapsule, Scaleway gère le provisionnement des nœuds et la publication des images, tandis que les utilisateurs gèrent les applicatifs et les configurations.
- Bien que Scaleway gère l'infrastructure hôte, l'hyperviseur et la sécurité physique, les clients restent responsables de la sécurité des charges de travail et des politiques au niveau du cluster, conformément à ce SRM Kapsule.

Note
Les nœuds Kosmos hébergés sur l'infrastructure Scaleway sont provisionnés et gérés à l'aide d'instances Scaleway. Par conséquent, les ressources de calcul sous-jacentes, la gestion du cycle de vie et la sécurité au niveau de l'hôte suivent ce modèle Scaleway Instances Shared Responsibility Model.

Nœuds externes

- Les nœuds hébergés en dehors de Scaleway relèvent de l'entière responsabilité de l'utilisateur en matière de mises à jour du système d'exploitation, de renforcement de la sécurité (“hardening”), de connectivité et de surveillance de l'état (“monitoring”).
- Scaleway continue de gérer le control-plane Kubernetes pour le cluster.

Cycle de vie des versions et fin du support

La politique de Scaleway concernant les versions de Kapsule exige que les clients :

- Suivre les notifications de dépréciation
- Effectuer les mises à niveau mineures et majeures de Kubernetes
- Activer la mise à niveau automatique pour les correctifs au sein des versions mineures prises en charge
- Remplacer les nœuds avant ou à la date limite de cycle de vie recommandée par la plateforme

Scaleway prend en charge chaque version mineure de Kubernetes pendant au moins **12 mois après sa sortie initiale**.

Note sur l’Auto-Upgrade
La fonction de mise à niveau automatique applique les correctifs uniquement au sein d'une même version mineure. Elle concerne à la fois le control-plane et les nœuds managés.
Pour éviter les échecs de mise à niveau, assurez-vous que le “namespace” kube-system reste vierge de modifications.

Étapes du cycle de vie des versions

Étape	Description	Action correspondante
Sortie	Version disponible pour les nouveaux clusters et les mises à niveau	Mise à jour optionnelle
Dépréciation	Version plus disponible pour les nouveaux clusters ; les clusters existants ont été informés par ticket d'assistance.	Mise à jour recommandée
Fin de support (EoS)	Mise à niveau automatique vers la prochaine version mineure prise en charge déclenchée dans les 30 jours.	Vérifier le bon fonctionnement des applicatifs après la mise à jour

Notifications:

- **Dépréciation**: Annoncé dans le Changelog
- **EoS**: Communication effectuée via un ticket d'assistance sur la console et un avis de maintenance planifiée

Scaleway peut effectuer une mise à niveau forcée pour les versions non prises en charge afin de garantir la continuité opérationnelle, mais les clients **doivent** valider les applicatifs après ces modifications.

Conformité d'utilisation

Les utilisateurs doivent s'assurer que leur utilisation des services Kubernetes est conforme aux conditions d'utilisation de Scaleway, aux lois applicables et aux exigences de conformité spécifiques à leur industrie (RGPD, HIPAA, SOC2, etc.).

Protection et chiffrement des données

L'utilisateur est responsable de :

- Garantir le chiffrement des données sensibles au repos ("at rest") et en transit au sein des applicatifs.
- Gérer les clés et les certificats nécessaires à la conformité.
- Mettre en œuvre des politiques de sauvegarde et de conservation conformes aux obligations réglementaires.

Scaleway fournit l'infrastructure nécessaire à la prise en charge de ces fonctionnalités, mais ne gère pas le contenu des données utilisateur ni le chiffrement des applicatifs.

Suppression des données et cycle de vie des ressources

Les utilisateurs doivent explicitement supprimer ou gérer les ressources (clusters, pools de nœuds, volumes, composants réseau, identifiants). Ils peuvent utiliser l'API Kapsule pour supprimer de manière synchrone les ressources Scaleway associées à un cluster existant.

Scaleway supprimera les composants d'infrastructure lors de la résiliation, mais n'est pas responsable de la conservation ou de la restauration des applicatifs ou des données des utilisateurs.

Intervention et résolution des incidents

Scaleway est responsable de :

- Rétablissement du control-plane à son état fonctionnel après des incidents d'infrastructure imprévus
- Mise à disposition de données d'observabilité et de recommandations suite à des défaillances au niveau de la plateforme

L'utilisateur est responsable de :

- Diagnostic des pannes au niveau des applicatifs
- Correction des ressources mal configurées
- Restauration de l'état de l'application et des flux de travail afférents

> **Note**
> Scaleway peut réinitialiser un cluster à son état d'usine par défaut, mais ne garantit pas le rétablissement des charges de travail mal configurées ou incompatibles.

Dispositions spécifiques pour l'hébergement de données de santé (HDS) avec l'offre dédiée Kapsule

Cette section décrit les exigences et les responsabilités spécifiques liées à l'hébergement des données de santé (ou au transit de ces données) conformément au cadre réglementaire HDS.

Lors du traitement des données de santé avec le produit Scaleway Kapsule, les utilisateurs doivent :

- signer le contrat Scaleway HDS
- créer des clusters Kapsule dédiés au traitement des données conformes à la norme HDS
- garantir l'accès restreint à ces clusters selon le principe du moindre privilège
- suivre les règles générales de conformité de Scaleway relatives à la norme HDS

Scaleway s'engage à fournir une infrastructure certifiée HDS et à maintenir cette certification.

Sauvegarde

Il incombe aux utilisateurs de sauvegarder leurs données à l'aide de solutions de stockage appropriées, telles que le stockage en mode bloc HDS. Scaleway doit sauvegarder la configuration du plan de contrôle Kapsule et être en mesure de restaurer l'état du cluster après un dysfonctionnement éventuel.

Résidence des données

Pour que Scaleway puisse garantir que le traitement des données reste confiné à des centres de données autorisés à Paris, les utilisateurs **doivent** :

- Créer des clusters Kapsule uniquement dans la région autorisée de Paris (fr-par).
- Créez les ressources de stockage et réseau associées dans la région de Paris.
- **Ne pas router le trafic du cluster en dehors de la région fr-par.**

Identification des ressources conformes à la norme HDS

L'utilisateur est responsable de :

- Identifier les ressources (Load Balancers, Instances, Block Volumes) compatibles HDS.
- Attacher uniquement ces ressources au cluster Kapsule compatible HDS.

Chiffrement des données

Les données de santé doivent être chiffrées lors de leur transit.

L'utilisateur est responsable de :

- Mise en œuvre du protocole HTTPS pour le trafic entrant et sortant du cluster, c'est-à-dire configuration des "load balancers" et des "gateways" en conséquence.
- Gestion de la génération et du renouvellement des certificats TLS
- Gestion du provisionnement et du chiffrement des volumes en mode bloc avec le composant Kapsule CSI et gestion des clés de chiffrement.

Scaleway est responsable de :

- Mise à disposition d'un réseau privé L2 sécurisé pour le routage du trafic des nœuds du cluster et du "control-plane".
- Mise à disposition d'API de stockage conformes pour le stockage au repos ("at rest") des données d'état avec Kapsule CSI.
- Gestion et renouvellement de la clé utilisée pour chiffrer la configuration du cluster dans la base de données etcd.

Journaux et traçabilité

L'utilisateur est responsable de :

- Configuration et maintenance des solutions de surveillance et de traçabilité pour ses applicatifs, éventuellement via Scaleway Cockpit.
- Activation et configuration de la solution d'audit des journaux ("Audit Trail").

Scaleway est responsable de :

- Mise à disposition d'interfaces de métriques et de journalisation pour la surveillance des composants du "control-plane" (y compris les fonctionnalités d'"Audit Trail").

Réversibilité

Comme Scaleway Kapsule n'est pas une distribution Kubernetes spécifique et que la plupart de ses composants sont open source, l'utilisateur peut simplement exporter toutes ses ressources YAML

Kubernetes vers un autre fournisseur de services Kubernetes managés. Les seuls changements à prendre en compte seront l'utilisation des nouvelles API du fournisseur (IAM, stockage en mode bloc, VPC, etc.). Voici un exemple simple :

Étape 1 : Évaluer et documenter les ressources actuelles du cluster

Commencez par documenter la configuration de votre cluster existant. Cela inclut les espaces de noms, les déploiements, les services, le stockage et toutes les ressources ou politiques personnalisées utilisées.

- Inventaire des ressources
    - Namespaces
    - Deployments and StatefulSets
    - Services: Document LoadBalancers, NodePorts, ClusterIPs.
    - ConfigMaps and Secrets
    - Ingress Controllers
    - Persistent Volumes and Claims
    - Custom Resource Definitions (CRDs) and associated operators.
    - Network Policies
- Export des manifestes. Utilisez kubectl pour exporter les manifestes de vos ressources :

```
kubectl get all --all-namespaces -o yaml > cluster-resources.yaml
kubectl get pvc --all-namespaces -o yaml > pvcs.yaml
kubectl get configmaps --all-namespaces -o yaml > configmaps.yaml
kubectl get secrets --all-namespaces -o yaml > secrets.yaml
kubectl get crd --all-namespaces -o yaml > crds.yaml
```

Étape 2 : Migrez les images de conteneurs vers votre nouveau registre de conteneurs

Votre nouveau cluster aura besoin d'accéder à vos images de conteneurs.

Étape 3 : Créez un cluster Kubernetes

Créez et configurez un nouveau cluster Kubernetes

Étape 4 : Configurez kubectl sur votre nouveau cluster Kubernetes

Étape 5 : Adaptez les manifestes et les configurations Kubernetes

Vos fichiers manifestes existants peuvent contenir des paramètres spécifiques au fournisseur de cloud qui doivent être ajustés pour correspondre à la configuration du nouveau fournisseur.

Étape 6 : Migration des données persistantes et du stockage

1. Sauvegardez les données de votre cluster existant : utilisez les outils appropriés pour sauvegarder les données des volumes persistants. Voici quelques méthodes :
    a. Exportation des données de bases de données

b. Copie du système de fichiers : pour le stockage de fichiers, copiez les données vers un emplacement temporaire.

2. Restaurez les données sur le cluster nouvellement créé.
    a. Créez des PersistentVolumeClaims dans votre nouveau cluster Kubernetes
    b. Restaurez les données dans les nouveaux volumes :
        i. Init containers: Utilisez les pour renseigner les données..
        ii. Data import jobs: Utilisez des jobs Kubernetes pour importer des données.

Étape 7 : Déployez les applications sur votre nouveau cluster

Étape 8 : Mise à jour des configurations réseau et DNS

Étape 9 : Testez et validez les déploiements

Effectuer des tests fonctionnels, de performance et de bout en bout pour vérifier que les applicatifs fonctionnent comme prévu dans le nouvel environnement.

> **Important**
> Cette documentation doit être lue conjointement avec l'accord HDS de Scaleway et les certifications applicables. Pour toute question, veuillez contacter le support HDS.