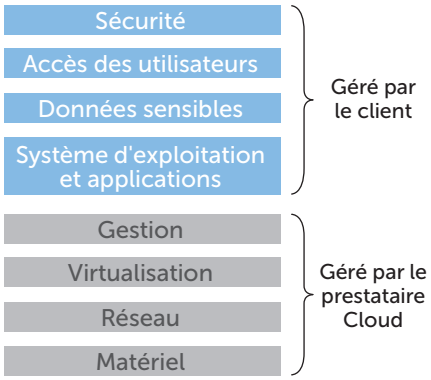
Kaspersky®
Cloud Security

Protégez votre Cloud Amazon grâce à la solution de sécurité dans le Cloud de Kaspersky Lab

Pourquoi choisir Kaspersky Lab pour la protection d'un Cloud hybride :

- **Solution de sécurité la plus souvent primée**, optimisée pour votre Cloud hybride.
- **Préservation de l'efficacité des systèmes**, aperçu et administration complets de la sécurité dans vos Clouds.
- **Amélioration des fonctions**, dont les contrôles des applications, d'Internet et des appareils, et protection contre les cybermenaces avancées et les attaques de ransomwares.
- **Intégration** à votre infrastructure d'entreprise.
- **Économie des ressources** et réduction sensible des coûts d'exploitation dans votre environnement Cloud hybride.

Responsabilités partagées en matière de sécurité dans les environnements Cloud publics



Organiser la sécurité de votre environnement Cloud hybride avec Amazon et Kaspersky Lab

L'adoption du concept de Cloud hybride dans la gestion et le stockage de données, où les charges de travail passent sans contraintes de votre propre environnement virtuel à un ou plusieurs environnements Cloud publics, donne naissance à de nouveaux problèmes au niveau de la sécurité. Que vous traitiez vos données sur site ou hors site, votre objectif global demeure inchangé : garantir de manière efficace la sécurité de votre entreprise, de ses actifs numériques, de ses opérations et de vos salariés.

La transition d'un Cloud privé à un Cloud hybride s'accompagne de la mise en place d'un nouveau modèle de responsabilité. Votre prestataire de services s'occupe de la sécurité du Cloud public (infrastructure, matériel, réseau et couches de virtualisation) tandis que vous assumez la responsabilité pour tout ce que vous hébergez dans le Cloud (charges de travail sécurisées, systèmes d'exploitation, données et applications). Bien entendu, il vous incombe également de garantir la cybersécurité des salariés et de confirmer que la solution de sécurité que vous avez adoptée répond à vos besoins en la matière.

Amazon Web Services (AWS) propose un Cloud public fiable, évolutif et rentable pour les charges de travail de votre activité. Les machines virtuelles et les charges de travail associées protégées par Kaspersky Cloud Security, qu'elles tournent dans l'environnement public AWS ou dans l'infrastructure privée de votre Cloud hybride, doivent non seulement être soumises à des niveaux de sécurité et des stratégies identiques, mais aussi pouvoir être consultées et gérées via une console « d'orchestration » unique.

Ce document illustre la simplicité avec laquelle vous pouvez étendre Kaspersky Cloud Security à vos ressources Cloud AWS afin de profiter de capacités de sécurité avancées, d'une visibilité complète des machines virtuelles et d'une orchestration unifiée sur l'ensemble de votre Cloud hybride.

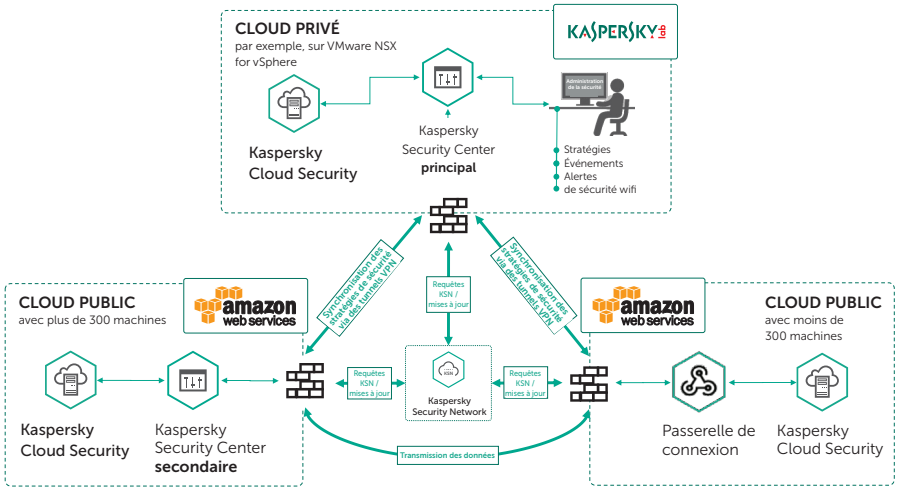


Illustration 1. Cloud hybride avec Amazon Web Services et Kaspersky Cloud Security

Nous formulerons une recommandation générale pour une bonne pratique : la communication entre les Clouds s'opère via l'Internet public. Par conséquent, nous vous conseillons vivement d'établir des **canaux de chiffrement sécurisés** (tunnels VPN) entre votre Cloud privé et le Cloud public afin de garantir les niveaux les plus élevés de protection et de confidentialité ; Amazon Virtual Private Cloud Network et Amazon Virtual Private Gateway sont deux options qui s'offrent à vous en la matière.

Si vous n'utilisez pas encore la version 10 de Kaspersky Security Center, il est vivement conseillé de réaliser la mise à niveau à cette version, car il se peut que les versions antérieures ne disposent pas de toutes les fonctions requises pour prendre en charge cette mise en œuvre.

Vous devez également veiller à ce que la configuration de votre **infrastructure réseau** soit adéquate pour gérer le trafic entre les différents composants de l'infrastructure comme illustré dans le schéma ci-dessus. Pour en savoir plus sur la configuration des ports réseau et des règles de pare-feu, consultez le Manuel de mise en œuvre de Kaspersky Security Center.

En fonction de la taille de votre environnement Cloud AWS, vous avez le choix entre deux méthodes de mise en œuvre de la solution Kaspersky Cloud Security. Toutes deux sont assez directes.

Sécurité du Cloud hybride : Cloud AWS + Cloud privé

Moins de 300 machines virtuelles dans le Cloud AWS

Pour appliquer Kaspersky Cloud Security à un Cloud hybride qui affiche ce niveau d'activité de Cloud public, il suffit de déployer une passerelle de connexion. Vous connectez ainsi les machines virtuelles protégées de votre Cloud public directement à votre Kaspersky Security Center principal dans le Cloud privé, si bien que toutes les machines virtuelles reçoivent les stratégies de sécurité, les mises à jour et les informations relatives à la licence.

En cas d'utilisation d'une **passerelle de connexion**, les machines virtuelles protégées de votre Cloud public AWS se connectent directement au serveur Kaspersky Security Center principal pour obtenir les stratégies de sécurité, les mises à jour et les informations relatives à la licence. Le cas échéant, il est également possible de télécharger les mises à jour de lutte contre les programmes malveillants, les statistiques d'analyse et les verdicts depuis le service international Kaspersky Security Network (KSN) basé dans le Cloud.

Il suffit d'installer un Agent d'administration Kaspersky Lab sur une machine virtuelle dans votre Cloud AWS en indiquant l'adresse IP du Kaspersky Security Center principal dans le Cloud privé. Cette machine virtuelle devient alors la « passerelle de connexion » qui va permettre au reste des machines virtuelles de votre Cloud AWS, identifiées lors de la définition de la topologie, de se connecter au Kaspersky Security Center principal.

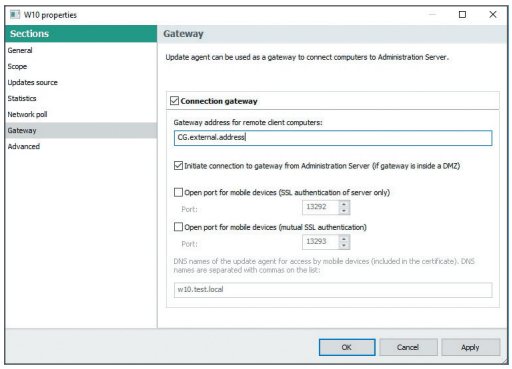


Illustration 2. Paramètres de configuration de la passerelle de connexion

300 machines virtuelles ou plus dans le Cloud AWS

En cas d'utilisation d'un Kaspersky Security Center secondaire, ce serveur se charge de la diffusion centralisée de l'ensemble des stratégies de sécurité, des mises à jour et des informations relatives à la licence sur les machines virtuelles protégées au sein de votre Cloud public AWS, après avoir reçu l'ensemble de ces données du serveur principal. Cela permet de réduire considérablement le trafic réseau entre les Clouds dans les exploitations de grande taille.

Si votre Cloud public compte au moins 300 machines virtuelles, il est préférable de déployer un Kaspersky Security Center secondaire au lieu d'une passerelle de connexion, ce qui garantit une redondance suffisante pour permettre le fonctionnement sécurisé de chaque machine virtuelle en permanence. Déployez le nouveau Kaspersky Security Center secondaire sur une machine virtuelle dans le Cloud AWS à l'aide de l'assistant de déploiement traditionnel.

Il est alors possible d'administrer la sécurité des machines virtuelles dans les deux Clouds soit via le Kaspersky Security Center secondaire, soit via la passerelle de connexion, tandis que l'ensemble de l'orchestration s'opère via le Kaspersky Security Center principal au sein du Cloud privé.

Si vous utilisez plus d'un Cloud public en plus de votre Cloud privé, il convient d'installer une passerelle de connexion distincte, ou le cas échéant un Kaspersky Security Center secondaire, sur une machine virtuelle de chacun des Clouds publics.

C'est aussi simple que cela. Dans les deux cas, vous êtes désormais prêt à administrer les machines virtuelles dans le Cloud privé et dans le Cloud public. Il ne vous reste plus alors qu'à déployer des agents de Kaspersky Cloud Security sur les machines virtuelles à protéger afin que vous puissiez profiter des capacités de sécurité et des contrôles avancés et les gérer via la console d'orchestration unifiée Kaspersky Security Center sur l'ensemble de votre Cloud hybride.

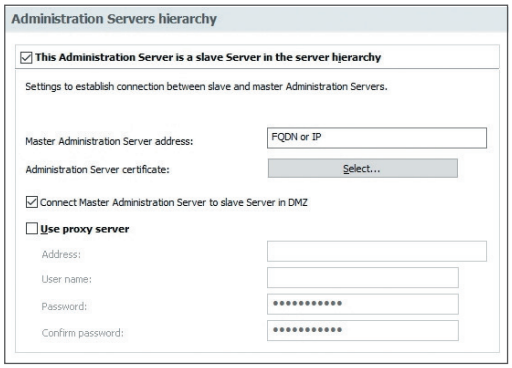


Illustration 3. Paramètres de configuration de KSC en rôle secondaire

Ainsi :

- Vous pouvez organiser de façon centralisée la configuration ou la diffusion de stratégies de sécurité depuis votre Cloud privé vers votre Cloud public, surveiller la sécurité et obtenir des rapports sur l'ensemble des machines virtuelles.
- Vos actifs virtuels dans le Cloud public AWS bénéficient du même niveau de sécurité que ceux qui se trouvent dans votre environnement Cloud privé et l'infrastructure Cloud hybride continue à fonctionner de la manière la plus efficace possible, sans impact sur les performances du système.
- À l'instar de celle de votre Cloud privé, l'orchestration de l'ensemble de votre Cloud hybride s'opère via un seul écran.

Sécurité du Cloud hybride : plusieurs Clouds publics uniquement

Une solution de Cloud hybride peut réunir plusieurs Clouds publics sans aucun Cloud privé, ce qui isole l'infrastructure publique du reste des technologies de l'information. Les machines virtuelles sont déployées dans AWS ainsi que dans un ou plusieurs autres Clouds publics, par exemple Microsoft Azure ou Managed Hybrid Cloud Hosting.

Ici aussi, **Kaspersky Cloud Security** permet d'offrir des capacités de protection harmonisées ainsi qu'une administration et une visibilité au niveau de l'entreprise, ce qui garantit la sécurité intégrale de toute machine virtuelle, quel que soit l'emplacement du Cloud public.

Dans la mesure où il n'existe pas déjà un Kaspersky Security Center principal dans un Cloud privé, ce mode de déploiement prévoit une étape supplémentaire. Il faudra installer le Kaspersky Security Center principal sur une machine virtuelle dans un Cloud public.

Puis, à l'instar de la procédure décrite pour les Clouds hybrides « public plus privé », il faut installer une passerelle de connexion ou un Kaspersky Security Center secondaire, si le Cloud contient plus de 300 machines virtuelles, dans chacun des autres Clouds publics utilisés. Ainsi, Kaspersky Cloud Security est à nouveau installé sur chacune des machines virtuelles à protéger, dans chaque emplacement.

Vous pouvez désormais administrer toutes vos machines virtuelles dans tous les Clouds publics, soit via un Kaspersky Security Center secondaire, soit via une passerelle de connexion, tandis que toutes les tâches essentielles d'orchestration de la sécurité sont réalisées via le seul écran de votre Kaspersky Security Center principal.

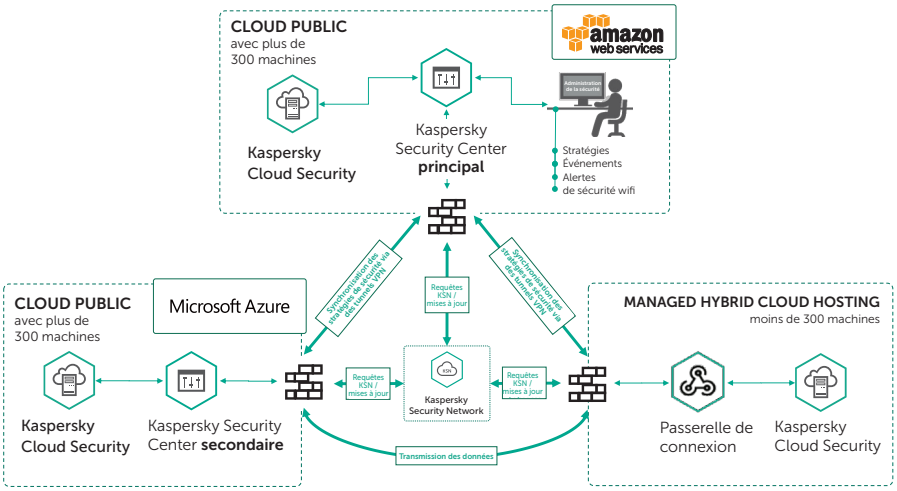
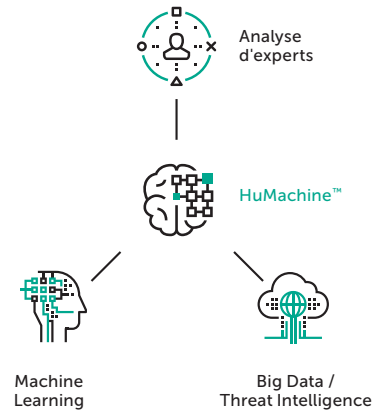


Illustration 4. Cloud hybride sur plusieurs Clouds publics uniquement

Synthèse de la sécurité du Cloud hybride

La solution Kaspersky Cloud Security a été spécialement conçue pour profiter des avantages technologiques offerts par les Clouds hybrides via un suivi dynamique des modifications de l'infrastructure et l'offre d'une sécurité robuste qui met l'accent sur la vitesse optimale et l'efficacité des ressources. Grâce à nos capacités exceptionnelles en matière de protection, associées à la gestion unifiée de la sécurité de tous les terminaux physiques et virtuels, peu importe où ils se trouvent, vous pouvez déployer vos projets de Cloud hybride à votre propre rythme, en douceur, en sécurité et en relâchant la pression sur vos ressources informatiques.

Pour en savoir plus sur Kaspersky Cloud Security, consultez
https://www.kaspersky.fr/enterprise-security/cloud-security



Kaspersky Lab
pour les entreprises : **https://www.kaspersky.fr/enterprise-security**
Actualités des cybermenaces : **www.viruslist.fr**
Actualités de la sécurité informatique : **business.kaspersky.com**

#truecybersecurity
#HuMachine

www.kaspersky.fr