Bitdefender

GravityZone

GUIDE D'INSTALLATION

Bitdefender GravityZone
Guide d'installation

Date de publication 2021.04.20

Mentions légales

Mentions légales

Tous droits réservés. Aucune partie de ce manuel ne peut être reproduite ou transmise, sous aucune forme et d'aucune façon, électronique ou physique, y compris photocopies, enregistrement, ou par quelque moyen de sauvegarde ou de restauration que ce soit, sans une autorisation écrite d'un représentant officiel de Bitdefender. Il est permis d'inclure de courtes citations dans la rédaction de textes sur le produit, à condition d'en mentionner la source. Le contenu ne peut en aucun cas être modifié.

Table des matières

Préface

Ce guide s'adresse aux administrateurs informatique en charge du déploiement de la protection GravityZone sur les sites de leur organisation. Les responsables informatiques en quête d'informations sur GravityZone trouveront dans ce guide les conditions préalables à l'installation de GravityZone ainsi que les modules de protection disponibles.

Ce document vise à expliquer comment installer et configurer la solution GravityZone et ses agents de sécurité sur tous les types d'endpoints de votre entreprise

1. Conventions utilisées dans ce guide

Normes Typographiques

Ce guide utilise différents styles de texte pour une meilleure lisibilité. Le tableau ci-dessous vous informe au sujet de leur aspect et de leur signification.

Apparence	Description
`échantillon`	Le nom et les syntaxes des lignes de commandes, les chemins et les noms de fichiers, la configuration, la sortie de fichier et les textes d'entrée sont affichés en police `monospace`.
http://www.bitdefender.com	Les liens URL pointent vers un emplacement externe comme un serveur http ou ftp.
gravityzone-docs@bitdefender.com	Les adresses e-mail sont insérées dans le texte pour plus d'informations sur les contacts.
« Préface » (p. vii)	Ceci représente un lien interne vers un emplacement à l'intérieur de ce document.
option	Toutes les options du produit sont imprimées à l'aide de caractères **gras**.
mot clé	Les options de l'interface, les mots-clés et les raccourcis sont mis en évidence à l'aide de caractères **gras**.

Avertissements

Les avertissements sont des notes textes graphiquement marquées, offrant à votre attention des informations additionnelles relatives au paragraphe actuel.

Note
La note consiste simplement en une courte observation. Bien que vous puissiez les ignorer, les notes apportent des informations non négligeables, comme des fonctions spécifiques ou un lien vers un thème proche.

Important
Cette icône requiert votre attention et il n'est pas recommandé de la passer. Elle fournit généralement des informations non essentielles mais importantes.

Avertissement
Marque une information critique que vous devrez lire attentivement. Rien de négatif ne se passera si vous suivez les indications. A lire très attentivement car décrit une opération potentiellement très risquée.

1. À PROPOS DE GRAVITYZONE

GravityZone est une solution de sécurité pour entreprises conçue nativement pour la virtualisation et le cloud afin de fournir des services de sécurité aux endpoints physiques, appareils mobiles, machines virtuelles dans les clouds privés et publics et les serveurs de messagerie Exchange.

GravityZone fournit une console d'administration unifiée disponible dans le cloud (hébergée par Bitdefender)ou en tant qu'appliance virtuelle à installer sur le site de l'entreprise.La solution permet de déployer,d'appliquer et de gérer des politiques de sécurité pour un nombre illimité d'endpoints,de tout type, quel que soit l'endroit où ils se trouvent,à partir d'un point unique d'administration.

GravityZone fournit plusieurs niveaux de sécurité aux endpoints y compris aux serveurs de messagerie Microsoft Exchange : antimalware avec analyse comportementale, protection contre les menaces de type « zero day », liste noire des applications et sandboxing, pare-feu, contrôle des appareils et du contenu, antiphishing et antispam.

2. COUCHES DE PROTECTION DE GRAVITYZONE

GravityZone fournit les couches de protection suivantes :

- Antimalware
- Advanced Threat Control
- Anti-exploit avancé
- Pare-feu
- Contrôle de contenu
- Gestion des correctifs
- Contrôle des appareils
- Chiffrement complet du disque
- Security for Exchange
- Network Traffic Security Analytics (NTSA)
- Security for Storage
- Security for Mobile

2.1. Antimalware

La couche de protection antimalware est basée sur l'analyse des signatures et l'analyse heuristique (B-HAVE, ATC) afin de détecter les virus, vers, chevaux de Troie, spywares, adwares, keyloggers, rootkits et autres types de logiciels malveillants.

La technologie d'analyse antimalware de Bitdefender s'appuie sur les technologies suivantes :

- Une méthode d'analyse traditionnelle est d'abord utilisée, le contenu analysé est comparé à une base de données de signatures. La base de données de signatures contient des morceaux de code spécifiques à certaines menaces et est régulièrement mise à jour par Bitdefender. Cette méthode d'analyse est efficace contre les menaces ayant fait l'objet de recherches et documentées. Cependant, quelle que la soit la vitesse à laquelle la base de données de signatures est mise à jour, il existe toujours une fenêtre de vulnérabilité entre le moment où une nouvelle menace est découverte et la publication de son correctif.
- **B-HAVE**, le moteur heuristique de Bitdefender fournit un second niveau de protection contre les nouvelles menaces, inconnues. Des algorithmes heuristiques détectent les malwares en fonction de caractéristiques comportementales. B-HAVE exécute les fichiers suspects dans un

environnement virtuel afin de tester leur impact sur le système et de vérifier qu'ils ne constituent aucune menace. Si une menace est détectée, l'exécution du malware est bloquée.

Moteurs d'analyse

Bitdefender GravityZone est capable de définir automatiquement les moteurs d'analyse en fonction de la configuration de l'endpoint lors de la création des packages d'agent de sécurité.

L'administrateur peut également personnaliser les moteurs d'analyse en choisissant parmi plusieurs technologies d'analyse :

1. L'**analyse locale**, lorsque l'analyse est effectuée sur l'endpoint local. Le mode d'analyse locale est adapté aux machines puissantes, puisque tous les contenus de sécurité sont stockés en local.
2. **Analyse hybride avec Moteurs Légers (Cloud Public)**, avec une empreinte moyenne, utilisant l'analyse dans le cloud et en partie les contenus de sécurité locaux. Ce mode d'analyse présente l'avantage d'une meilleure consommation des ressources, tout en impliquant l'analyse hors site.
3. **Analyse centralisée dans un Cloud public ou privé**, avec une petite empreinte nécessitant Security Server pour l'analyse. Dans ce cas, aucun jeu de contenus de sécurité n'est stocké en local et l'analyse est transférée vers le Security Server.

   Note
   Il y a un nombre minimum de moteurs stockés localement, nécessaires pour décompresser les fichiers.

4. **Analyse centralisée (Cloud public ou privé avec Security Server), avec une analyse locale de secours* (moteurs complets)**
5. **Analyse centralisée (Cloud public ou privé avec Security Server), avec une analyse hybride de secours* (Cloud public avec des moteurs légers)**

* Lorsqu'on utilise une analyse à double moteur, si le premier moteur n'est pas disponible, le moteur de secours est utilisé. La consommation des ressources et l'utilisation du réseau dépendent des moteurs utilisés.

2.2. Advanced Threat Control

Pour les menaces échappant même au moteur heuristique, un autre niveau de protection est présent sous la forme d'Advanced Threat Control (ATC).

Advanced Threat Control surveille en permanence les processus en cours d'exécution et évalue les comportements suspects tels que les tentatives visant à : dissimuler le type de processus, exécuter du code dans l'espace d'un autre processus (détourner la mémoire d'un processus pour obtenir des privilèges plus élevés), se répliquer, déposer des fichiers, éviter que des processus ne soient listés par des applications énumérant des processus etc. Chaque comportement suspect fait augmenter le score du processus. À partir d'un certain seuil, une alarme est déclenchée.

2.3. Anti-exploit avancé

Basée sur le machine learning, cet anti-exploit avancé est une technologie proactive qui bloque les attaques de type zero-day menée par le biais d'exploits évasifs. L'Anti-exploit avancé détecte les exploits les plus récents en temps réel et atténue les vulnérabilités de corruption de mémoire pouvant échapper aux autres solutions de sécurité. Il protège les applications les plus utilisées, telles que les navigateurs, Microsoft Office ou Adobe Reader, ou toutes les applications auxquelles vous pourriez penser. Il surveille les processus du système et le protège contre les failles de sécurité et le détournement de processus existants.

2.4. Pare-feu

Le pare-feu contrôle l'accès des applications au réseau et à Internet. L'accès est automatiquement autorisé pour une base de données complète d'applications connues, légitimes. Le pare-feu peut également protéger le système contre le balayage de port, limiter le partage de connexion Internet et prévenir lorsque de nouveaux nœuds rejoignent une connexion Wifi.

2.5. Contrôle de contenu

Le module Contrôle de Contenu aide à appliquer les politiques de l'entreprise liées au trafic autorisé, à l'accès à Internet, à la protection des données et au contrôle des applications. Les administrateurs peuvent définir des options d'analyse du trafic et des exclusions, planifier l'accès à Internet tout en bloquant ou autorisant

certaines catégories web ou URL, configurer des règles de protection des données et définir des permissions pour l'utilisation d'applications spécifiques.

2.6. Network Attack Defense

Le module Network Attack Defense s'appuie sur une technologie de Bitdefender qui se concentre sur la détection des attaques réseau conçues pour accéder aux endpoints via des techniques spécifiques comme la force brute, les exploits réseau, les passwords stealers, les vecteurs d'infection drive-by-download, les bots et les chevaux de Troie.

2.7. Gestion des correctifs

Complètement intégré à GravityZone, Patch Management veille à ce que les applications logicielles et les systèmes d'exploitation soient à jour et donne une visibilité complète sur l'état des patchs sur les endpoints Windows administrés.

Le module GravityZone Patch Management comprend de nombreuses fonctionnalités, telles que l'analyse des patchs à la demande/planifiée, le patching automatique/manuel, ou l'édition de rapports sur les patchs manquants.

Pour en apprendre plus sur les prestataires et produits pris en charge par GravityZone Patch Management, consultez cet article de la base de connaissances.

Note
Patch Management est une extension disponible avec une clé de licence séparée pour tous les packs GravityZone.

2.8. Contrôle des appareils

Le module Contrôle des appareils permet d'éviter la fuite de données confidentielles et les infections de malwares par des appareils externes connectés aux endpoints. Cela passe par l'application de règles de blocage et d'exceptions, via une politique, à un large éventail de types d'appareils (tels que les clés USB, les appareils Bluetooth, les lecteurs de CD/DVD, les supports de stockage etc.)

2.9. Chiffrement complet du disque

Cette couche de protection vous permet d'appliquer le chiffrement de disque entier sur les endpoints en gérant BitLocker sur Windows, ou FileVault et diskutil sur macOS. Vous pouvez chiffrer et déchiffrer des volumes d'amorçage et de non-amorçage en quelques clics, tandis que GravityZone gère l'ensemble du

processus, avec une intervention minime des utilisateurs. En prime, GravityZone stocke les clés de récupération nécessaires pour débloquer les volumes, lorsque les utilisateurs oublient leurs mots de passe.

Note
Full Disk Encryption est une extension disponible avec une clé de licence séparée pour tous les packs GravityZone.

2.10. Security for Exchange

Bitdefender Security for Exchange offre une protection antimalware, anstispam, antiphishing et un filtrage des pièces jointes et du contenu parfaitement intégrés à Microsoft Exchange Server, afin de garantir un environnement de messagerie et de collaboration sûr et d'augmenter la productivité. À l'aide de technologies antimalware et antispam primées, elle protège les utilisateurs Exchange contre les malwares les plus récents et élaborés ainsi que contre les tentatives de vol de données confidentielles et de valeur d'utilisateurs.

Important
Security for Exchange a été conçu pour protéger l'intégralité de l'organisation Exchange à laquelle le serveur Exchange appartient. Cela signifie qu'il protège l'intégralité des messageries actives, y compris les messageries partagées et celles rattachées à un utilisateur/un bureau/un équipement.
En plus de la protection Microsoft Exchange, la licence couvre également les modules de protection endpoint installés sur le serveur.
La capacité de licences d' Security for Exchange est égale à 150% du nombre total de sièges de licence pour Security for Endpoints. Si le nombre de boites e-mail actives de votre organisation dépasse le nombre de boites protégées par la licence, une notification vous invitera à étendre votre licence.

2.11. Sandbox Analyzer

Offrant une puissante couche de protection contre les menaces avancées, le Sandbox Analyzer for Endpoints de Bitdefender effectue des analyses automatiques détaillées des fichiers suspects, qui n'ont pas encore été signalés par les moteurs antimalware de Bitdefender. Le sandbox utilise un large éventail de technologies Bitdefender afin d'exécuter des charges dans un environnement virtuel confiné déployé en local, d'analyser leur comportement et de signaler toute modification observée au sein du système, révélatrice d'une intention malveillante.

Sandbox Analyzer utilise un ensemble de capteurs pour détoner des contenus depuis les flux du trafic réseau, une quarantaine centralisée ou des serveurs ICAP.

En outre, Sandbox Analyzer permet d'envoyer des échantillons manuellement ou via une API.

Note
Le fonctionnement de ce module repose sur Sandbox Analyzer On-Premises, qui nécessite une clé de licence séparée.

2.12. Network Traffic Security Analytics (NTSA)

Bitdefender Network Traffic Security Analytics (NTSA) est une solution de sécurité du réseau qui analyse les flux IPFIX, en quête de comportements malveillants et de malwares.

Bitdefender NTSA a été conçu pour fonctionner en parallèle à vos mesures de sécurité existantes en tant que sureté supplémentaire capable de couvrir les angles morts des outils traditionnels.

Les outils de protection du réseau traditionnels essayent généralement de prévenir les infections de malwares en inspectant le trafic entrant (via une sandbox, un pare-feu, un antivirus, etc.). Bitdefender NTSA se concentre uniquement sur la surveillance des comportements malveillants du trafic sortant.

2.13. Security for Storage

GravityZone Security for Storage garantit une protection en temps réel de pointe pour les systèmes de partage de fichiers et de stockage en réseau les plus courants. Le système et les algorithmes de détection des menaces sont mis à jour automatiquement. Cela ne vous demande aucun effort et ne perturbe pas le travail des utilisateurs finaux.

Au moins deux Security Server GravityZone multiplateforme jouent le rôle de serveur ICAP qui effectue un service de lutte contre les malwares pour les appareils de stockage en réseau (NAS) et les systèmes de partage de fichiers conformes au Internet Content Adaptation Protocol (ICAP, standardisé par la norme RFC 3507).

Lorsqu'un utilisateur demande à ouvrir, lire, modifier ou fermer un fichier sur un ordinateur portable, un poste de travail, un smartphone ou un autre appareil ; le client ICAP (un NAS ou un système de partage de fichiers) envoie une demande d'analyse au Security Server et reçoit les conclusions de ce dernier au sujet du

fichier concerné. En fonction du résultat, Security Server autorise ou interdit l'accès au fichier. Il peut également le supprimer.

Note
Ce module est un complément disponible avec une clé de licence distincte.

2.14. Security for Mobile

Elle unifie la sécurité au sein de l'entreprise avec l'administration et le contrôle de la conformité des appareils iPhone, iPad et Android en assurant une distribution fiable des logiciels et des mises à jour via les marketplaces Apple et Android. Cette solution a été conçue pour permettre l'adoption contrôlée des initiatives de « Bring your own device » (BYOD) par l'application homogène de politiques d'utilisation sur l'ensemble des appareils portables. Les fonctions de sécurité comprennent le verrouillage de l'écran, le contrôle d'authentification, la localisation de l'appareil, la suppression des données à distance, la détection des appareils rootés ou jailbreakés et des profils de sécurité. Sur les appareils Android, le niveau de sécurité est amélioré par l'analyse en temps réel et le cryptage des supports amovibles. Les appareils mobiles sont donc contrôlés et les informations professionnelles sensibles qui s'y trouvent sont protégées.

2.15. Disponibilité des couches de protection de GravityZone

La disponibilité des couches de protection de GravityZone varie en fonction du système d'exploitation de l'endpoint. Pour en apprendre plus, consultez l'article de la base de connaissances Disponibilité des couches de protection de GravityZone.

3. L'ARCHITECTURE DE GRAVITYZONE

L'architecture unique de GravityZone permet à la solution de s'adapter facilement et de protéger un nombre illimité de systèmes. GravityZone peut être configuré pour utiliser plusieurs appliances virtuelles et plusieurs instances de rôles spécifiques (Base de données, Serveur de communication, Serveur de mise à jour et Console web) pour assurer fiabilité et extensibilité.

Chaque instance de rôle peut être installée sur une appliance différente. Les équilibreurs de rôles intégrés permettent au déploiement de GravityZone de protéger même les plus grands réseaux d'entreprise sans provoquer de ralentissements ni de goulets d'étranglement. Si des logiciels ou du matériel d'équilibrage de charge sont présents dans le réseau, ils peuvent être utilisés au lieu des équilibreurs intégrés.

Fournie sous la forme d'une appliance virtuelle, GravityZone peut être importée pour s'exécuter sur toute plate-forme de virtualisation, y compris VMware, Citrix, Microsoft Hyper-V, Nutanix Prism et Microsoft Azure.

L'intégration à VMware vCenter, Citrix XenServer, Microsoft Active Directory, Nutanix Prism Element et Microsoft Azure facilite le déploiement de la protection pour les endpoints physiques et virtuels.

La solution GravityZone comporte les composants suivants :

- Appliance virtuelle GravityZone
- Security Server
- Agents de sécurité

3.1. Appliance virtuelle GravityZone

La solution sur site GravityZone est fournie sous la forme d'une appliance virtuelle sécurisée (VA) Linux Ubuntu, se configurant automatiquement et intégrée à une image de machine virtuelle. Elle est facile à installer et à configurer via une interface en ligne de commande (CLI). L'appliance virtuelle est disponible en plusieurs formats, compatibles avec les principales plates-formes de virtualisation (OVA, XVA, VHD, OVF, RAW).

3.1.1. Base de données de GravityZone

La logique centrale de l'architecture de GravityZone. Bitdefender utilise une base de données non relationnelle MongoDB, facilement extensible et réplicable.

3.1.2. Serveur de mise à jour GravityZone

Le serveur de mise à jour a un important rôle de mise à jour de la solution GravityZone et des agents des endpoints par la réplication et la publication des packages ou des fichiers d'installation nécessaires.

3.1.3. Serveur de communication GravityZone

Le serveur de communication est le lien entre les agents de sécurité et la base de données ; il transmet les politiques et les tâches aux endpoints protégés ainsi que les événements signalés par les agents de sécurité.

3.1.4. Console Web (GravityZone Control Center)

Les solutions de sécurité de Bitdefender sont gérées depuis un seul endroit, la console web Control Center. La gestion est ainsi plus simple, et il est possible d'accéder au niveau général de sécurité, aux menaces de sécurité globales et d'utiliser tous les modules de sécurité en charge de la protection des bureaux physiques ou virtuels, des serveurs et des appareils mobiles. Intégrant l'architecture "Gravity", le Control Center est capable de répondre aux besoins de toutes les entreprises, quelle que soit leur taille.

Control Center s'intègre aux systèmes de surveillance et de gestion des infrastructures existantes afin d'appliquer automatiquement la protection aux postes de travail, serveurs ou appareils mobiles non administrés apparaissant dans Microsoft Active Directory, VMware vCenter, Citrix XenServer, Nutanix Prism Element, ou à ceux qui sont simplement détectés dans le réseau.

3.2. Security Server

Le Security Server est une machine virtuelle dédiée qui déduplique et centralise la plus grande partie de la fonctionnalité antimalware des agents antimalware, en agissant en tant que serveur d'analyse.

Il existe trois versions de Security Server, pour chaque type d'environnement de virtualisation :

- **Security Server pour VMware NSX.** Cette version s'installe automatiquement sur chaque hôte dans le cluster où Bitdefender a été déployé.
- **Security Server pour VMware vShield Endpoint.** Cette version doit être installée sur chaque hôte à protéger.

- **Security Server Multi-Plateformes.** Cette version est pour d'autres environnements virtualisés et doit être installée sur un ou plusieurs hôtes afin d'accueillir le nombre de machines virtuelles protégées.

3.3. Agents de sécurité

Pour protéger votre réseau avec Bitdefender, vous devez installer les agents de sécurité de GravityZone adaptés sur les endpoints du réseau.

- Bitdefender Endpoint Security Tools
- Endpoint Security for Mac
- GravityZone Mobile Client
- Bitdefender Tools (vShield)

3.3.1. Bitdefender Endpoint Security Tools

GravityZone assure la protection des machines Windows et Linux physiques et virtuelles avec Bitdefender Endpoint Security Tools, un agent de sécurité intelligent et conscient de son environnement qui s'adapte au type d'endpoint. Bitdefender Endpoint Security Tools peut être déployé sur n'importe quelle machine, physique ou virtuelle, pour fournir un système d'analyse flexible, un choix idéal pour les environnements mixtes (physique, virtuel et cloud).

En plus de la protection du système de fichiers, Bitdefender Endpoint Security Tools comprend étalement une protection des serveurs de messagerie pour les serveurs Microsoft Exchange.

Bitdefender Endpoint Security Tools utilise un modèle de politique unique pour les machines physiques et virtuelles et un kit d'installation pour tout environnement (physique ou virtuel) sous Windows.

Couches de protection

Les couches de protection suivantes sont disponibles avec Bitdefender Endpoint Security Tools :

- Antimalware
- Advanced Threat Control
- Pare-feu
- Contrôle de contenu
- Network Attack Defense
- Gestion des correctifs

- Contrôle des appareils
- Chiffrement complet du disque
- Security for Exchange

Rôles des endpoints

- Power User
- Relais
- Serveur de mise en cache des patchs
- Protection Exchange

Power User

Les administrateurs de Control Center peuvent accorder des droits Power User aux utilisateurs d'endpoints via des paramètres de politique. Le module Power User fournit des droits d'administration au niveau de l'utilisateur, permettant à l'utilisateur de l'endpoint d'accéder et de modifier les paramètres de sécurité via une console locale. Control Center est informé lorsqu'un endpoint est en mode Power User et l'administrateur de Control Center peut toujours écraser les paramètres de sécurité locaux.

Important
Ce module est disponible uniquement pour les systèmes d'exploitation des postes de travail et serveurs Windows pris en charge. Pour plus d'informations, reportez-vous à « Systèmes d'exploitation pris en charge » (p. 26).

Relais

Les agents des endpoints avec le rôle Bitdefender Endpoint Security Tools Relay servent de serveurs de communication proxy et de serveurs de mise à jour aux autres endpoints du réseau. Les agents d'endpoints avec le rôle relais sont particulièrement nécessaires dans les entreprises ayant des réseaux isolés, dans lesquels tout le trafic passe par un point d'accès unique.

Dans les entreprises ayant de grands réseaux distribués, les agents relais contribuent à diminuer l'utilisation de la bande passante, en empêchant les endpoints protégés et les serveurs de sécurité de se connecter directement à l'appliance GravityZone.

Lorsqu'un agent Bitdefender Endpoint Security Tools Relay est installé dans le réseau, d'autres endpoints peuvent être configurés avec une politique pour communiquer avec Control Center via l'agent relais.

Les agents Bitdefender Endpoint Security Tools Relay remplissent les fonctions suivantes :

- Ils détectent tous les endpoints non protégés dans le réseau.
- Ils déploient l'agent de l'endpoint dans le réseau local.
- Ils mettent à jour les endpoints protégés du réseau.
- Ils assurent la communication entre Control Center et les endpoints connectés.
- Ils agissent en tant que serveurs proxy pour les endpoints protégés.
- Optimiser le trafic réseau pendant les mises à jour, les déploiements, les analyses et autres tâches qui consomment des ressources.

Serveur de mise en cache des patchs

Les endpoints avec rôle de Relais peuvent également faire office de Serveur de mise en cache des patchs. Une fois ce rôle activé, les Relais servent à stocker les patchs téléchargés sur le site Web du fournisseur, et les distribuent aux endpoints cibles de votre réseau. Lorsqu'un des endpoints connectés a un logiciel pour lequel tous les patchs ne sont pas installés, il les récupère sur le serveur et non pas sur le site Web du fournisseur, optimisant ainsi le trafic généré et la bande passante utilisée.

Important
Ce rôle supplémentaire est disponible une fois l'extension Gestion des patchs enregistrée.

Protection Exchange

Bitdefender Endpoint Security Tools avec le rôle Exchange peut être installé sur les serveurs Microsoft Exchange afin de protéger les utilisateurs d'Exchange contre les menaces présentes dans les e-mails.

Bitdefender Endpoint Security Tools avec le rôle Exchange protège à la fois la machine serveur et la solution Microsoft Exchange.

3.3.2. Endpoint Security for Mac

Endpoint Security for Mac est un agent de sécurité conçu pour protéger les postes de travail et les ordinateurs portables Macintosh équipés d'un processeur Intel. La technologie d'analyse disponible est l'**Analyse locale**, avec les contenus de sécurité stockés en local.

Couches de protection

Les couches de protection suivantes sont disponibles avec Endpoint Security for Mac :

- Antimalware
- Advanced Threat Control
- Contrôle de contenu
- Contrôle des appareils
- Chiffrement complet du disque

3.3.3. GravityZone Mobile Client

GravityZone Mobile Client applique facilement les politiques de sécurité à un nombre illimité d'appareils Android et iOS, les protégeant ainsi de l'utilisation non autorisée, des riskwares et de la perte de données confidentielles. Les fonctions de sécurité comprennent le verrouillage de l'écran, le contrôle d'authentification, la localisation de l'appareil, la suppression des données à distance, la détection des appareils rootés ou jailbreakés et des profils de sécurité. Sur les appareils Android, le niveau de sécurité est amélioré par l'analyse en temps réel et le cryptage des supports amovibles.

GravityZone Mobile Client est distribué exclusivement via Apple App Store et Google Play.

3.3.4. Bitdefender Tools (vShield)

Bitdefender Tools est un agent léger pou les environnements virtualisés VMware qui sont intégrés dans vShield Endpoint. L'agent de sécurité s'installe sur des machines virtuelles protégées par Security Server, afin de vous permettre de profiter de la fonctionnalité supplémentaire qu'il fournit :

- Vous permet d'exécuter des tâches d'analyse de la mémoire et des processus sur la machine.
- Informe l'utilisateur des infections détectées et des actions qui leur ont été appliquées.
- Ajoute plus d'options pour les exclusions d'analyse antimalware.

3.4. Architecture de Sandbox Analyzer

Offrant une puissante couche de protection contre les menaces avancées, le Sandbox Analyzer for Endpoints de Bitdefender effectue des analyses automatiques

détaillées des fichiers suspects, qui n'ont pas encore été signalés par les moteurs antimalware de Bitdefender.

Pour utiliser ce module avec GravityZone, vous devez installer Sandbox Analyzer On-Premises.

Sandbox Analyzer On-Premises

Sandbox Analyzer On-Premises est une appliance virtuelle Linux Ubuntu embarquée sur une image de machine virtuelle, facile à installer et à configurer via une interface de ligne de commande. Sandbox Analyzer On-Premises est disponible au format OVA, déployable sur VMWare ESXi.

Une instance Sandbox Analyzer On-Premises contient les composants suivants :

- **Sandbox Manager**. Ce composant est le gestionnaire de la sandbox. Sandbox Manager se connecte à l'hyperviseur ESXi via une API et utilise ses ressources matérielles pour créer et exploiter un environnement d'analyse des malwares.
- **Machines virtuelles de détonation**. Ce composant est constitué de machines virtuelles exploitées par Sandbox Analyzer pour exécuter des fichiers et analyser leur comportement. Les machines virtuelles de détonation peuvent tourner sous les systèmes d'exploitation Windows 7 et Windows 10 64 bits.

GravityZone Control Center est à la fois console d'administration et de reporting, où vous pourrez configurer les politiques de sécurité, consulter les rapports d'analyses et voir les notifications.

Sandbox Analyzer On-Premises utilise les capteurs d'alimentation suivants :

- **Capteur réseau**. Network Security Virtual Appliance (NSVA) est une appliance virtuelle déployable sur le même environnement virtualisé ESXi que l'instance Sandbox Analyzer. Le capteur réseau extrait le contenu des flux réseau et l'envoie à Sandbox Analyzer.
- **Capteur ICAP** Déployé sur un serveur de stockage en réseau utilisant le protocole ICAP, Bitdefender Security Server prend en charge l'envoi de contenu à Sandbox Analyzer.

En plus de ces capteurs, Sandbox Analyzer On-Premises permet d'envoyer des échantillons manuellement ou via une API. Pour plus de détails, consultez le chapitre **Utilisation de Sandbox Analyzer** du Guide de l'administrateur de GravityZone.

4. CONFIGURATION REQUISE

Toutes les solutions GravityZone sont installées et gérées via le Control Center.

4.1. Appliance virtuelle GravityZone

4.1.1. Plateformes de virtualisation et formats pris en charge

GravityZone est fournie sous la forme d'une appliance virtuelle (AV). Elle est disponible dans les formats suivants, compatibles avec la plupart des plateformes de virtualisation :

- OVA (compatible avec VMware vSphere, View, VMware Player)
- XVA (compatible avec Citrix XenServer, XenDesktop, VDI-in-a-Box)
- VHD (compatible avec Microsoft Hyper-V)
- VMDK (compatible avec Nutanix Prism)
- OVF (compatible avec Red Hat Enterprise Virtualization)*
- OVF (compatible avec Oracle VM)*
- RAW (compatible avec Kernel-based Virtual Machine ou KVM)*

*les packages OVF et RAW sont archivés au format tar.bz2.

Pour la compatibilité avec la plateforme Oracle VM VirtualBox, veuillez vous référer à cet article KB.

Le support d'autres plateformes de virtualisation est fourni sur demande.

4.1.2. Matériel

La configuration matérielle requise pour l'installation de l'appliance virtuelle GravityZone dépend de la taille de votre réseau et de l'architecture de déploiement que vous choisissez. Pour les réseaux comptant jusqu'à 3 000 endpoints, vous pouvez choisir d'installer tous les rôles GravityZone sur une même appliance. Pour les réseaux de plus grande ampleur, il est préférable de distribuer les rôles sur plusieurs appliances. Les ressources nécessaires au fonctionnement de l'appliance varient en fonction des rôles que vous installez sur celle-ci et de l'utilisation (ou non) de Replica Set.

Note
Replica Set est une fonctionnalité de MongoDB qui permet la réplication des bases de données et assure ainsi la redondance et la grande disponibilité des données stockées. Pour plus d'informations, consultez la documentation MongoDB et « Gérer l'appliance GravityZone » (p. 99).

Important
Ces mesures proviennent de tests réalisés en interne par Bitdefender avec une configuration GravityZone de base et dans des conditions d'utilisation classiques. Les résultats que vous obtiendrez peuvent varier selon la configuration du réseau, les logiciels installés, le nombre d'événements générés, etc. Pour recevoir des métriques personnalisées sur l'extensibilité, contactez Bitdefender.

vCPU

Le tableau suivant indique le nombre de vCPU nécessaires pour chacun des rôles de l'appliance virtuelle.

Chaque vCPU doit être d'au moins 2 GHz.

Composant	Nombre d'endpoints (jusqu'à)							
	250	500	1000	3000	5000	10000	25000	50000
Fonctionnalités de base de GravityZone								
Serveur de mise à jour*	8	12	14	16	4	4	6	8
Console Web**					6	10	12	12
Serveur de communication					6	10	12	18
Base de données***					6	6	9	12
Total	**8**	**12**	**14**	**16**	**22**	**30**	**39**	**50**
GravityZone avec Bitdefender HVI								
Serveur de mise à jour*	8	4	4	4	4	4	6	8
Console Web**		6	8	8	10	10	12	12
Serveur de communication		6	8	8	10	10	16	20
Base de données***		6	6	6	6	6	9	12
Total	**8**	**22**	**26**	**26**	**30**	**30**	**43**	**52**

* Recommandé si aucun relais n'est déployé.

** Pour chaque intégration active, ajoutez une vCPU sur l'appliance virtuelle sur laquelle le rôle de Console Web est installé.
*** En cas de distribution des rôles, avec utilisation de Replica Set : pour chaque instance de base de données supplémentaire, ajoutez le nombre indiqué au nombre total.

RAM (Go)

Composant	Nombre d'endpoints (jusqu'à)							
	250	500	1000	3000	5000	10000	25000	50000
Fonctionnalités de base de GravityZone								
Serveur de mise à jour	16	16	18	20	2	2	3	3
Console Web*					8	8	12	16
Serveur de communication					6	12	12	16
Base de données**					8	10	12	12
Total	**16**	**16**	**18**	**20**	**24**	**32**	**39**	**47**
GravityZone avec Bitdefender HVI								
Serveur de mise à jour	16	2	2	2	2	2	3	3
Console Web*		8	10	10	10	10	12	16
Serveur de communication		8	10	10	12	12	16	20
Base de données**		8	8	8	8	12	12	12
Total	**16**	**26**	**30**	**30**	**32**	**36**	**43**	**51**

** Pour chaque intégration active, ajoutez un Go de RAM sur l'appliance virtuelle sur laquelle le rôle de Console Web est installé.
** En cas de distribution des rôles, avec utilisation de Replica Set : pour chaque instance de base de données supplémentaire, ajoutez le nombre indiqué au nombre total.

Espace disque disponible (Go)

Composant	Nombre d'endpoints (jusqu'à)								
	250	250*	500	1000	3000	5000	10000	25000	50000
Fonctionnalités de base de GravityZone									
Serveur de mise à jour	120	**160**	160	200	200	80	80	80	80
Console Web						80	80	80	80
Serveur de communication						80	80	80	80
Base de données**						80	120	200	500
Total	**120**	**160**	**160**	**200**	**200**	**320**	**360**	**440**	**740**
GravityZone avec Bitdefender HVI									
Serveur de mise à jour	120	160	80	80	80	80	80	80	80
Console Web			80	80	80	80	80	80	80
Serveur de communication			80	80	80	80	80	80	80
Base de données**			80	80	100	100	160	300	700
Total	**120**	**160**	**320**	**320**	**340**	**340**	**400**	**540**	**940**

Important
L'utilisation de disques SSD est fortement recommandée.

* Un espace SSD supplémentaire est nécessaire si vous optez pour l'installation automatique, car dans ce cas le Security Server est également installé. Après l'installation, vous pouvez désinstaller le Security Server pour libérer de l'espace sur le disque.
** En cas de distribution des rôles, avec utilisation de Replica Set : pour chaque instance de base de données supplémentaire, ajoutez le nombre indiqué au nombre total.

4.1.3. Connexion Internet

L'appliance GravityZone requiert un accès à Internet.

4.2. Control Center

Pour accéder à la console Web Control Center, la configuration requise est la suivante :

- Internet Explorer 9+, Mozilla Firefox 14+, Google Chrome 15+, Safari 5+, Microsoft Edge 20+, Opera 16+
- Résolution d'écran recommandée : 1280 x 800 ou supérieure
- L'ordinateur à partir duquel vous vous connectez doit avoir une connectivité réseau avec Control Center.

Avertissement
Le Control Center ne fonctionnera pas / ne s'affichera pas correctement dans Internet Explorer 9+ avec la fonctionnalité Affichage de compatibilité activée, ce qui revient à utiliser une version de navigateur non supportée.

4.3. Protection des postes de travail

Pour protéger votre réseau avec Bitdefender, vous devez installer les agents de sécurité GravityZone sur les endpoints du réseau. Pour une protection optimisée, vous pouvez également installer des Security Servers. Pour ce faire, vous avez besoin d'un utilisateur Control Center avec des privilèges administrateurs sur les services que vous devez installer et sur les endpoints du réseau que vous gérez.

La configuration requise pour les agents de sécurité varie selon qu'ils ont ou non un rôle complémentaire de serveur (serveur relais, serveur de protection Exchange ou serveur de mise en cache des patchs). Pour plus d'informations sur les rôles des agents, reportez-vous à « Agents de sécurité » (p. 11).

4.3.1. Matériel

Agent de sécurité sans rôle

Util. du proc.

Systèmes cibles	Type de proc.	Systèmes d'exploitation pris en charge
Postes de travail	Processeurs compatibles Intel® Pentium, 2 GHz ou plus	Systèmes d'exploitation Microsoft Windows de bureau
	Intel® Core 2 Duo, 2 GHz ou plus	macOS
Appareils connectés	Processeurs compatibles Intel® Pentium, 800 MHz ou plus	Systèmes d'exploitation intégrés Microsoft Windows
Serveurs	Minimum : processeurs compatibles Intel® Pentium 2,4 GHz	Systèmes d'exploitation Microsoft Windows Server et Linux
	Recommandé : processeur Intel® Xeon multicœurs, 1,86 GHz ou plus	

Avertissement
Les processeurs ARM ne sont actuellement pas pris en charge.

Mémoire RAM disponible

À l'installation (Mo)

OS	MOTEUR UNIQUE					
	Analyse locale		Analyse hybride		Analyse centralisée	
	AV seul.	Toutes les options	AV seul.	Toutes les options	AV seul.	Toutes les options
Windows	1024	1200	512	660	256	400
Linux	1024	1024	512	512	256	256
macOS	1024	1024	n/d	n/d	n/d	n/d

Pour l'utilisation quotidienne (Mo)*

OS	Antivirus /n(Moteur unique)			Modules de protection				
	Local	Hybride	Centralisé	Analyse comporte-mentale	Pare-feu	Contrôle du contenu	Power User	Mise à jour Serveur
Windows	75	55	30	+13	+17	+41	+29	+80
Linux	200	180	90	-	-	-	-	-
macOS	650	-	-	+100	-	+50	-	-

* Les mesures couvrent l'usage client quotidien d'endpoint, sans prendre en compte les tâches supplémentaires, comme les analyses à la demande ou les mises à jour produit.

Espace disque libre

À l'installation (Mo)

OS	MOTEUR UNIQUE						MOTEUR DOUBLE			
	Analyse locale		Analyse hybride		Analyse centralisée		Analyse centralisée + locale		Analyse centralisée + hybride	
	AV seul.	Toutes les options	AV seul.	Toutes les options	AV seul.	Toutes les options	AV seul.	Toutes les options	AV seul.	Toutes les options
Windows	1024	1200	500	700	350	570	1024	1200	500	700
Linux	1600	1600	1100	1100	600	600	1600	1600	1100	1100
macOS	1024	1024	n/d	n/d	n/d	n/d	n/d	n/d	n/d	n/d

Pour l'utilisation quotidienne (Mo)*

OS	Antivirus (Moteur unique)			Modules de protection				
	Local	Hybride	Centralisé	Analyse comporte-mentale	Pare-feu	Contrôle du contenu	Power User	Mise à jour Serveur
Windows	410	190	140	+12	+5	+60	+80	+10
Linux	500	200	110	-	-	-	-	-
macOS	1700	-	-	+20	-	+0	-	-

* Les mesures couvrent l'usage client quotidien d'endpoint, sans prendre en compte les tâches supplémentaires, comme les analyses à la demande ou les mises à jour produit.

Agent de sécurité avec rôle de serveur relais

Le rôle de serveur relais nécessite des ressources supplémentaires, qui s'ajoutent à la configuration de base. Cela permet de prendre en charge le serveur de mise à jour et les packages d'installation hébergés par l'endpoint . :

Nombre d'endpoint connectés	Processeur prenant en charge le serveur de mise à jour	RAM	Espace disque disponible pour le serveur de mise à jour
1-300	Minimum : processeur Intel® Core™ i3 ou équivalent, 2 vCPU par cœur	1,0 Go	10 Go
300-1000	Minimum : processeur Intel® Core™ i5 ou équivalent, 4 vCPU par cœur	1,0 Go	10 Go

Avertissement

- Les processeurs ARM ne sont actuellement pas pris en charge.
- Les agents relais ont besoin de disques SSD, pour prendre en charge le grand nombre d'opérations de lecture/écriture.

Important

- Si vous souhaitez sauvegarder les packages d'installation et les mises à jour sur un autre disque que celui sur lequel l'agent est installé, veillez à ce que les deux

disques contiennent suffisamment d'espace disponible (10 Go). Sinon l'agent abandonne le processus d'installation. C'est nécessaire uniquement pendant l'installation.

- Sur les endpoints Windows, les liens symboliques local à local doivent être activés.

Agent de sécurité avec rôle de serveur de protection Exchange

La quarantaine des Serveurs Exchange requiert de l'espace disque supplémentaire sur la partition où l'agent de sécurité est installé.

La taille de la quarantaine dépend du nombre d'éléments qu'elle comporte et de leur taille.

Par défaut, l'agent est installé sur la partition système.

Agent de sécurité avec rôle de serveur de mise en cache des patchs

L'agent avec rôle de serveur de mise en cache des patchs doit cumuler les configurations suivantes :

- La configuration matérielle requise pour l'agent de sécurité simple (sans rôle)
- La configuration matérielle requise pour le rôle de serveur relais
- 100 Go supplémentaires d'espace disponible sur le disque pour le stockage des patchs téléchargés

Important
Si vous souhaitez sauvegarder les patchs sur un autre disque que celui sur lequel l'agent est installé, veillez à ce que les deux disques contiennent suffisamment d'espace disponible (100 Go). Sinon l'agent abandonne le processus d'installation. C'est nécessaire uniquement pendant l'installation.

Pré-requis pour les environnements VMware vShield

Voici la configuration requise et empreinte des Bitdefender Tools pour les systèmes intégrés aux environnements VMware avec vShield Endpoint.

Plateforme	RAM	Espace disque
Windows	6-16* Mo (~ 10 Mo for GUI)	24 Mo
Linux	9-10 Mo	10-11 Mo

*5 Mo quand l'option Mode Silencieux est activée et 10 Mo quand elle est désactivée. Lorsque le mode silencieux est activé, l'interface utilisateur graphique des Bitdefender Tools n'est pas chargée automatiquement au démarrage du système, libérant les ressources associées.

4.3.2. Systèmes d'exploitation pris en charge

Systèmes d'exploitation pour postes de travail Windows

- Windows 10 October 2020 Update (20H2)
- Windows 10 May 2020 Update (20H1)
- Windows 10 November 2019 Update (19H2)
- Windows 10 May 2019 Update (19H1)
- Mise à jour de Windows 10 du 10 octobre 2018 (Redstone 5)
- Windows 10 April 2018 Update (Redstone 4)
- Windows 10 Fall Creators Update (Redstone 3)
- Windows 10 Creators Update (Redstone 2)
- Windows 10 Anniversary Update (Redstone 1)
- Windows 10 November Update (Threshold 2)
- Windows 10
- Windows 8.1 (1)(2)
- Windows 8(3)
- Windows 7

Avertissement
* (3) Le support de la plate-forme VMware vShield (version sans agents) pour Windows 8.1 (32/64 bits) est disponible à partir de VMware vSphere 5.5 – ESXi build 1892794 et versions supérieures.
(2) Dans VMware NSX, la version OS est prise en charge à partir de vSphere 5.5 Patch 2.
(3) Dans VMware NSX, la version OS est prise en charge à partir de vSphere 5.5.

Avertissement
Bitdefender n'est pas compatible avec les builds du programme Insider de Windows.

Systèmes d'exploitation pour tablettes Windows et systèmes embarqués

- Windows 10 IoT Enterprise
- Windows Embedded 8.1 Industry
- Windows Embedded 8 Standard
- Windows Embedded Standard 7
- Windows Embedded Compact 7
- Windows Embedded POSReady 7
- Windows Embedded Enterprise 7

Windows Server

- Windows Server 2019
- Windows Server 2019 Core
- Windows Server 2016
- Windows Server 2016 Core
- Windows Server 2012 R2[(1)(2)]
- Windows Server 2012[(3)(4)]
- Windows Small Business Server (SBS) 2011
- Windows Server 2008 R2[(4)]

Avertissement

(1) Le support de la plate-forme VMware vShield (version sans agents) pour Windows Server 2012 R2 (64 bits) est disponible à partir de VMware vSphere 5.5 – ESXi build 1892794 et versions supérieures.
(2) Dans VMware NSX, la version OS est prise en charge à partir de vSphere 5.5 Patch 2.
(3) Dans VMware NSX, la version OS est prise en charge à partir de vSphere 5.5.
(4) VMware NSX ne prend pas en charge les versions 32 octets de Windows 2012 et Windows Server 2008 R2.

Linux

Important
Les endpoints Linux utilisent des sièges issus du pool de licences pour les systèmes d'exploitation serveur.

- Ubuntu 14.04 LTS ou supérieur
- Red Hat Enterprise Linux / CentOS 6.0 ou supérieur(2)
- SUSE Linux Enterprise Server 11 SP4 ou supérieur
- OpenSUSE Leap 42.x
- Fedora 25 ou supérieur(1)
- Debian 8.0 ou supérieur
- Oracle Linux 6.3 ou supérieur
- Amazon Linux AMI 2016.09 ou supérieure
- Amazon Linux 2

Avertissement
(1) Sur Fedora 28 et supérieur, Bitdefender Endpoint Security Tools nécessite une installation manuelle du package `libnsl`, en exécutant la commande suivante :

```
sudo dnf install libnsl -y
```

(2) pour les installations minimales de CentOS, Bitdefender Endpoint Security Tools nécessite l'installation manuelle du package `libnsl`, en exécutant la commande suivante :

```
sudo yum install libnsl
```

Prérequis d'Active Directory

Lors de l'intégration d'endpoints Linux avec un domaine Active Directory via System Security Services Daemon (SSSD), vérifiez que les outils **ldbsearch, krb5-user,** et **krb5-config** sont installés et que kerberos est correctement configuré.

```
/etc/krb5.conf

[logging]
```

```
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
        default_realm = DOMAIN.NAME
        dns_lookup_realm = true
        dns_lookup_kdc = true
        kdc_timesync = 1
        ccache_type = 4
        forwardable = true
        proxiable = true
        fcc-mit-ticketflags = true
        default_keytab_name = FILE:/etc/krb5.keytab

[realms]
        DOMAIN.NAME = {
                        kdc = dc1.domain.name
                        kdc = dc2.domain.name
                        admin_server = dc.domain.com
                        default_domain = domain.com
        }

[domain_realm]
 domain.name = DOMAIN.NAME
 .domain.name = DOMAIN.NAME

[appdefaults]
 pam = {
        debug = false
        ticket_lifetime = 36000
        renew_lifetime = 36000
        forwardable = true
        krb4_convert = false
        }
```

Note
Toutes les entrées sont sensibles à la casse .

Prise en charge de l'analyse à l'accès

L'analyse à l'accès est disponible pour tous les systèmes d'exploitation supportés. Sur les systèmes Linux, le support de l'analyse à l'accès est assuré dans les situations suivantes :

Versions du noyau	Distributions Linux	Prérequis à l'accès
2.6.38 ou supérieur*	Red Hat Enterprise Linux / CentOS 6.0 ou supérieur Ubuntu 14.04 ou supérieur SUSE Linux Enterprise Server 11 SP4 ou supérieur OpenSUSE Leap 42.x Fedora 25 ou supérieur Debian 9.0 ou supérieur Oracle Linux 6.3 ou supérieur Amazon Linux AMI 2016.09 ou supérieure	**Fanotify** (option du noyau) doit être activé.
2.6.38 ou supérieur	Debian 8	**Fanotify** doit être activé et en mode « enforce », puis le noyau doit être recompilé. Pour plus d'informations, consultez cet article de la base de connaissances :
2.6.32 - 2.6.37	CentOS 6.x Red Hat Enterprise Linux 6.x	Bitdefender assure la prise en charge des modules préinstallés avec le noyau via **DazukoFS**.
Tous les autres noyaux	Tous les autres systèmes pris en charge	Le module **DazukoFS** doit être compilé manuellement. Pour plus d'informations, reportez-vous à « Compiler manuellement le module DazukoFS » (p. 147).

* Avec certaines limitations décrites ci-dessous.

Limitations de l'analyse à l'accès

Versions du noyau	Distributions Linux	Détails
2.6.38 ou supérieur	Tous les systèmes pris en charge	L'analyse à l'accès ne surveille les partages réseau montés que dans les conditions suivantes : • **Fanotify** est activé sur les systèmes à distance et locaux. • Le partage est basé sur les systèmes de fichier CIFS et NFS. **Note** L'analyse à l'accès n'analyse pas les partages réseau montés par SSH ou FTP.
Tous les noyaux	Tous les systèmes pris en charge	Pour les systèmes sur lesquels **DazukoFS** est installé, l'analyse à l'accès n'est pas prise en charge pour les partages réseau montés à des emplacements déjà protégés par le module à l'accès.

macOS

- macOS Big Sur (11.0)*
- macOS Catalina (10.15)
- macOS Mojave (10.14)
- macOS High Sierra (10.13)
- macOS Sierra (10.12)
- OS X El Capitan (10.11)

Content Control non pris en charge par macOS Big Sur (11.0).

4.3.3. Système de fichiers pris en charge

Bitdefender installe et protège les systèmes de fichier suivants :

AFS, BTRFS, ext2, ext3, ext4, FAT, FAT16, FAT32, VFAT, exFAT, NTFS, UFS, ISO 9660 / UDF, NFS, CIFS/SMB, VXFS, XFS.

Note
La prise en charge de l'analyse à l'accès n'est pas fournie pour NFS et CIFS/SMB.

4.3.4. Navigateurs pris en charge

La sécurité du navigateur du poste de travail fonctionne avec les navigateurs suivants :

- Internet Explorer 8+
- Mozilla Firefox 30+
- Google Chrome 34+
- Safari 4+
- Microsoft Edge 20+
- Opera 21+

4.3.5. Plateformes de virtualisation supportées

Security for Virtualized Environments fournit un support immédiat pour les plateformes de virtualisation suivantes :

- VMware vSphere & vCenter Server 7.0, 6.7 update 3, update 2a, 6.7 update 1, 6.7, 6.5, 6.0, 5.5, 5.1, 5.0

  Note
  La fonctionnalité Workload Management de vSphere 7.0 n'est pas prise en charge.

- VMware Horizon/View 7.8, 7.7, 7.6, 7.5, 7.1, 6.x, 5.x
- VMware Workstation 11.x, 10.x, 9.x, 8.0.6
- Lecteur VMware 7.x, 6.x, 5.x
- Citrix XenServer 8.x, 7.x, 6.5, 6.2, 6.0, 5.6 or 5.5 (y compris Xen Hypervisor)
- Citrix Virtual Apps et Desktops 7 1808, 7 1811, 7 1903, 7 1906
- Citrix XenApp et XenDesktop 7.18, 7.17, 7.16, 7.15 LTSR, 7.6 LTSR
- Citrix VDI-in-a-Box 5.x

- Microsoft Hyper-V Server 2008 R2, 2012, 2012 R2 ou Windows Server 2008 R2, 2012, 2012 R2 (avec l'hyperviseur Hyper-V)
- Red Hat Enterprise Virtualization 3.0 (avec KVM Hypervisor)
- Oracle VM 3.0
- Oracle VM VirtualBox 5.2, 5.1
- Nutanix Prism with AOS (LTS) 5.5, 5.10, 5.15
- Nutanix Prism with AOS (STS) 5.6, 5.11, 5.18
- Nutanix Prism with AHV (Community Edition) 20170830.115, 20170830.301, 20170830.395, 20190916.294

Note
Le support d'autres plateformes de virtualisation peut être fourni sur demande.

Pré-requis pour l'intégration avec VMware NSX-V

- ESXi 5.5 ou plus pour chaque serveur
- vCenter Server 5.5 ou plus
- NSX Manager 6.2.4 ou plus
- VMware Tools 9.1.0 ou supérieur, avec l'agent léger Guest Introspection.
  - Pour les machines virtuelles Windows, consultez cet article VMware Docs.
  - Pour les machines virtuelles Linux, consultez cet article VMware Docs.

Note
VMware recommande d'utiliser les versions suivantes de VMware Tools :

- 10.0.8 ou suivante pour résoudre les problèmes de lenteur des VM après mise à niveau de VMware Tools dans NSX/vCloud Networking and Security (article 2144236 de la Base de connaissances VMware).
- 10.0.9 et suivantes pour prise en charge par Windows 10.

Important
Nous vous recommandons de maintenir à jour tous les produits VMware avec le dernier correctif.

Configuration requise pour l'intégration à VMware NSX-T Data Center

- VMware NSX-T Manager 2.4, 2.5 ou 3.0
- ESXi compatible avec la version de NSX-T Manager
- vCenter Server & vSphere compatible avec la version de NSX-T Manager
- VMware Tools avec l'agent léger Guest Introspection, compatible avec la version de NSX-T Manager

Pour en apprendre plus sur la compatibilité, consultez les pages web suivantes de VMware :

- VMware Compatibility Guide – GravityZone vs. NSX-T Manager
- VMware Product Interoperability Matrices - NSX-T Data Center vs. VMware vCenter and VMware Tools

Prérequis de l'intégration avec Nutanix Prism Element

- Les identifiants d'un utilisateur de Nutanix Prism Element avec les privilèges administrateur (Administrateur de cluster ou Utilisateur admin).
- Nutanix Prism with AOS (LTS) 5.5, 5.10, 5.15
- Nutanix Prism with AOS (STS) 5.6, 5.11, 5.18
- Nutanix Prism with AHV (Community Edition) 20170830.115, 20170830.301, 20170830.395, 20190916.294

Plateformes cloud prises en charge

En plus des environnements de virtualisation sur site, GravityZone peut aussi intégrer les plateformes cloud suivantes :

- **Amazon EC2**

  En tant que client Amazon EC2, vous pouvez intégrer l'inventaire des instances EC2 (groupées par régions et zones de disponibilité) à l'inventaire réseau GravityZone.

- **Microsoft Azure**

  En tant que client Microsoft Azure, vous pouvez intégrer les machines virtuelles Microsoft Azure (groupées par régions et zones de disponibilité) à l'inventaire réseau GravityZone.

Compatibilité avec les technologies de virtualisation des applications et des bureaux

GravityZone est compatible avec les technologies de virtualisation suivantes à compter de Bitdefender Endpoint Security Tools version 6.6.16.226 :

- **VMware :**

  VMware V-App (même version que vCenter Server)

  VMware ThinApp 5.2.6

  VMware AppVolumes 2.180

  Important
  Il est recommandé de ne pas procéder à l'installation dans la pile d'application ou sur des volumes inscriptibles.

- **Microsoft :**

  Microsoft App-V 5.0, 5.1

  Microsoft FSLogix 2.9.7237

- **Citrix :**

  Citrix App Layering 19.10

  Citrix Appdisks 7.12

  Important
  Affectez les politiques sur la base de règles de l'utilisateur pour que le Contrôle des appareils n'empêche pas la création de couches OS et plateforme.
  Il vous faudra peut-être configurer les règles du Pare-feu GravityZone pour permettre le trafic réseau vers chacune de ces applications. Pour en apprendre plus, voir la documentation produit Citrix App Layering.

Outils de gestion de la virtualisation pris en charge

Le Control Center s'intègre actuellement avec les outils de gestion de virtualisation suivants :

- VMware vCenter Server
- Citrix XenServer
- Nutanix Prism Element

Pour paramétrer l'intégration, vous devez indiquer le nom d'utilisateur et le mot de passe d'un administrateur.

4.3.6. Security Server

Security Server est une machine virtuelle préconfigurée s'exécutant sur une distribution Unbuntu Server avec les versions suivantes :

- 16.04 (VMware NSX et multiplateforme)
- 12.04 LTS (VMware vShield)

Mémoire et processeur

L'allocation de ressources mémoire et processeur au Security Serverdépend du nombre et du type de VM en cours d'exécution sur l'hôte. Le tableau suivant dresse la liste des ressources recommandées à allouer :

Nombre de VM protégées	RAM	Processeurs
1-50 VM	2 Go	2 processeurs
51-100 VM	2 Go	4 processeurs
101-200 VM	4 Go	6 processeurs

Security Server pour NSX est livré avec une configuration prédéfinie du matériel (CPU et RAM), que vous pouvez régler dans VMware vSphere Client Web en éteignant la machine, modifiant ses paramètres, puis rallumer. Pour plus d'informations, reportez-vous à « Installation de Security Server sur VMware NSX » (p. 117).

Espace disque

Environnement	Allocation de l'espace disque
VMware NSX-V / NSX-T	40 Go
VMware avec vShield Endpoint	40 Go
Autre	16 Go

Distribution de Security Server sur les hôtes

Environnement	Security Server vs. hôtes
VMware NSX-V / NSX-T	Security Server s'installe automatiquement sur chaque hôte ESXi dans le cluster pour être protégé, au moment du déploiement de service de Bitdefender.
VMware avec vShield Endpoint	Security Server doit être installé sur chaque hôte ESXi à protéger.
Autre	Bien que ce ne soit pas obligatoire, Bitdefender recommande d'installer le Security Server sur chaque hôte physique pour de meilleures performances.

Latence du réseau

La latence de communication entre Security Server et les endpoints protégés doit être inférieure à 50 ms.

Charge de Storage Protection

L'impact de la Protection de stockage sur Security Server pour l'analyse de 20 Go est le suivant :

État de Storage Protection	Ressources du Security Server	Charge du Security Server	Durée du transfert (mm:ss)
Désactivé (valeur de référence)	N/A	N/A	10:10
Activé	4 vCPU 4 Go de RAM	Normal	10:30
Activé	2 vCPU 2 Go de RAM	Lourde	11:23

Note
Ces résultats sont obtenus avec une variété de fichiers (.exe, .txt, .doc, .eml, .pdf, .zip, etc.) dont la taille est comprise entre 10 Ko et 200 Mo. La durée indiquée est celle du transfert de 20 Go de données contenues dans 46 500 fichiers.

4.3.7. Utilisation du trafic

- **Trafic des mises à jour produit entre les endpoints clients et le serveur de mise à jour**

  Chaque mise à jour produit Bitdefender Endpoint Security Tools périodique génère le trafic téléchargement suivant sur chaque endpoint client :

  - Sous Windows : ~20 Mo
  - Sous Linux : ~26 Mo
  - Sur macOS : ~25 Mo

- **Trafic des mises à jour du contenu de sécurité téléchargé entre les endpoints clients et le serveur de mise à jour (Mo/j)**

Type de serveur de mise à jour	Type de moteur d'analyse		
	Local	Hybride	Central.
Relais	65	58	55
Serveur public de mise à jour Bitdefender	3	3.5	3

- **Le trafic Analyse centrale entre client endpoint et Security Server**

Objets analysés	Type de trafic		Téléchargement (Mo)	Upload (Mo)
Fichiers*	Première analyse		27	841
	Analyse en cache		13	382
Sites Web**	Première analyse	Trafic Web	621	N/A
		Security Server	54	1050
	Analyse en cache	Trafic Web	654	N/A
		Security Server	0.2	0.5

* Les données proposées ont été mesurées pour 3.49 GB des fichiers (6,658 fichiers), dont 1.16 GB sont des fichiers Portable Executable (PE).

** Les données proposées ont été mesurées pour les 500 sites web les mieux notés.

- **Le trafic Analyse hybride entre le client endpoint et les services Cloud Bitdefender**

Objets analysés	Type de trafic	Téléchargement (Mo)	Upload (Mo)
Fichiers*	Première analyse	1.7	0.6
	Analyse en cache	0.6	0.3
Trafic Web**	Trafic Web	650	N/A
	Services Cloud Bitdefender	2.6	2.7

  * Les données proposées ont été mesurées pour 3.49 GB des fichiers (6,658 fichiers), dont 1.16 GB sont des fichiers Portable Executable (PE).

  ** Les données proposées ont été mesurées pour les 500 sites web les mieux notés.

- **Le trafic entre les clients Bitdefender Endpoint Security Tools Relay et le serveur de mise à jour pour le téléchargement du contenu de sécurité**

  Les clients avec un rôle Bitdefender Endpoint Security Tools Relay téléchargent ~16 MB / jour* à partir du serveur mise à jour.

  * Disponible avec les clients Bitdefender Endpoint Security Tools à partir de la version 6.2.3.569.

- **Le trafic entre les clients endpoint et la web console Control Center**

  Un trafic moyen de 618 KB / jour est généré entre les clients endpoint et la web console Control Center.

4.4. Protection Exchange

Security for Exchange est délivé via Bitdefender Endpoint Security Tools, qui peut protéger à la fois le système de fichiers et le serveur de messagerie Microsoft Exchange.

4.4.1. Environnements Microsoft Exchange pris en charge

Security for Exchange est compatible avec les versions et rôles Microsoft Exchange suivants :

- Exchange Server 2019 avec le rôle de Transport Edge ou le rôle Boîte aux lettres
- Exchange Server 2016 avec le rôle de Transport Edge ou le rôle Boîte aux lettres

- Exchange Server 2013 avec le rôle de Transport Edge ou le rôle Boîte aux lettres
- Exchange Server 2010 avec le rôle de Transport Edge, de Transport Hub ou Boîte aux lettres
- Exchange Server 2007 avec le rôle de Transport Edge, de Transport Hub ou Boîte aux lettres

Security for Exchange est compatible avec les Groupes de disponibilité de la base de données Microsoft Exchange (DAG).

4.4.2. Configuration requise

Security for Exchange est compatible avec tout serveur 64 bits physique ou virtuel (Intel ou AMD) ayant une version et un rôle de Serveur Exchange de Microsoft pris en charge. Pour des informations concernant la configuration système requise de Bitdefender Endpoint Security Tools, reportez-vous à « Agent de sécurité sans rôle » (p. 22).

Ressources serveur disponibles recommandées :

- Mémoire RAM disponible : 1 Go
- Espace disponible sur le disque dur : 1 Go

4.4.3. Autres prérequis logiciels

- Pour Microsoft Exchange Server 2013 avec Service Pack 1 : KB2938053 de Microsoft.
- Pour Microsoft Exchange Server 2007 : .NET Framework 3.5 Service Pack 1 ou version supérieure

4.5. Sandbox Analyzer On-Premises

Sandbox Analyzer On-Premises a les prérequis suivants :

- ESXi Hypervisor (la plateforme de virtualisation qui exécutera l'environnement).
- Appliance virtuelle Sandbox Analyzer (l'appliance d'administration qui contrôlera les machines virtuelles de détonation).
- Appliance virtuelle de sécurité du réseau (une VM intégrant un capteur réseau capable d'extraire une charge active du trafic réseau).

- Connectivité à une Control Center GravityZone utilisée pour l'administration de haut niveau de l'environnement sandbox.
- Connexion Internet pour le téléchargement de l'appliance virtuelle Sandbox Analyzer, avec une bande passante d'au moins 5 Mbit/s.

> **Important**
> Assurez-vous qu'aucune autre application ou aucun autre processus ne peut bloquer la connexion Internet pendant le téléchargement et l'installation de Sandbox Analyzer.

4.5.1. Hyperviseur ESXi

L'appliance virtuelle Sandbox Analyzer est disponible au format OVA, et peut être déployée sur un seul hôte physique sous hyperviseur VMware ESXi (version 6.5 ou 6.7).

Configuration matérielle requise pour l'hôte physique

- Processeur : le nombre total de cœurs (avec hyperthreading) peut être déduit grâce au calcul présenté dans la section « Prérequis de l'hôte physique et évolutivité matérielle » (p. 44).
- Mémoire vive : la quantité totale de mémoire vive nécessaire pour l'hôte physique peut être déduite grâce au calcul présenté dans la section « Prérequis de l'hôte physique et évolutivité matérielle » (p. 44).
- Espace disque : au moins 1 To de stockage SSD (pour 8 VM de détonation, évolutif avec au moins 50 Go pour chaque VM supplémentaire).
- Réseau : une carte réseau dédiée.

  Cette carte réseau peut être séparée en deux cartes virtuelles, avec les mappings suivants :

  – Une carte réseau pour l'interface d'administration.

  – Une carte réseau pour le réseau de détonation.

> **Note**
> Il est recommandé d'utiliser des cartes réseau physiques dédiées avec les mêmes mappages que les cartes réseau virtuelles susmentionnées si la configuration matérielle le permet.

Logiciels

Versions prises en charge du serveur ESXi : 6.5 ou supérieure, VMFS version 5.

Configuration supplémentaire sur l'hôte ESXi :

- SSH activé au démarrage.
- Service NTP configuré et actif.
- L'option **start/stop with host** est activée.

Note
Sandbox Analyzer est compatible avec la version d'évaluation de VMWare ESXi. Néanmoins pour les déploiements en production, il est recommandé d'utiliser une version d'ESXi sous licence.

4.5.2. Appliance virtuelle Sandbox Analyzer

L'appliance virtuelle de Sandbox Analyzer assure une évolutivité théoriquement illimitée, tant que les ressources matérielles nécessaires sont disponibles.

Sur la quantité totale de ressources disponibles pour ESXi, Sandbox Analyzer partage les ressources du processeur et de la RAM entre Sandbox Manager et les machines virtuelles de détonation.

Configuration système minimale pour Sandbox Manager

- 6 vCPU
- 20 Go de RAM
- 600 Go d'espace disque

Sandbox Manager compte trois cartes réseau virtuelles internes affectées comme suit :

- Une carte réseau pour la communication avec la console de gestion (GravityZone Control Center).
- Une carte réseau pour la connectivité à Internet.
- Une carte réseau pour la communication avec la VM de détonation.

Note
Pour permettre la communication, la carte réseau virtuelle de gestion ESXi et la carte réseau virtuelle de gestion de Sandbox Manager doivent être sur le même réseau.

Machines virtuelles de détonation

Configuration requise

- 4 vCPUs (surprovisionnement selon un rapport 4:1, voir « Prérequis de l'hôte physique et évolutivité matérielle » (p. 44))
- 3 Go de RAM
- 50 Go d'espace disque

Sandbox Analyzer On-Premises prend en charge les images personnalisées de machine virtuelle. Il est ainsi possible de détoner les échantillons dans un environnement d'exécution qui correspond à l'environnement de production réel.

La création d'une image de machine virtuelle nécessite les éléments suivants :

- L'image de machine virtuelle est au format VMDK, version 5.0.
- Systèmes d'exploitation pris en charge pour la création de machines virtuelles de détonation :
  - Windows 7 64 bits (tous niveaux de correctifs)
  - Windows 10 64 bits (tous niveaux de correctifs)

Important

- Le système d'exploitation doit être installé sur la seconde partition de la table de partitionnement et monté sur le lecteur C: (configuration par défaut pour l'installation de Windows).
- Le compte « Administrateur » local doit être activé et la chaîne de caractères de son mot de passe doit être vide (mot de passe désactivé).
- Avant d'exporter l'image VM, vous devez appliquer la licence du système d'exploitation et de tous les logiciels installés sur l'image de la machine virtuelle.

Logiciel d'image de machine virtuelle

Sandbox Analyzer prend en charge la détonation d'un grand nombre de formats et de types de fichiers. Pour plus d'informations, veuillez consulter « Objets de Sandbox Analyzer » (p. 206)

Pour que les rapports soient probants, vérifiez que vous avez installé sur l'image un logiciel pouvant ouvrir le type de fichier que vous voulez détoner. Pour plus d'informations, veuillez consulter « Applications recommandées pour les VM de détonation » (p. 207)

4.5.3. Appliance virtuelle de sécurité du réseau

Network Security Virtual Appliance utilise le capteur réseau, qui extrait les charges actives des flux réseau et les envoie à Sandbox Analyzer. La configuration matérielle minimum est la suivante :

- 4 vCPU
- 4 Go de RAM
- 1 To d'espace disque
- 2 vNICs

4.5.4. Prérequis de l'hôte physique et évolutivité matérielle

L'algorithme d'évolutivité de l'environnement de Sandbox Analyzer s'appuie sur la formule suivante, où « K » est égal au nombre de créneaux de détection (ou VM de détonation) :

- Sandbox Analyzer VA vCPU = 6 vCPUs + K x 1vCPU
- Mémoire vive VA Sandbox Analyzer = 20 Go mémoire vive + K x 2 Go

De même, l'algorithme d'évolutivité pour l'hôte est le suivant :

- ESXi Host vCPU = 6 vCPUs + K x 2 vCPU
- Mémoire vive hôte ESXi = 20 Go mémoire vive + K x 5 Go

La principale différence entre la VA Sandbox Analyzer et les ressources ESXi tient aux ressources allouées à chaque VM de détonation.

Ainsi, un environnement de détonation standard (8 VM) aura les prérequis suivants :

- Sandbox Analyzer VA vCPU = 6 vCPUs + 8 x 1vCPU = 14 vCPUs
- Mémoire vive VA Sandbox Analyzer = 20 Go mémoire vive + 8 x 2 Go = 36 Go de mémoire vive
- ESXi Host vCPU = 6 vCPUs + 8 x 2 vCPUs = 22 vCPUs

> **Note**
> Chaque VM de détonation a besoin d'un vCPU alloué à la VA Sandbox Analyzer et d'un vCPU pour la VM de détonation. Les VM de détonation seront provisionnées de 4 vCPU, mais surprovisionnées selon un rapport 4:1, donc un seul vCPU sera nécessaire pour l'hôte ESXi.

- Mémoire vive hôte ESXi = 20 Go mémoire vive + 8 x 5 Go = 60 Go de mémoire vive

> **Note**
> La mémoire vive est utilisée selon un rapport 1:1 entre la VA Sandbox Analyzer, les VM de détonation et l'hôte ESXi. Chaque VM de détonation aura donc besoin de 5 Go de mémoire vive de l'hôte ESXi, sur lesquelles 2 Go seront alloués à la VA Sandbox Analyzer et 3 Go seront alloués à la VM de détonation elle-même.

L'hôte physique en résultant nécessite, dans le scénario susmentionné, au moins 22 cœurs de processeur (avec hyperthreading), et au moins 60 Go de mémoire vive, avec 10-20 % de mémoire vive supplémentaire réservée pour l'hyperviseur.

Habituellement, la détonation d'un échantillon prend neuf minutes et génère un rapport de détonation. Elle utilise toutes les ressources provisionnées. Il est conseillé de concevoir votre environnement sandbox en commençant par les capacités de détonation (fichiers/heure), puis de transformer cette métrique en ressources nécessaires au niveau de l'hôte et des VM.

4.5.5. Prérequis de communication de Sandbox Analyzer

Les composants de Sandbox Analyzer On-Premises utilisent certains ports de communication liés à des interfaces réseau spécifiques pour communiquer entre eux et/ou avec les serveurs publics de Bitdefender.

L'environnement sandbox nécessite trois interfaces réseau :

- **eth0 – Interface du réseau géré**. Il se connecte à GravityZone et à l'hôte ESXi.

  Il est recommandé de connecter eth0 au même réseau que l'interface d'administration d'ESXi. Il est également recommandé de le mapper à un adaptateur physique dédié.

  Le tableau suivant présente les prérequis de communication réseau pour eth0 :

Direction	Ports de communication (sur TCP).	Source / Destination
Sortant	8443	Serveur de communication GravityZone
	443	Appliance virtuelle GravityZone
	80	Appliance virtuelle GravityZone

Direction	Ports de communication (sur TCP).	Source / Destination
	22	hôte ESXi
	443	API de l'hôte ESXi
Entrant	8443	Tous

- **eth1 – Réseau de détonation**. Il ne nécessite aucune configuration. La procédure d'installation crée les ressources virtuelles nécessaires.
- **eth2 – Réseau d'accès à Internet**. Il est recommandé d'avoir un accès non restreint et non filtré à Internet.

  Il est recommandé d'assigner le réseau d'administration et le réseau d'accès à Internet à deux sous-réseaux différents.

L'appliance virtuelle de GravityZone doit pouvoir accéder à l'appliance virtuelle de Sandbox Analyzer sur le port 443 (TCP) pour consulter et télécharger les rapports de Sandbox Analyzer.

L'appliance virtuelle de GravityZone doit pouvoir se connecter à l'appliance virtuelle de Sandbox Analyzer sur le port 443 (TCP) pour demander l'état des échantillons détonés.

4.6. Chiffrement complet du disque

Le module de chiffrement complet du disque de GravityZone vous permet d'utiliser BitLocker sur les endpoints Windows, ainsi que FileVault et l'utilitaire de ligne de commande diskutil sur les endpoints macOS via Control Center.

Pour une protection garantie de vos données ce module assure le chiffrement complet, pour les volumes de démarrage et les autres, sur des disques durs fixes ; et conserve les clés de récupération au cas où les utilisateurs oublient leurs mots de passe.

Le module de Chiffrement utilise les ressources matérielles de votre environnement GravityZone.

En ce qui concerne le logiciel, la configuration requise est presque la même que pour BitLocker, FileVault et l'utilitaire de ligne de commande diskutil, et la plupart des restrictions sont liées à ces outils.

Sous Windows

Le module de chiffrement de GravityZone est compatible avec BitLocker à partir de la version 1.2, sur les machines équipées ou non d'une puce (Trusted Platform Module).

GravityZone prend en charge BitLocker sur des postes fonctionnant avec les systèmes d'exploitation suivants :

- Windows 10 Education
- Windows 10 Enterprise
- Windows 10 Pro
- Windows 8.1 Enterprise
- Windows 8.1 Pro
- Windows 8 Enterprise
- Windows 8 Pro
- Windows 7 Ultimate (avec TPM)
- Windows 7 Enterprise (avec TPM)
- Windows Server 2019*
- Windows Server 2016*
- Windows Server 2012 R2*
- Windows Server 2012*
- Windows Server 2008 R2* (avec TPM)

*BitLocker n'est pas intégré à ces systèmes d'exploitation et doit être installé séparément. Pour plus d'informations sur le déploiement de Bitlocker sur Windows Server, consultez ces articles sur la Base de connaissances Microsoft :

- https://technet.microsoft.com/en-us/itpro/bitlocker-how-to-deploy-on-windows-server
- https://technet.microsoft.com/en-us/library/cc732725(v=ws.10).aspx

Important
GravityZonene prend pas en charge le chiffrement sur Windows 7 et Windows 2008 R2 sans TPM.

Pour plus de détails sur la configuration requise pour BitLocker, consultez cet article sur la Base de connaissances Microsoft : https://technet.microsoft.com/en-us/library/cc766200(v=ws.10).aspx

Sous Mac

GravityZone prend en charge FileVault et diskutil sur des postes macOS fonctionnant avec les systèmes d'exploitation suivants :

- macOS Big Sur (11.0)
- macOS Catalina (10.15)
- macOS Mojave (10.14)
- macOS High Sierra (10.13)
- macOS Sierra (10.12)
- OS X El Capitan (10.11)

4.7. Protection de stockage

Solutions de stockage et de partage de fichiers prises en charge :

- Serveurs de stockage en réseau (NAS) et sous-réseaux de stockage compatibles avec le protocole ICAP, fournis par Dell®, EMC®, IBM®, Hitachi®, HPE® et Oracle®, entre autres.
- Nutanix® Files 3.x jusqu'à 3.6.2
- Citrix® ShareFile

4.8. Protection Mobile

4.8.1. Plateformes supportées

Security for Mobile supporte les types d'appareils mobiles et de systèmes d'exploitation suivants :

- Apple iPhone et iPad (iOS 8.1+)
- Smartphones et tablettes Google Android (4.2+)

4.8.2. Besoins en connectivité

Les appareils mobiles doivent disposer d'une connexion Wifi ou aux données du l'appareil active et d'une connectivité au serveur de communication.

4.8.3. Notifications Push

Security for Mobile utilise des notifications Push pour prévenir les clients d'appareils mobiles lorsque des mises à jour de politiques et des tâches sont disponibles. Les notifications Push sont envoyées par le Serveur de Communication via le service fourni par le fabricant du système d'exploitation :

- Service Firebase Cloud Messaging (FCM) pour appareils Android. Pour que FCM fonctionne, les conditions suivantes doivent être remplies :
  - Google Play Store doit être installé.
  - Appareils sous Android 4.2 ou version supérieure.
  - Pour envoyer des notifications push, un certain nombre de ports doivent être ouverts.
- Service de Notification Push d'Apple (APN) pour appareils iOS. Pour plus d'informations, veuillez consulter cet article KB Apple.

Vous pouvez vérifier que les notifications push mobiles fonctionnent correctement dans la rubrique **Vérification des notifications push mobiles** dans **Configuration > Divers**.

Pour plus d'informations sur le workflow de la gestion des appareils mobiles GravityZone, veuillez vous référer à cet article KB.

4.8.4. Certificats d'administration iOS

Pour configurer l'infrastructure de l'administration des appareils mobiles iOS, vous devez fournir des certificats de sécurité.

Pour plus d'informations, reportez-vous à « Certificats » (p. 92).

4.9. Ports de communication de GravityZone

GravityZone est une solution distribuée, ce qui signifie que ses composants communiquent entre eux via le réseau local ou Internet. Chaque composant utilise un ensemble de ports pour communiquer avec les autres. Vous devez veiller à ce que les ports nécessaires à GravityZone soient ouverts.

Pour des informations détaillées au sujet des ports de GravityZone, veuillez vous référer à cet article KB.

5. INSTALLATION DE LA PROTECTION

GravityZone est une solution client-serveur. Pour protéger votre réseau avec Bitdefender, vous devez déployer les rôles de serveur GravityZone, enregistrer votre licence, configurer les packages d'installation et les déployer sur les endpoints via les agents de sécurité. Certaines couches de protection nécessitent des composants supplémentaires pour être installées et configurées.

5.1. Installation et configuration de GravityZone

Pour vous assurer que l'installation se déroule sans problème, procédez comme suit :

1. Préparer l'installation
2. Déployer et configurer GravityZone
3. Connectez-vous à Control Center et configurez le premier compte utilisateur
4. Configurer les paramètres de Control Center

5.1.1. Préparer l'installation

Pour l'installation, vous avez besoin de l'image d'une appliance virtuelle GravityZone. Une fois que vous avez déployé et configuré l'appliance GravityZone, vous pouvez installer le client ou télécharger à distance les packages d'installation nécessaires à partir de l'interface Web de Control Center.

L'image de l'appliance GravityZone est disponible dans plusieurs formats, compatibles avec les principales plateformes de virtualisation. Vous pouvez obtenir les liens de téléchargement en vous inscrivant pour une version d'évaluation sur le site web de Bitdefender.

Pour l'installation et la configuration initiale, vous devez disposer des éléments suivants :

- Les noms DNS ou les adresses IP fixes (par configuration statique ou via une réservation DHCP) des appliances GravityZone.
- Le nom d'utilisateur et le mot de passe d'un administrateur du domaine
- Les informations vCenter Server, vShield Manager, XenServer (nom d'hôte ou adresse IP, port de communication, nom d'utilisateur et mot de passe de l'administrateur)

- Les clés de licence (reportez-vous à l'e-mail d'enregistrement de la version d'évaluation ou de l'achat)
- Les paramètres du serveur de messagerie pour courrier sortant
- Si besoin, les paramètres du serveur proxy
- Certificats de sécurité

5.1.2. Déployer GravityZone

Un déploiement GravityZone consiste en une ou plusieurs appliances ayant le rôle de serveur. La quantité d'appliances dépend de plusieurs critères, tels que la taille et la conception de votre infrastructure réseau, ou les fonctionnalités de GravityZone que vous utiliserez. Les rôles de serveur sont de trois types : basique, auxiliaire et optionnel.

Important
Les rôles auxiliaires et optionnels ne sont disponibles que pour certaines solutions GravityZone.

Rôle GravityZone	Type de rôle	Installer
Serveur de base de données Update Server Console Web Serveur de communication	Basique (nécessaire)	Au moins une instance de chaque rôle. Une appliance GravityZone peut avoir un, plusieurs ou tous ces rôles.
	Auxiliaire	Une appliance pour chaque rôle
Security Server	Optionnel	Recommandé uniquement pour les petits réseaux ou en cas de ressources limitées. Sinon, déployez un Security Server indépendant depuis la Control Center, une fois le déploiement de GravityZone terminé.

Selon la façon dont vous répartissez les rôles de GravityZone, vous déploierez une appliances GravityZone ou plus. Le rôle Serveur base de données est le premier à installer.

Dans un scénario avec plusieurs appliances de GravityZone, vous installerez le rôle du Serveur de base de données sur la première appliance et configurerez toutes les autres appliances pour se connecter à l'instance de la base de données existante.

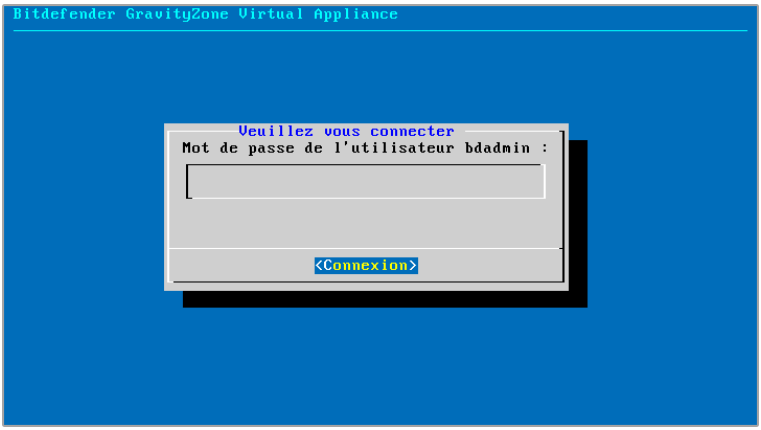
Vous pouvez déployer plus d'instances des rôles Serveur de base de données, Console web, et Serveur de communication . En ce cas, vous utiliserez Replica Set pour le Serveur de base de données et des équilibreurs de charge pour la Console web et le Serveur de communication sur les appliances GravityZone.

Pour déployer et configurer GravityZone :

1. Téléchargez l'image de l'appliance virtuelle de GravityZone sur le site web de Bitdefender (le lien est indiqué dans l'e-mail reçu lors de l'inscription ou de l'achat).
2. Importez l'image de l'appliance virtuelle GravityZone dans votre environnement virtualisé.
3. Allumez l'appliance.
4. Depuis l'outil de gestion de la virtualisation, accédez à l'interface de la console de l'appliance GravityZone.
5. Configurez le mot de passe de `bdadmin`, l'administrateur système intégré.

Interface de la console de l'appliance : saisissez un nouveau mot de passe (attention il sera saisi en mode QWERTY)

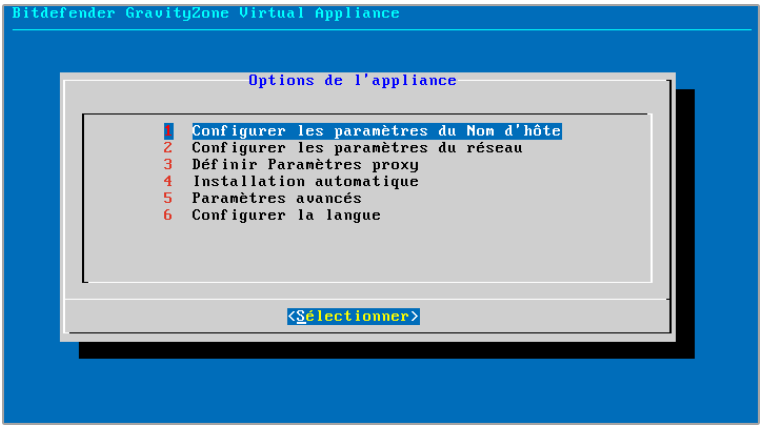
6. Connectez-vous avec le mot de passe que vous venez de définir.



Interface de la console de l'appliance : connexion

Vous accéderez à l'interface de configuration de l'appliance.

Utilisez les flèches et la touche `Tab` pour vous déplacer dans les menus et les options. Appuyez sur `Entrée` pour sélectionner une option spécifique.



Interface de la console de l'appliance : menu principal

7. Si vous devez changer la langue de l'interface, sélectionnez l'option **Configurer la langue**. Pour en apprendre plus sur la configuration, consultez « Configurer la langue » (p. 61).
8. Configurer le nom d'hôte de l'appliance.
9. Configurez les paramètres du réseau.
10. Configurer les paramètres du proxy (si nécessaire)
11. Installer les rôles serveur de GravityZone. Vous avez deux options :
    - Installation automatique. Sélectionnez cette option si vous devez uniquement déployer une instance de GravityZone sur votre réseau.
    - Paramètres avancés . Sélectionnez cette option si vous devez déployer GravityZone manuellement ou sur une architecture distribuée.

Après avoir déployé et configuré l'appliance GravityZone, vous pouvez modifier les paramètres de l'appliance à tout moment à l'aide de l'interface de configuration. Pour plus d'informations sur la configuration de l'appliance GravityZone, reportez-vous à « Gérer l'appliance GravityZone » (p. 99).

Configurer les paramètres du Nom d'hôte

La communication avec les rôles GravityZone s'effectue à l'aide de l'adresse IP ou du nom DNS de l'appliance sur laquelle ils sont installés. Par défaut, les composants de GravityZone communiquent en utilisant les adresses IP. Si vous souhaitez activer la communication via des noms DNS, vous devez configurer les appliances GravityZone avec un nom DNS et vérifier que la résolution vers l'adresse IP configurée de l'appliance est correcte.

Prérequis :

- Configurez l'enregistrement DNS dans le serveur DNS.
- Le nom DNS doit effectuer correctement la résolution vers l'adresse IP configurée de l'appliance. Vous devez donc vous assurer que l'appliance est configurée avec l'adresse IP correcte.

Pour configurer les paramètres du Nom d'hôte :

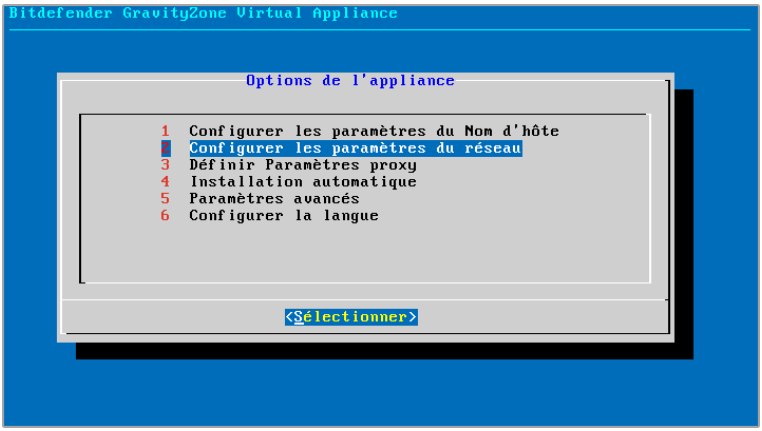
1. Dans le menu principal, sélectionnez **Configurer les paramètres Nom d'hôte**.
2. Saisissez le Nom d'hôte de l'appliance et le nom de domaine de l'Active Directory (si nécessaire).

3. Sélectionnez **OK** pour enregistrer les modifications.

Configurer les paramètres du réseau

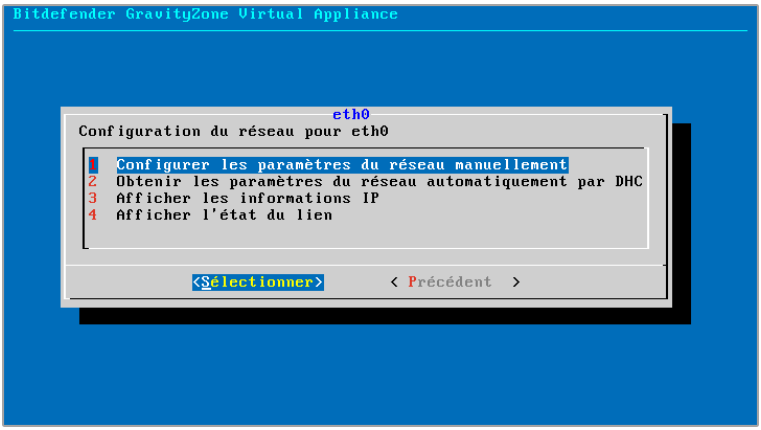
Vous pouvez configurer l'appliance afin qu'elle obtienne automatiquement les paramètres du réseau à partir du serveur DHCP ou vous pouvez configurer manuellement les paramètres du réseau. Si vous choisissez d'utiliser DHCP, vous devez configurer le serveur DHCP afin qu'il réserve une adresse IP spécifique à l'appliance.

1. Dans le menu principal, sélectionnez **Configurer les paramètres réseau**.



Interface de la console de l'appliance : option des paramètres du réseau

2. Sélectionnez l'interface réseau.
3. Sélectionnez la méthode de configuration :
   - **Configurer les paramètres du réseau manuellement.** Vous devez indiquer l'adresse IP, le masque de réseau, l'adresse de la passerelle et les adresses du serveur DNS.
   - **Obtenir les paramètres du réseau automatiquement par DHCP.** Utilisez cette option uniquement si vous avez configuré le serveur DHCP afin qu'il réserve une adresse IP spécifique à l'appliance.



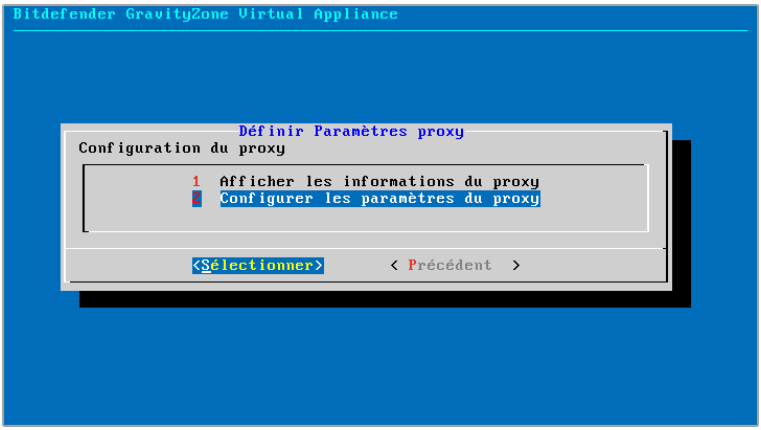
Interface de la console de l'appliance : configuration du réseau

4. Vous pouvez consulter les détails de la configuration IP actuelle ou l'état du lien en sélectionnant les options correspondantes.

Définir les paramètres de proxy

Si vous voulez que l'appliance se connecte à Internet via un serveur proxy, vous devez configurer les paramètres du proxy.

1. Dans le menu principal, sélectionnez **Configurer les paramètres du proxy**.
2. Sélectionnez **Afficher les informations du proxy** pour vérifier si le proxy est activé.
3. Cliquez sur **OK** pour revenir à l'écran précédent.
4. Sélectionnez de nouveau **Définir paramètres proxy**.



Interface de la console de l'appliance : configurer les paramètres du proxy

5. Saisissez l'adresse du serveur proxy. Utilisez la syntaxe suivante :
   - Si le serveur proxy ne requiert pas d'authentification :

     `http(s)://<IP/nom d'hôte>:<port>`
   - Si le serveur proxy requiert une authentification :

     `http(s)://<nom d'utilisateur>:<mot de passe>@<IP/nom d'hôte>:<port>`
6. Sélectionnez **OK** pour enregistrer les modifications.

Installation automatique

Pendant l'installation automatique, tous les rôles de base s'installent sur la même appliance. Pour procéder à un déploiement distribué de GravityZone, consultez « Paramètres avancés » (p. 59).

Important
Le déploiement automatique installera également le Security Server, embarqué dans l'appliance GravityZone. Pour plus d'informations sur Security Server, consultez « L'architecture de GravityZone » (p. 9).
L'option permettant d'installer les rôles automatiquement n'est disponible que lors de l'installation initiale de GravityZone.

Pour installer les rôles automatiquement :

1. Dans le menu principal, sélectionnez **Installation automatique**.
2. Lire et accepter le contrat de licence utilisateur final (CLUF) pour continuer.
3. Confirmez les rôles à installer.
4. Saisissez le mot de passe du Serveur de base de données.

   Le mot de passe peut contenir n'importe quelle combinaison de caractères ASCII_et doit faire entre 6 et 32 caractères de longueur, dont au moins_un chiffre, une majuscule, une minuscule et un caractère spécial.

Interface de la console de l'appliance : configurez mot de passe base de données

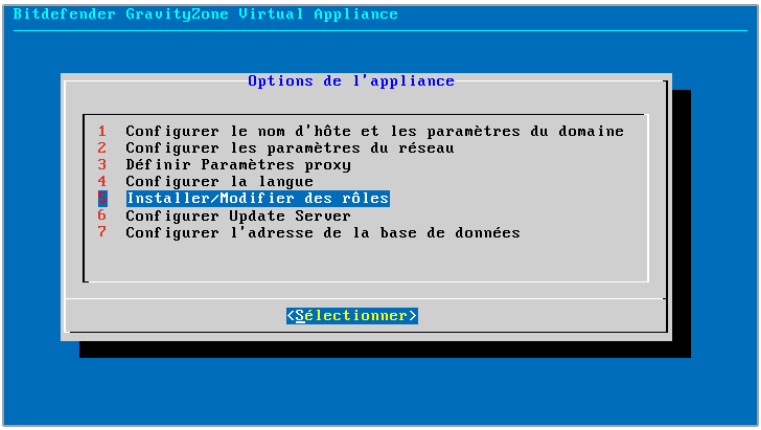
5. Patientez jusqu'à ce que le processus d'installation soit terminé.

Paramètres avancés

Utilisez cette option pour n'installer qu'une partie, ou l'ensemble, des rôles de GravityZone, individuellement ou pour étendre votre infrastructure GravityZone. Vous pouvez installer les rôles sur une ou plusieurs appliances. La méthode d'installation est nécessaire pour les mises à jour par phase ou dans les architectures GravityZone distribuées pour faire évoluer GravityZone pour les grands réseaux et assurer la disponibilité des services GravityZone.

Pour installer les rôles individuellement :

1. Dans le menu principal, sélectionnez **Paramètres avancés**.



Interface de la console de l'appliance : installer les rôles

2. Sélectionnez **Installer/Désinstaller Rôles** pour installer l'appliance dans un environnement GravityZone avec un seul serveur base de données.

   Note
   Les autres options permettent d'étendre le déploiement de GravityZone sur une architecture distribuée. Pour plus d'informations, reportez-vous à « Se connecter à une base de données existante » (p. 111) ou à « Se connecter à la Base de données existante (Cluster de VPN sécurisés) » (p. 112).

3. Sélectionnez **Ajouter ou supprimer des rôles**. Une message de confirmation s'affichera.
4. Appuyez sur `Entrée` pour poursuivre.
5. Appuyez sur la `Barre d'espace` puis sur la touche `Entrée` pour installer le rôle Serveur de base de données. Vous devez confirmer votre choix en appuyant à nouveau sur `Entrée`.
6. Configurer un mot de passe pour la base de données

   Le mot de passe peut contenir n'importe quelle combinaison de caractères ASCII_et doit faire entre 6 et 32 caractères de longueur, dont au moins_un chiffre, une majuscule, une minuscule et un caractère spécial.
7. Appuyez sur `Entrée` et attendez que l'installation soit terminée.

8. Installez les autres rôles en choisissant **Ajouter ou supprimer des rôles** dans le menu **Installer/Désinstaller Rôles** puis les rôles à installer.
   a. Choisissez **Ajouter ou supprimer des rôles** dans le menu **Installer/Désinstaller des rôles**.
   b. Lire l'accord de licence de l'utilisateur final. Appuyez sur `Entrée` pour accepter et continuer.

      Note
      Cette étape ne doit être réalisée qu'une seule fois, après avoir installé le Serveur de base de données.

   c. Sélectionnez les rôles à installer. Appuyez sur la `Barre d'espace` pour sélectionner un rôle et sur `Entrée` pour poursuivre.
   d. Appuyez sur `Entrée` pour confirmer puis attendez que l'installation soit terminée.

Note
Chaque rôle est normalement installé en quelques minutes. Lors de l'installation, les fichiers nécessaires sont téléchargés à partir d'Internet. L'installation prend donc plus de temps si la connexion à Internet est lente. Si l'installation bloque, redéployez l'appliance.

Configurer la langue

Initialement, l'interface de configuration de l'appliance est en anglais.

Pour changer la langue de l'interface :

1. Sélectionnez **Configurer Langue** dans le menu principal.
2. Sélectionnez la langue dans les options disponibles : Une message de confirmation s'affichera.

   Note
   Vous devrez peut être faire dérouler la liste pour voir apparaître votre langue.

3. Sélectionnez **OK** pour enregistrer les modifications.

5.1.3. Configuration initiale du Control Center

Après avoir déployé et configuré l'appliance GravityZone, vous devez accéder à l'interface Web de Control Center et configurer le compte administrateur de votre société.

1. Dans la barre d'adresses de votre navigateur Web, saisissez l'adresse IP ou le nom d'hôte DNS de l'appliance Control Center (en utilisant le préfixe `https://`).

   Un assistant de configuration s'affichera.

2. Indiquez la clé de licence nécessaire pour valider la solution GravityZone que vous avez achetée. Vous pouvez également indiquer toute clé d'extension GravityZone en votre possession.

   Reportez-vous à l'e-mail d'enregistrement de la version d'évaluation ou de l'achat pour connaître vos clés de licence.

   a. Cliquez sur le bouton ⊕**Ajouter** en haut du tableau. Une fenêtre de configuration s'affichera.

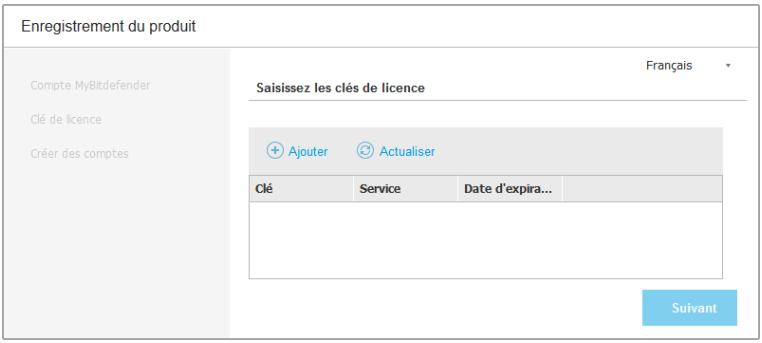
   b. Sélectionnez le type d'enregistrement de la licence (en ligne ou hors connexion)

   c. Saisissez la clé de licence dans le champ **Clé de licence**. Pour l'activation hors connexion, vous devez également indiquer le code d'activation.

   d. Patientez pendant la validation de la clé de licence. Cliquez sur **Ajouter** pour terminer.

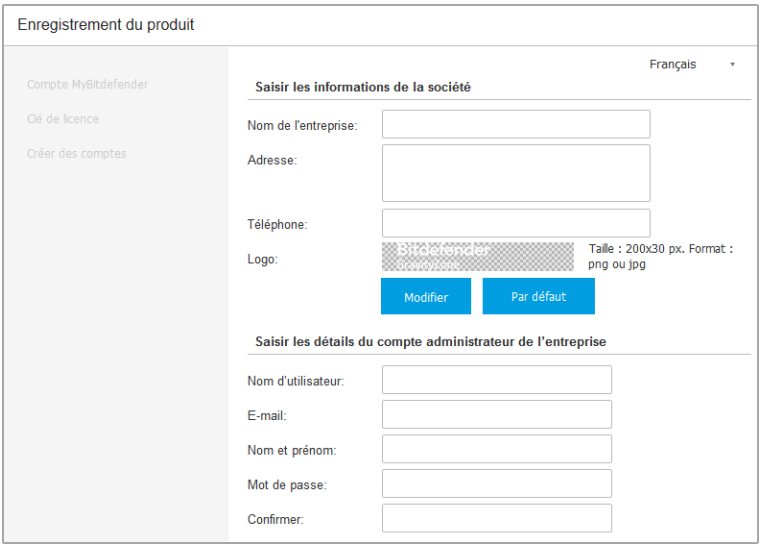
   La clé de licence et sa date d'expiration apparaîtront dans le tableau des licences.

> **Note**
>
> - Pendant la configuration initiale, vous devez indiquer une clé de licence de base valide pour commencer à utiliser GravityZone. Vous pourrez ajouter des clés de licence dans un second temps, ou bien modifier les clés existantes.
> - Vous pouvez utiliser les extensions tant que la licence de base est valide. Sinon, vous pourrez voir les fonctionnalités sans être en mesure de les utiliser.



Configuration initiale - Fournir une clé de licence

3. Cliquez sur **Suivant** pour continuer.
4. Indiquez les données de votre entreprise telles que son nom, adresse et téléphone.
5. Vous pouvez changer le logo apparaissant dans Control Center ainsi que dans les rapports de votre entreprise et les notifications d'e-mail comme suit :
   - Cliquez sur **Modifier** pour rechercher le logo sur votre ordinateur. Le format du fichier de l'image doit être .png ou .jpg et la taille de l'image doit être 200x30 pixels.
   - Cliquez sur **Par défaut** pour supprimer l'image et rétablir l'image fournie par Bitdefender.
6. Spécifiez les informations requises du compte administrateur de votre société : nom d'utilisateur, adresse e-mail et mot de passe. Le mot de passe doit contenir au moins une majuscule, une minuscule et un chiffre ou un caractère spécial.



Configuration initiale - Configurer votre compte

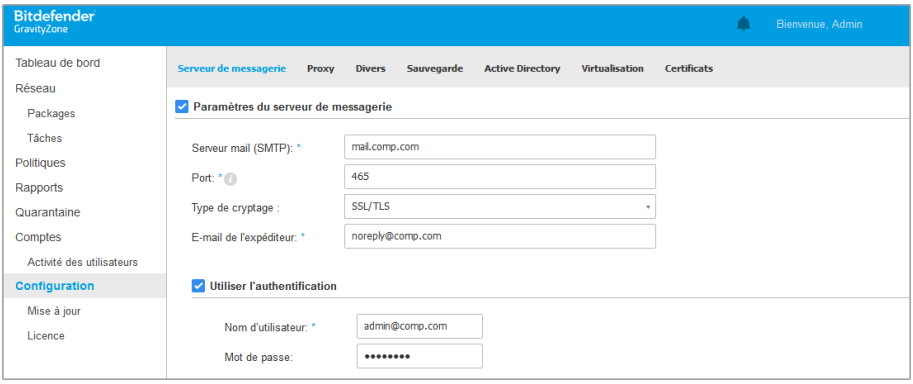
7. Cliquez sur **Créer un compte**.

Le compte administrateur de la société sera créé et vous serez automatiquement connecté avec le nouveau compte à Bitdefender Control Center.

5.1.4. Configurer les paramètres du Control Center

Après la configuration initiale, vous avez besoin de configurer les paramètres de Control Center. En tant qu'administrateur de la société, vous pouvez effectuer les actions suivantes :

- Configurer les paramètres de messagerie, proxy et généraux.
- Exécuter ou planifier la sauvegarde de la base de données du Control Center.
- Configurer l'intégration à Active Directory et aux outils de gestion de la virtualisation (vCenter Server, XenServer).
- Installer des certificats de sécurité.



Les paramètres du serveur de messagerie

Serveur de messagerie

Le Control Center nécessite un serveur de messagerie externe pour envoyer des communications par e-mail.

Note
Nous vous recommandons de créer un compte de messagerie dédié au Control Center.

Pour permettre au Control Center d'envoyer des e-mails :

1. Allez sur la page **Configuration**.
2. Sélectionnez l'onglet **Serveur de messagerie**.
3. Sélectionnez **Paramètres du serveur de messagerie** et configurez les paramètres requis :
   - **Serveur mail (SMTP).** Indiquez l'adresse IP ou le nom d'hôte du serveur de messagerie qui enverra les e-mails.
   - **Port.** Indiquez le port utilisé pour se connecter au serveur de messagerie.
   - **Type de chiffrement.** Si le serveur de messagerie requiert une connexion chiffrée, sélectionnez le type approprié dans le menu (SSL, TLS ou STARTTLS).
   - **E-mail de l'expéditeur.** Saisissez l'adresse e-mail que vous souhaitez voir apparaître dans le champ "De" de l'e-mail (adresse e-mail de l'expéditeur).

- **Utiliser l'authentification.** Cochez cette case si le serveur de messagerie requiert une authentification. Vous devez indiquer un nom d'utilisateur / une adresse e-mail et un mot de passe valides.

4. Cliquez sur **Enregistrer**.

Control Center valide automatiquement les paramètres de messagerie lorsque vous les enregistrez. Si les paramètres indiqués ne peuvent pas être validés, un message d'erreur vous signale le paramètre incorrect. Corrigez la configuration et réessayez.

Proxy

Si votre entreprise se connecte à Internet via un serveur proxy, vous devez configurer les paramètres du proxy:

1. Allez sur la page **Configuration**.
2. Sélectionnez l'onglet **Proxy**.
3. Sélectionnez **Utiliser les paramètres du proxy** et configurez les paramètres requis :
   - **Adresse** - saisissez l'adresse IP du serveur proxy.
   - **Port** - entrez le port utilisé pour se connecter au serveur proxy.
   - **Nom d'utilisateur** - entrez le nom d'utilisateur reconnu par le serveur proxy.
   - **Mot de passe** - saisissez le mot de passe valide de l'utilisateur dont le nom vient d'être indiqué.
4. Cliquez sur **Enregistrer**.

Divers

L'onglet **Divers** de la page **Configuration** vous permet de configurer les préférences générales suivantes :

- **Quand une image du Security Server non disponible est requise.** L'appliance GravityZone ne comprend pas par défaut les images de la machine virtuelle Security Server. Si un administrateur essaie de télécharger une image du Security Server ou d'exécuter une tâche d'installation du Security Server, cette action échouera. Vous pouvez configurer une action automatisée pour cette situation à l'aide de l'une des options suivantes :
  - **Télécharger l'image automatiquement**

- **Avertir l'administrateur et ne pas télécharger**

> **Note**
> Pour éviter d'interférer avec le travail de l'administrateur, vous pouvez télécharger manuellement les packages de Security Server requis à partir de la page **Mise à jour**, onglet **Mise à jour du produit**. Pour plus d'informations, reportez-vous à « Téléchargement des mises à jour de produits » (p. 176).

- **Quand un kit non disponible est nécessaire.** Vous pouvez configurer une action automatisée pour cette situation à l'aide de l'une des options suivantes :
  - **Télécharger le package automatiquement**
  - **Avertir l'administrateur et ne pas télécharger**
- **Déploiements simultanés.** Les administrateurs peuvent déployer à distance des composants de sécurité en exécutant des tâches d'installation. Utilisez cette option pour spécifier le nombre maximal de déploiements simultanés pouvant être réalisés.

  Par exemple, si le nombre maximal de déploiements simultanés est défini à 10 et qu'une tâche d'installation de client à distance est affectée à 100 ordinateurs, le Control Center commencera par envoyer 10 packages d'installation via le réseau. Dans ce cas, l'installation du client s'effectue simultanément sur 10 ordinateurs au maximum, toutes les autres sous-tâches étant en attente. Dès qu'une sous-tâche est effectuée, un autre package d'installation est envoyé et ainsi de suite.
- **Forcer l'authentification à deux facteurs pour tous les comptes.** L'authentification à deux facteurs (2FA) ajoute une couche de sécurité supplémentaire aux comptes GravityZone, en demandant un code d'identification en plus des identifiants Control Center. Cette fonctionnalité nécessite de télécharger et d'installer Google Authenticator, Microsoft Authenticator, ou toute autre application d'authentification TOTP (Time-Based One-Time Password Algorithm) - compatible avec le standard RFC6238 - sur l'appareil mobile de l'utilisateur, de la relier au compte GravityZone, puis de l'utiliser lors de chaque connexion à Control Center. L'application d'authentification génère un code à six chiffres toutes les 30 secondes. Pour se connecter à Control Center, l'utilisateur devra saisir le code d'authentification à six chiffres après avoir saisi son mot de passe.

  L'authentification à deux facteurs est activée par défaut lors de la création d'une entreprise. Après cela, lors de l'identification, une fenêtre de configuration

demandera à l'utilisateur d'activer cette fonctionnalité. Les utilisateurs ne pourront passer l'activation de l'authentification à deux facteurs que trois fois. Lors de la quatrième tentative de connexion, il ne sera plus possible de passer l'identification à deux facteurs et l'utilisateur ne pourra pas s'identifier.

Si vous souhaitez désactiver l'authentification à deux facteurs forcée pour tous les comptes GravityZone, il vous suffit de décocher l'option. Un message de confirmation apparaitra avant que les modifications ne soient appliquées. Une fois cela fait, l'authentification à deux facteurs de tous les utilisateurs sera toujours activée, mais ils pourront la désactiver dans les paramètres de leur compte.

Note

- Vous pouvez voir le statut de l'authentification à deux facteurs d'un compte utilisateur sur la page **Comptes**.
- Si un utilisateur pour lequel l'authentification à deux facteurs est activée ne peut pas se connecter à GravityZone (car il a un nouvel appareil ou a perdu sa clé secrète), vous pouvez réinitialiser son authentification à deux facteurs depuis la page du compte de l'utilisateur, dans la section **Authentification à deux facteurs**. Pour en savoir plus, consultez le chapitre **Comptes utilisateurs > gestion de l'authentification à deux facteurs** du Guide de l'administrateur.

- **Paramètres du serveur NTP**. Le serveur NTP est utilisé pour synchroniser l'heure entre toutes les appliances de GravityZone. Une adresse de serveur NTP par défaut est fournie; vous pouvez la modifier dans le champ **Adresse du serveur NTP**.

  Note
  Pour que les appliances GravityZone communiquent avec le serveur NTP, le port (UDP) 123 doit être ouvert.

- **Activer Syslog**. En activant cette fonctionnalité, vous permettez à GravityZone d'envoyer des notifications à un serveur de journalisation qui utilise le protocole Syslog. Vous pouvez ainsi mieux surveiller les événements de GravityZone.

  Pour afficher ou configurer la liste des notifications envoyées au serveur Syslog, référez-vous au chapitre **Notifications** du Guide de l'Administrateur GravityZone.

  Pour activer la journalisation auprès d'un serveur Syslog distant :

  1. Cochez la case **Activer Syslog**

2. Indiquez le nom ou l'IP du serveur, le protocole de votre choix et le port qu'écoute Syslog.
3. Sélectionnez le format dans lequel les données sont envoyées au serveur Syslog :
   - **Format JSON**. Le JSON est un format léger d'échange de données complètement indépendant de tout langage de programmation. JSON présente les données sous format d'un texte lisible par un humain. Au format JSON, les informations de chaque évènement sont organisées en objets, chaque objet consistant en une paire nom/valeur.

     Par exemple :

     ```
     {
         "name":"Login from new device",
         "created":"YYYY-MM-DDThh:mm:ss+hh:ss",
         "company_name":"companyname",
         "user_name":"username",
         "os":"osname",
         "browser_version":"browserversion",
         "browser_name":"browsername",
         "request_time":"DD MMM YYYY, hh:mm:ss +hh:ss",
         "device_ip":"computerip"
     }
     ```

     Pour en apprendre plus, rendez-vous sur www.json.org/.

     Il s'agit du format par défaut de GravityZone.
   - **Common Event Format (CEF)**. Le CEF est un format ouvert développé par ArcSight qui simplifie la gestion des fichiers journaux.

     Par exemple :

     ```
     CEF:0|Bitdefender|GZ|<GZ version>|NNNNN|Login from new
     device|3|start=MMM DD YYYY hh:mm:ss+hh:mm
     BitdefenderGZCompanyName=companyname suser=username
     BitdefenderGZLoginOS=osname
     BitdefenderGZAuthenticationBrowserName=browsername
     BitdefenderGZAuthenticationBrowserVersion=browserversion
     dvchost=computerip
     ```

Pour en apprendre plus, consultez ArcSight Common Event Format (CEF) Implementation Standard.

Dans le chapitre **Notifications** du Guide de l'administrateur, vous pourrez consulter les types de notification disponibles pour chaque format.

4. Cliquez sur le bouton ⊕ **Ajouter** dans la colonne **Action**.

Cliquez sur **Enregistrer** pour appliquer les modifications.

Sauvegarde

Afin de vous assurer que les données du Control Center sont en sécurité, vous pouvez sauvegarder la base de donnée de GravityZone. Vous pouvez exécuter autant de sauvegardes de bases de données voulues ou planifier des sauvegardes automatiques et périodiques, à des intervalles de temps déterminés.

Toutes les commandes de sauvegarde de base de données créent un fichier `tgz` (fichier archive créé avec Tar et compressé avec GZIP) à l'emplacement spécifié dans les paramètres de la sauvegarde.

Lorsque plusieurs administrateurs disposent de privilèges d'administration sur les paramètres de Control Center, vous pouvez également configurer les **Paramètres des notifications** afin d'être informé de toutes les sauvegardes de bases de données terminées. Pour plus d'informations, consultez le chapitre **Notifications** du Guide de l'administrateur de GravityZone.

Création de sauvegardes de la base de donnée

Pour exécuter une sauvegarde de base de données:

1. Allez sur la page **Configuration** de Control Center et cliquez sur l'onglet **Sauvegarde**.
2. Cliquez sur le bouton **Sauvegarder** en haut du tableau. Une fenêtre de configuration s'affichera.
3. Sélectionnez le type d'emplacement où l'archive de la sauvegarde sera sauvegardé:
   - **Local**, pour enregistrer les archives de sauvegarde sur l'appliance de GravityZone. Dans ce cas, vous devez spécifier le chemin vers le répertoire spécifique de l'appliance GravityZone où l'archive sera enregistrée.

L'appliance GravityZone a une structure de répertoire sous Linux. Par exemple, vous pouvez choisir de créer la sauvegarde sur le répertoire `tmp`. Dans ce cas, entrez `/tmp` dans le champs **chemin d'accès**.

- **FTP**, pour enregistrer l'archive de sauvegarde sur un serveur FTP. Dans ce cas, entrez les accès du FTP dans les champs suivants.
- **Réseau**, pour enregistrer les archives de sauvegarde sur un partage réseau. Dans ce cas, saisissez le chemin vers l'emplacement souhaité sur le réseau (par exemple`\\computer\folder`), le nom de domaine et les identifiants de l'utilisateur du domaine.

4. Cliquez sur le bouton **Tester**. Une notification écrite vous indiquera si les paramètres spécifiés sont ou non valides.

   Pour créer une sauvegarde, tous les paramètres doivent être valides.

5. Cliquez sur **Générer**. La page **Sauvegarde** s'affichera. Une nouvelle entrée de sauvegarde sera ajoutée à la liste. Vérifiez l'**État** de la nouvelle sauvegarde. Une fois la sauvegarde terminée, une archive `tgz` sera disponible à l'emplacement spécifié.

> **Note**
> La liste se trouvant sur la page **Sauvegarde** comprend les journaux de toutes les sauvegardes créées. Ces journaux ne permettent pas d'accéder aux archives de sauvegarde, ils affichent uniquement des informations sur les sauvegardes créées.

Pour planifier une sauvegarde de base de données :

1. Allez sur la page **Configuration** de Control Center et cliquez sur l'onglet **Sauvegarde**.
2. Cliquez sur le bouton **Paramètres sauvegarde** en haut du tableau. Une fenêtre de configuration s'affichera.
3. Sélectionnez **Sauvegarde planifiée**.
4. Configurez la fréquence des sauvegardes (quotidienne, hebdomadaire ou mensuelle) et l'heure de début.

   Vous pouvez par exemple planifier l'exécution hebdomadaire de sauvegardes, tous les vendredis à partir de 22h00.

5. Configurez l'emplacement de la sauvegarde planifiée.

6. Sélectionnez le type d'emplacement où l'archive de la sauvegarde sera sauvegardé:
   - **Local**, pour enregistrer les archives de sauvegarde sur l'appliance de GravityZone. Dans ce cas, vous devez spécifier le chemin vers le répertoire spécifique de l'appliance GravityZone où l'archive sera enregistrée.

     L'appliance GravityZone a une structure de répertoire sous Linux. Par exemple, vous pouvez choisir de créer la sauvegarde sur le répertoire `tmp`. Dans ce cas, entrez `/tmp` dans le champs **chemin d'accès**.
   - **FTP**, pour enregistrer l'archive de sauvegarde sur un serveur FTP. Dans ce cas, entrez les accès du FTP dans les champs suivants.
   - **Réseau**, pour enregistrer les archives de sauvegarde sur un partage réseau. Dans ce cas, saisissez le chemin vers l'emplacement souhaité sur le réseau (par exemple`\\computer\folder`), le nom de domaine et les identifiants de l'utilisateur du domaine.
7. Cliquez sur le bouton **Tester**. Une notification écrite vous indiquera si les paramètres spécifiés sont ou non valides.

   Pour créer une sauvegarde, tous les paramètres doivent être valides.
8. Cliquez sur **Enregistrer** pour créer la sauvegarde planifiée.

Restauration d'une sauvegarde de base de données

Lorsque, pour diverses raisons, votre instance GravityZone ne fonctionne pas correctement (échecs de mise à jour, interface dysfonctionnelle, fichiers endommagés, erreurs, etc.), vous pouvez restaurer la base de données de GravityZone à partir d'une copie de sauvegarde en utilisant :

- La même appliance
- Une nouvelle image de GravityZone
- La fonctionnalité Replica Set

Choisissez l'option qui correspond le mieux à votre situation et poursuivez la procédure de restauration uniquement après avoir lu attentivement les prérequis décrits ci-après.

Restaurer la base de données sur la même appliance virtuelle GravityZone

Configuration nécessaire

- Une connexion SSH à l'appliance GravityZone, à l'aide des privilèges **root**.

  Vous pouvez utiliser les identifiants de **putty** et **bdadmin** pour vous connecter à l'appliance via SHH puis exécutez la commande `sudo su` pour passer au compte **root**.
- L'infrastructure de GravityZone n'a pas changé depuis la sauvegarde.
- La sauvegarde est postérieure au 30 avril 2017 et la version de GravityZone est supérieure à la version 6.2.1-30. Dans le cas contraire, contactez l'équipe de support technique.
- Dans les architectures distribuées, GravityZone n'a pas été configuré pour utiliser la réplication de base de données (Replica Set).

  Pour vérifier la configuration, procédez comme suit :

  1. Ouvrez le fichier `/etc/mongodb.conf`.
  2. Vérifiez que `replSet` n'est pas configuré, comme dans l'exemple ci-dessous :

     ```
     # replSet = setname
     ```

  Note
  Pour restaurer la base de données lorsque le Replica Set est activé, reportez-vous à « Restaurer la base de données dans un environnement Replica Set » (p. 78).

- Aucun processus de l'interface en ligne de commande n'est en cours d'exécution.

  Pour vous assurer que tous les processus de l'interface en ligne de commande sont arrêtés, exécutez la commande suivante :

  ```
  # killall -9 perl
  ```

- Le package **mongoconsole** est installé sur l'appliance.

  Pour vérifier que la condition est remplie, exécutez cette commande :

```
# /opt/bitdefender/bin/mongoshellrestore --version
```

La commande ne devrait pas retourner d'erreurs, sinon exécutez :

```
# apt-get update
# apt-get install --upgrade mongoconsole
```

Restauration de la base de données

1. Rendez-vous à l'emplacement contenant l'archive de la base de données :

   ```
   # cd /directory-with-backup
   ```

   , où `répertoire-avec-sauvegarde` est le chemin vers l'emplacement des fichiers de sauvegarde.

   Par exemple :

   ```
   # cd /tmp/backup
   ```

2. Restaurez la base de données.

   ```
   # /opt/bitdefender/bin/mongoshellrestore -u bd -p 'GZ_db_password
   --authenticationDatabase admin --gzip --drop --archive < \
   gz-backup-$AAAAMMJJhorodatage
   ```

   Important

   Veillez à remplacer `GZ_db_password` avec le mot de passe réel du Serveur de base de données de GravityZone et les variables d'horodatage dans le nom de l'archive par la date du jour.
   La date finale doit par exemple ressembler à la suivante :

   ```
   gz-backup-2019-05-17(1495004926).tar.gz
   ```

3. Redémarrez les appliances.

La restauration de la base de données est désormais terminée.

Restaurer la base de données à partir d'une appliance virtuelle GravityZone retirée.

Configuration nécessaire

- Une nouvelle installation de l'appliance virtuelle de GravityZone :
  - Avec la même IP que l'ancienne appliance
  - Le rôle Serveur base de données est le SEUL installé.

  Vous pouvez télécharger l'image de l'appliance virtuelle GravityZone à partir d'ici.
- Une connexion SSH à l'appliance virtuelle GravityZone, à l'aide des privilèges **root**.
- L'infrastructure de GravityZone n'a pas changé depuis que la sauvegarde a été effectuée.
- La sauvegarde est postérieure au 30 avril 2017.
- Dans les architectures distribuées, GravityZone n'a pas été configuré pour utiliser la réplication de base de données (Replica Set).

  Si vous utilisez Replica Set dans votre environnement GravityZone, vous avez également le rôle Serveur de base de données d'installé sur d'autres instances de l'appliance.

  Pour restaurer la base de données lorsque le Replica Set est activé, reportez-vous à « Restaurer la base de données dans un environnement Replica Set » (p. 78).

Restauration de la base de données

1. Connectez-vous à l'appliance GravityZone via SSH et passez en **root**.
2. Arrêter VASync :

   ```
   # stop vasync
   ```

3. Stopper CLI:

   ```
   # # killall -9 perl
   ```

4. Rendez-vous à l'emplacement de la sauvegarde :

```
# cd /directory-with-backup
```

, où `répertoire-avec-sauvegarde` est le chemin vers l'emplacement des fichiers de sauvegarde.

Par exemple :

```
# cd /tmp/backup
```

5. Restaurez la base de données.

```
# /opt/bitdefender/bin/mongoshellrestore -u bd -p 'GZ_db_password
--authenticationDatabase=admin --gzip --drop \
--archive='/home/bdadmin/gz-backup-$AAAAMMJJhorodatage
```

Important

Veillez à remplacer `GZ_db_password` avec le mot de passe réel du Serveur de base de données de GravityZone et les variables d'horodatage dans le nom de l'archive par la date du jour.

La date finale doit par exemple ressembler à la suivante :

```
gz-backup-2019-05-17(1495004926).tar.gz
```

6. Restaurez l'ID de l'ancienne appliance :

```
# /opt/bitdefender/bin/mongoshell -u bd -p 'GZ-db_password
--eval print(db.applianceInstalls.findOne({name:'db'}).\
applianceId)" --quiet > /opt/bitdefender/etc/applianceid
```

Important

Veillez à remplacer `GZ_db_password` par le mot de passe réel du Serveur de base de données de GravityZone.

7. Supprimer les références aux anciens rôles.

```
# /opt/bitdefender/bin/mongoshell -u bd -p 'GZ_db_password
'db.applianceInstalls.remove({ip:db.applianceInstalls.findOne(
{name:"db"}).ip,name:{"$ne": "db"}});' --quiet devdb
```

Important
Veillez à remplacer `GZ_db_password` par le mot de passe réel du Serveur de base de données de GravityZone.

8. Lancez VASync :

```
# start vasync
```

9. Démarrer CLI :

```
# /opt/bitdefender/eltiw/installer
```

10. Installez les autres rôles.

```
# dpkg -l gz*
```

Notez que le schéma de base de données a bien été mis à jour vers la dernière version :

```
> db.settings.findOne().database
{
"previousVersion" : "000-002-009",
"ranCleanUpVersions" : {
"b0469c84f5bf0bec0b989ae37161b986" : "000-002-008"
},
"updateInProgress" : false,
"updateTimestamp" : 1456825625581,
"version" : "000-002-011"
}
```

11. Redémarrez l'appliance.

La restauration de la base de données est désormais terminée.

Restaurer la base de données dans un environnement Replica Set

Si vous avez déployé la base de données dans un environnement Replica Set, la procédure de restauration officielle est disponible dans le manuel mongoDB en ligne (en anglais uniquement).

Note
La procédure nécessite des compétences techniques avancées et devrait être réalisée uniquement par un technicien expérimenté. Si vous rencontrez des difficultés, veuillez contacter notre Support Technique afin qu'il vous aide à restaurer la base de données.

Active Directory

Grâce à l'intégration Active Directory, vous pouvez importer l'inventaire existant dans la Control Center à partir d'Active Directory sur site et à partir d'Active Directory hébergé dans Microsoft Azure, ce qui simplifie le déploiement, la gestion et le contrôle de la sécurité ainsi que l'édition de rapports en lien avec celle-ci. De plus, les utilisateurs d'Active Directory peuvent recevoir différents rôles utilisateur dans Control Center.

Pour intégrer et synchroniser le GravityZone avec un domaine Active Directory :

1. Allez sur **Configuration > Active Directory > Domaines** et cliquez sur ⊕ **Ajouter**.
2. Configurez les paramètres requis :
   - L'intervalle de synchronisation (en heures)
   - Le nom du domaine Active Directory (y compris l'extension du domaine)
   - Le nom d'utilisateur et le mot de passe d'un administrateur du domaine
   - Emplacement de l'inventaire réseau où afficher les endpoints AD:
     - Conserver la structure AD et ignorer les OU vides
     - Ignorer la structure AD, importer dans les Groupes personnalisés
     - Conserver la structure AD uniquement avec les OU sélectionnés
   - Les Contrôleurs de domaine avec lesquels Control Center est en cours de synchronisation. Développez la section **Contrôle requête domaine** et sélectionnez les contrôleurs dans le tableau.
3. Cliquez sur **Enregistrer**.

Important
Lorsque le mot de passe de l'utilisateur change, pensez à le mettre à jour également dans le Control Center.

Permissions d'accès

Avec les permissions d'accès, vous pouvez pour donner à GravityZone Control Center l'accès aux utilisateurs Active Directory (AD), en fonction des règles d'accès. Pour intégrer et synchroniser des domaines AD, voir Active Directory. Pour en apprendre plus sur la gestion des comptes utilisateurs via les règles d'accès, consultez le chapitre **Comptes utilisateurs** du Guide d'installation de GravityZone.

Responsable virtualisation

GravityZone peut actuellement être intégrée à VMware vCenter Server, Citrix XenServer, Nutanix Prism Element, Amazon EC2 et Microsoft Azure.

- « Intégration à vCenter Server » (p. 79)
- « Intégration à XenServer » (p. 82)
- « Intégration avec Nutanix Prism Element » (p. 83)
- « Intégration au service Amazon EC2 » (p. 85)
- « Intégration de Microsoft Azure » (p. 86)
- « Gestion des intégrations à des plateformes » (p. 87)

Important
Lorsque vous configurez une nouvelle intégration à un autre système vCenter Server, XenServer, Nutanix Prism Element ou Microsoft Azure, pensez également à vérifier et mettre à jour les privilèges d'accès des utilisateurs existants.

Intégration à vCenter Server

Vous pouvez intégrer le GravityZone à un ou plusieurs systèmes vCenter Server. Les systèmes vCenter Server en mode Linked Mode doivent être ajoutés séparément au Control Center.

Pour configurer l'intégration avec un système vCenter Server :

1. Rendez-vous sur la page **Configuration** de Control Center puis dans **Responsable virtualisation > Plateformes d'administration**.
2. Cliquez sur le bouton ⊕ **Ajouter** en haut du tableau et sélectionnez **vCenter Server** dans le menu. Une fenêtre de configuration s'affichera.
3. Spécifiez les informations de vCenter Server.
   - Le nom du système vCenter Server dans le Control Center
   - Le nom d'hôte ou l'adresse IP du système vCenter Server

- Le port vCenter Server (le `443` par défaut)

4. Spécifiez les identifiants à utiliser pour l'authentification avec vCenter Server. Vous pouvez choisir d'utiliser les identifiants fournis pour l'intégration à Active Directory ou un jeu d'identifiants différent. L'utilisateur dont vous indiquez les identifiants doit disposer d'une autorisation de niveau root ou administrateur sur le vCenter Server.
5. Choisissez la plateforme VMware installée que vous utilisez et configurez les paramètres en conséquence :
   - **Aucune**. Sélectionnez cette option pour NSX-T ou si aucune plateforme spécifique n'est installée pour VMware et cliquez sur **Enregistrer**. Il est nécessaire d'accepter le certificat de sécurité auto-signé pour procéder à l'intégration.

     Pour configurer l'intégration à NSX-T Manager et appliquer la protection pour endpoints à vos VM via la politique GravityZone Guest Introspection, consulter cet article de la base de connaissances.
   - **vShield**. Spécifiez les détails du système vShield Manager intégré à vCenter Server.
     - Le nom d'hôte ou l'adresse IP du système vShield Manager
     - Le port de vShield Manager (le `443` par défaut)
   - **NSX-V**. Spécifiez les détails de NSX Manager intégré à vCenter Server.

     Note
     Pour mettre à niveau VMWare vShield vers NSX, référez-vous à cet article de support.

     - Nom de l'hôte ou adresse IP du NSX Manager
     - Le port de NSX Manager (le `443` par défaut)
     - Identifiant et mot de passe utilisés pour s'identifier à NSX Manager.

       Ces identifiants seront enregistrés sur l'entité protégée et non pas dans le gestionnaire d'identifiants.
     - Cochez la case **Taguer si un virus est trouvé** pour utiliser les tags de sécurité NSX par défaut quand un malware est détecté sur la machine virtuelle.

       Une machine peut être taguée avec trois différents tags de sécurité, selon le niveau de risque de la menace :

- `ANTI_VIRUS.VirusFound.threat=low`, s'applique sur la machine lorsque Bitdefender classe le malware en risque faible, qu'il peut supprimer.
- `ANTI_VIRUS.VirusFound.threat=medium`, s'applique sur la machine si Bitdefender ne peut pas supprimer les fichiers infectés, mais il les désinfecte.
- `ANTI_VIRUS.VirusFound.threat=high`, s'applique sur la machine si Bitdefender ne peut ni supprimer les fichiers infectés, ni les désinfecte, mais en bloque l'accès.

Lorsque les menaces de différents niveaux de risques sont détectées sur la même machine, tous les tags associés seront appliqués. Par exemple, une machine sur laquelle des malwares à faible et haut risques sont détectés se verra attribuer les deux types de tags de sécurité.

Note
Vous pouvez trouver les tags de sécurité dans VMware vSphere, sous l'onglet **Réseau & Sécurité > NSX Managers >** `NSX Manager` **> Gérer > Tags de sécurité**.
Même si vous pouvez créer autant de tags que vous voulez, seuls les trois tags mentionnés fonctionnent avec Bitdefender.

6. **Limiter l'affectation de la politique à partir de l'affichage réseau**. Utilisez cette option pour contrôler la permission des administrateurs réseau de modifier les politiques des machines virtuelles via l'affichage **Ordinateurs et Machines virtuelles** de la page **Réseau**. Quand cette option est sélectionnée, les administrateurs peuvent modifier les politiques des machines virtuelles uniquement à partir de l'affichage **Machines virtuelles** de l'inventaire réseau.
7. Cliquez sur **Enregistrer**. Il vous sera demandé d'accepter les certificats de sécurité pour vCenter Server et NSX Manager. Ces certificats garantissent une communication sécurisée entre GravityZone et les composants VMware, résolvant le risque d'attaques man-in-the-middle.

   Vous pouvez vérifier si les certificats corrects ont été installés en vérifiant les informations du site du navigateur pour chaque composant VMware contre les informations de certificat affichées dans Control Center.
8. Cochez les cases pour accepter d'utiliser les certificats.

9. Cliquez sur **Enregistrer**. Vous pourrez visualiser le serveur vCenter dans la liste des intégrations actives.
10. Si vous utilisez la plateforme NSX-V :
    a. Allez dans l'onglet **Mise à jour > Composants**.
    b. Téléchargez puis publiez le package du **Security Server (VMware avec NSX)**. Pour plus d'informations sur comment mettre à jour les rôles de GravityZone, veuillez vous référer à « Mise à jour GravityZone » (p. 172).
    c. Allez dans l'onglet **Configuration > Responsables virtualisation**.
    d. Dans la colonne **Action**, cliquez sur le bouton **Enregistrer** correspondant au vCenter intégré à NSX afin d'enregistrer le service de Bitdefender avec VMware NSX Manager.

Avertissement
Lorsque le certificat de sécurité a expiré et que le vCenter tente de synchroniser, un pop-up vous invite à mettre à jour. Ouvrez la fenêtre de configuration de l'intégration de vCenter Server, cliquez sur **Enregistrer**, acceptez les nouveaux certificats, puis cliquez à nouveau sur **Enregistrer**.

Après l'enregistrement, Bitdefender ajoute à la console VMware vSphere :
- Service de Bitdefender
- Service manager de Bitdefender
- Trois nouveaux profils de service par défaut pour les modes d'analyse : permissif, normal et agressif.

Note
Vous pouvez aussi visualiser ces profils de service sur la page **Politiques** de la Control Center. Cliquez sur le bouton **Colonnes** en haut à droite du volet de droite pour voir plus d'informations.

À la fin vous pouvez voir que le serveur vCenter se synchronise. Patientez quelques minutes le temps que la synchronisation se termine.

Intégration à XenServer

Vous pouvez intégrer le GravityZone à un ou plusieurs systèmes XenServer.

Pour configurer l'intégration avec un système XenServer :

1. Allez sur la page **Configuration** de la Control Center et cliquez sur l'onglet **Responsables virtualisation**.
2. Cliquez sur le bouton ⊕ **Ajouter** en haut du tableau et sélectionnez **XenServer** dans le menu. Une fenêtre de configuration s'affichera.
3. Spécifiez les informations de XenServer.
   - Le nom du système XenServer dans le Control Center
   - Le nom d'hôte ou l'adresse IP du système XenServer
   - Le port XenServer (le `443` par défaut)
4. Spécifiez les identifiants à utiliser pour l'authentification avec XenServer. Vous pouvez choisir d'utiliser les identifiants fournis pour l'intégration à Active Directory ou un jeu d'identifiants différent.
5. **Limiter l'affectation de la politique à partir de l'affichage réseau**. Utilisez cette option pour contrôler la permission des administrateurs réseau de modifier les politiques des machines virtuelles via l'affichage **Ordinateurs et Machines virtuelles** de la page **Réseau**. Quand cette option est sélectionnée, les administrateurs peuvent modifier les politiques des machines virtuelles uniquement à partir de l'affichage **Machines virtuelles** de l'inventaire réseau.
6. Cliquez sur **Enregistrer**. Vous pourrez visualiser le serveur vCenter dans la liste des intégrations actives et qu'il se synchronise. Patientez quelques minutes le temps que la synchronisation se termine.

Intégration avec Nutanix Prism Element

Vous pouvez intégrer un ou plusieurs clusters Nutanix Prism Element à GravityZone, qu'ils soient ou non enregistrés sur Nutanix Prism Central.

Pour configurer l'intégration avec Nutanix Prism Element :

1. Allez sur la page **Configuration** de la Control Center et cliquez sur l'onglet **Responsables virtualisation**.
2. Cliquez sur le bouton ⊕ **Ajouter** en haut du tableau et sélectionnez **NutanixPrismElement** dans le menu. Une fenêtre de configuration s'affichera.
3. Saisissez les informations de Nutanix Prism Element :
   - Nom de Nutanix Prism Element dans Control Center.
   - L'adresse IP d'une Controller Virtual Machine (CVM) du cluster Nutanix Prism Element ou l'adresse IP de cluster virtuel.

- Port de Nutanix Prism Element (`9440` par défaut).

4. Saisissez les identifiants à utiliser pour s'authentifier à Nutanix Prism Element.

   Important
   L'utilisateur dont vous fournissez les identifiants doit avoir les privilèges Cluster Admin ou User Admin dans Nutanix Prism Element.

5. **Limiter l'affectation de la politique à partir de l'affichage réseau**. Utilisez cette option pour contrôler la permission des administrateurs réseau de modifier les politiques des machines virtuelles via l'affichage **Ordinateurs et Machines virtuelles** de la page **Réseau**. Quand cette option est sélectionnée, les administrateurs peuvent modifier les politiques des machines virtuelles uniquement à partir de l'affichage Machines virtuelles de l'inventaire réseau.
6. Cliquez sur **Enregistrer**. Il vous sera demandé d'accepter les certificats de sécurité pour Nutanix Prism. Ces certificats garantissent une communication sécurisée entre GravityZone et Nutanix Prism Element, résolvant le risque d'attaques man-in-the-middle.

   Vous pouvez vérifier que les bons certificats ont été installés en contrôlant que les informations du site du navigateur pour chaque cluster Nutanix Prism Element ou CVM sont identiques aux informations affichées dans Control Center.
7. Cochez les cases pour accepter d'utiliser les certificats.
8. Cliquez sur **Enregistrer**.

   Si vous avez saisi l'IP d'une CVM pour configurer l'intégration, il vous sera demandé dans une nouvelle fenêtre si vous voulez utiliser l'IP de cluster virtuel au lieu de l'IP de la CVM :

   a. Cliquez sur **Oui** pour utiliser l'IP de cluster virtuel pour l'intégration. L'IP de cluster virtuel remplacera l'IP de la CVM dans les informations de Nutanix Prism Element.

   b. Cliquez sur **Non** pour continuer à utiliser l'IP de la CVM.

      Note
      Les meilleures pratiques recommandent d'utiliser l'IP de cluster virtuel plutôt que l'IP de la CVM. De cette manière, l'intégration reste active même lorsqu'un hôte en particulier est indisponible.

c. Dans la fenêtre **Ajouter Nutanix Prism Element**, cliquez sur **Enregistrer**.

Vous pourrez voir Nutanix Prism Element dans la liste des intégrations actives. Patientez quelques minutes le temps que la synchronisation se termine.

Intégration au service Amazon EC2

Vous pouvez intégrer la GravityZone à votre inventaire Amazon EC2 pour protéger vos instances EC2 hébergées dans le cloud Amazon.

Prérequis :

- L'accès à un compte AWS valide et aux clés secrètes correspondantes
- Le compte AWS doit avoir les permissions suivantes :
  - `IAMReadOnlyAccess`
  - `AmazonEC2ReadOnly` pour toutes les régions AWS

Vous pouvez créer plusieurs intégrations à Amazon EC2. Pour chacune d'entre elles, vous devez fournir un compte AWS valide.

Note
Il n'est pas possible de créer intégration à l'aide des identifiants des différents rôles IAM créés pour le même compte AWS.

Pour configurer l'intégration à Amazon EC2 :

1. Allez sur la page **Configuration** de la Control Center et cliquez sur l'onglet **Responsables virtualisation**.
2. Cliquez sur le bouton ⊕ **Ajouter** en haut du tableau et sélectionnez **Intégration à Amazon EC2** dans le menu. Une fenêtre de configuration s'affichera.
3. Précisez les détails de l'intégration à Amazon EC2 :
   - Le nom de l'intégration. Lorsque vous ajoutez plusieurs intégrations à Amazon EC2, vous pouvez les identifier par leur nom.
   - L'accès au compte utilisateur AWS et les clés secrètes correspondantes.
4. **Limiter l'affectation de la politique à partir de l'affichage réseau**. Utilisez cette option pour contrôler la permission des administrateurs réseau de modifier les politiques des machines virtuelles via l'affichage **Ordinateurs et Machines virtuelles** de la page **Réseau**. Quand cette option est sélectionnée, les

administrateurs peuvent modifier les politiques des machines virtuelles uniquement à partir de l'affichage **Machines virtuelles** de l'inventaire réseau.

5. Cliquez sur **Enregistrer**. Si toutes les données saisies sont valides, l'intégration est créée et ajoutée à la grille.

Patientez quelques instants pendant que GravityZone se synchronise avec l'inventaire Amazon EC2.

Intégration de Microsoft Azure

Vous pouvez intégrer GravityZone à Microsoft Azure et protéger vos machines virtuelles hébergées dans le cloud Microsoft.

Prérequis :

- Application Azure avec permission de lecture
- Identifiants Active Directory
- Identité de l'application
- Secret de l'application

Pour plus d'informations sur comment obtenir les identifiants nécessaires et paramétrer l'application Azure, reportez-vous à cet article de la base de connaissances.

Vous pouvez créer plusieurs intégrations Microsoft Azure. Pour chaque intégration, vous devez avoir un identifiant Active Directory valide.

Pour configurer l'intégration à Microsoft Azure :

1. Allez sur la page **Configuration** de la Control Center et cliquez sur l'onglet **Responsables virtualisation**.
2. Cliquez sur le bouton ⊕ **Ajouter** en haut du tableau et sélectionnez **Azure Integration** dans le menu. Une fenêtre de configuration s'affichera.
3. Spécifiez les détails de l'intégration à Azure :
   - **Le nom de l'intégration**. Lorsque vous ajoutez plusieurs intégrations à Azure, vous pouvez les identifier par leur nom.
   - **Identifiants Active Directory**. Chaque instance d'Azure Active Directory possède un identifiant unique disponible dans les informations du compte Microsoft Azure.
   - **Identité de l'application**. Chaque application Azure possède un identifiant unique disponible dans les informations de l'application.

- **Secret de l'application**. Le secret de l'application est la valeur affichée lorsque vous sauvegardez une clé dans les paramètres de l'application Azure.

4. Sélectionnez l'option **Limiter l'affectation de la politique à partir de l'affichage réseau** pour modifier la politique uniquement à partir de l'affichage **Machines virtuelles**. Si l'option n'est pas sélectionnée, vous pouvez modifier la politique à partir de l'affichage **Ordinateurs et machines virtuelles**.
5. Cliquez sur **Enregistrer**. Si toutes les données saisies sont valides, l'intégration est créée et ajoutée à la grille.

Patientez quelques instants pendant que GravityZone se synchronise avec l'inventaire Microsoft Azure.

Gestion des intégrations à des plateformes

Pour modifier ou mettre à jour une intégration à une plateforme :

1. Dans la Control Center, allez dans l'onglet **Configuration > Responsables virtualisation**.
2. Cliquez sur le bouton **Modifier** dans la colonne **Action**.
3. Configurez les paramètres de règle selon vos besoins. Pour plus d'informations, veuillez vous référer à l'une des sections suivantes, selon la situation :
   - « Intégration à vCenter Server » (p. 79)
   - « Intégration à XenServer » (p. 82)
   - « Intégration avec Nutanix Prism Element » (p. 83)
   - « Intégration au service Amazon EC2 » (p. 85)
   - « Intégration de Microsoft Azure » (p. 86)
4. Cliquez sur **Enregistrer**. Veuillez patienter quelques minutes le temps que le serveur se resynchronise.

Les intégrations à Nutanix Prism Element, Amazon EC2 et Microsoft Azure sont automatiquement synchronisées toutes les 15 minutes. Vous pouvez synchroniser manuellement une intégration à tout moment, en procédant de la manière suivante :

1. Dans la Control Center, allez dans l'onglet **Configuration > Responsables virtualisation**.
2. Cliquez sur le bouton **Resynchronisation de l'inventaire** dans la colonne **Action**.
3. Cliquez sur **Oui** pour confirmer l'action.

Le bouton **Resynchronisation de l'inventaire** est particulièrement utile lorsque le statut de l'intégration change et nécessite une synchronisation, par exemple dans les situations suivantes :

- Pour l'intégration à Nutanix Prism Element :
  - L'utilisateur n'a plus les privilèges d'administration dans l'inventaire.
  - L'utilisateur devient invalide (mot de passe modifié ou supprimé).
  - Le certificat de sécurité devient invalide.
  - En cas d'erreur de connexion.
  - Un hôte est ajouté ou supprimé du cluster Nutanix Prism Element.
- Pour l'intégration à Microsoft Azure :
  - Un abonnement est ajouté ou supprimé dans Microsoft Azure.
  - Les machines virtuelles sont ajoutées ou supprimées dans l'inventaire Microsoft Azure.

Vous pouvez également synchroniser l'intégration en cliquant sur le bouton **Modifier**, puis sur **Enregistrer**.

Pour supprimer une intégration à vShield, XenServer, Nutanix Prism Element, Amazon EC2 ou Microsoft Azure :

1. Dans la Control Center, allez dans l'onglet **Configuration > Responsables virtualisation**.
2. Cliquez sur le bouton **Supprimer** dans la colonne **Action**, correspondant à l'intégration à supprimer.
3. Cliquez sur **Oui** pour confirmer l'action.

Pour supprimer une intégration NSX :

1. Connectez-vous à la console VMware vSphere et supprimez toutes les politiques de Bitdefender et les Security Servers.
2. Dans la Control Center, allez dans l'onglet **Configuration > Responsables virtualisation**.
3. Dans la colonne **Action**, correspondant à l'intégration à supprimer, cliquez sur **Désenregistrer** puis **Supprimer**.
4. Cliquez sur **Oui** pour confirmer l'action.

Pour afficher les informations les plus récentes, cliquez sur le bouton **Actualiser** en haut du tableau.

Fournisseurs de services de sécurité

GravityZone Security for Virtualized Environments s'intègre à VMware NSX-T Data Center via NSX-T Manager.

Intégration avec NSX-T Manager

NSX-T Manager est le système d'administration de vos Center Servers intégré à NSX-T Data Center. Pour que l'intégration fonctionne, vous devez configurer l'intégration des vCenter Servers associés avec NSX-T Manager. Pour en apprendre plus, consultez Intégration à vCenter Server.

Pour configurer l'intégration avec NSX-T Manager :

1. Dans Control Center, rendez-vous dans **Configuration > Responsable virtualisation > Fournisseurs de services de sécurité**.
2. Cliquez sur le bouton ⊕**Ajouter** en haut du tableau. Une fenêtre de configuration s'affichera.
3. Spécifiez les détails de l'intégration à NSX-T :
   - Nom de l'intégration NSX-T.
   - Le nom d'hôte ou l'adresse IP du système vCenter Server associé.
   - port de NSX-T (par défaut : 433).
4. Spécifiez les identifiants pour l'authentification avec vCenter Server. Vous pouvez choisir d'utiliser les identifiants fournis pour l'intégration à Active Directory ou un jeu d'identifiants différent. L'utilisateur dont vous indiquez les identifiants doit disposer d'une autorisation de niveau root ou administrateur sur le vCenter Server.
5. Cliquez sur **Enregistrer**.

   La Control Center intègre maintenant NSX-T. Pour appliquer la protection des endpoints à vos VM via la politique GravityZone Guest Introspection, consulter l'article de la base de connaissances Configurer et appliquer la protection des endpoints aux VM invitées VMware NSX-T via la politique GravityZone Guest Introspection.

Note
GravityZone ne peut être utilisé que pour protéger le vCenter Server associé.

NTSA

Dans cette section, vous pouvez configurer l'intégration de Bitdefender Network Traffic Security Analytics, une solution de sécurité qui détecte avec précision les failles de sécurité et qui fournit des informations sur les attaques avancées, en analysant le trafic réseau. Pour en apprendre plus sur cette solution, consultez la documentation de Bitdefender NTSA.

Important
La section intégration de NTSA est seulement disponible après avoir indiqué une clé de licence NTSA valide sur la page **Configuration > Licence**.

Pour configurer l'intégration NTSA, la solution NTSA doit être installée sur votre environnement et vous devez avoir les identifiants à la console web de NTSA.

Pendant l'intégration, vous devrez indiquer l'adresse de la console web NTSA (IP ou nom d'hôte) et fournir un token (clé d'appariement) généré depuis la console web NTSA, comme expliqué ci-dessus.

Configurer l'intégration de NTSA

1. Connectez-vous à Control Center GravityZone.
2. Allez sur la page **Configuration** et cliquez sur l'onglet NTSA.
3. Activez l'option **Intégrer avec Network Traffic Security Analytics (NTSA)**.
4. Saisissez les données suivantes :
   - L'adresse de la console web de NTSA (IP / Nom d'hôte).
   - Le port utilisé par GravityZone pour communiquer avec NTSA (par défaut : 443).
   - La clé d'appariement (token) générée par la console web de NTSA comme suit :
     a. Rendez-vous sur votre console web NTSA et ouvrez la page **Licences**.
     b. Sélectionnez l'option **Intégration avec GravityZone**.
     c. Cliquez sur **Générer une clé d'appariement**. La clé apparait automatiquement.

d. Appuyez sur le bouton **Copier dans le presse-papier**.

e. Cliquez sur **OK** pour confirmer.

5. Vérifiez que l'empreinte de l'hôte affichée correspond au certificat SSL de l'appliance NTSA, puis activez la fonction en sélectionnant **J'accepte le certificat**.
6. Cliquez sur **Enregistrer**.

Une fois la configuration terminée, l'intégration apparaitra comme **Synchronisée**. L'intégration NTSA peut avoir les statuts suivants :

- **N/A** : l'intégration n'a pas encore été configurée.
- **Synchronisée** : l'intégration est configurée et activée.
- **Token invalide**: la clé d'appariement de la console NTSA est invalide.
- **Erreur de connexion** : impossible de se connecter à l'adresse de la console web NTSA indiquée (IP / nom d'hôte invalide).
- **Erreur de certificat** : l'empreinte actuelle du certificat SSL de l'appliance NTSA ne correspond pas à l'empreinte acceptée à l'origine.
- **Erreur inconnue** : une erreur de communication inconnue est survenue.

Le champ **Dernière modification de l'état** indique la date et l'heure auxquelles a eu lieu la dernière modification des paramètres d'intégration, ou de dernière modification de l'état.

Une fois l'intégration avec NTSA configurée, vous pouvez désactiver / activer l'intégration en cochant la case située en haut de la page **NTSA**.

Connecter vos comptes GravityZone et NTSA

Une fois l'intégration configurée, vos comptes GravityZone et NTSA seront connectés, et vous pourrez facilement vous rendre sur la console web de NTSA, comme suit :

1. Dans GravityZone Control Center, cliquez sur le bouton **NTSA** situé en bas à gauche de la fenêtre.
2. Vous serez redirigé vers la page de connexion de la console web de NTSA. Après avoir saisir vos identifiants de connexion à NTSA, vous pouvez commencer à utiliser la console web de NTSA.

Vous n'aurez à saisir vos identifiants NTSA que lors de la première connexion. Après cela, vous aurez automatiquement accès à la console web de NTSA en cliquant sur le bouton **NTSA**, sans avoir à vous identifier.

Supprimer l'intégration de NTSA

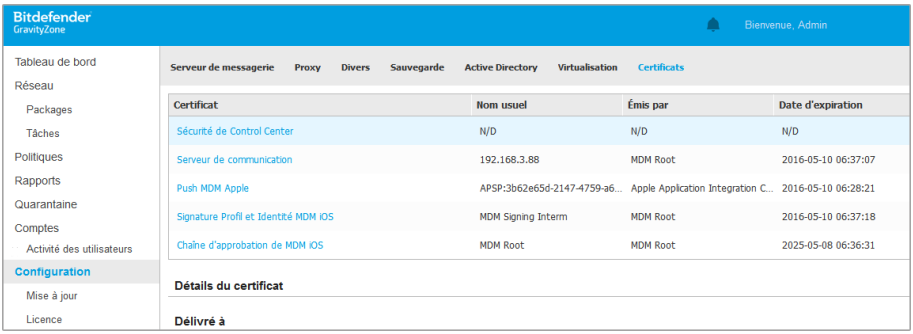
La suppression de la clé de licence de NTSA de la page **Configuration > Licence** supprimera également l'intégration de NTSA.

Note
Votre compte NTSA sera également déconnecté de GravityZone dans les cas suivants :

- La clé de licence de NTSA a été supprimée.
- Votre mot de passe NTSA a été modifié.
- Votre mot de passe GravityZone a été modifié.
- Les paramètres d'intégration de NTSA ont été modifiés.

Certificats

Afin que votre déploiement de GravityZone fonctionne correctement et en toute sécurité, vous devez créer et ajouter un nombre de certificats de sécurité dans Control Center.



La page Certificats

Control Center prend en charge les formats de certificat suivants :

- PEM (.pem, .crt, .cer, .key)

- DER (.der, .cer)
- PKCS#7 (.p7b, .p7c
- PKCS#12 (.p12, .pfx

Note
Les certificats suivants sont nécessaires uniquement pour gérer la sécurité sur les appareils Apple iOS :

- Certificat du Serveur de Communication
- Certificat Push MDM Apple
- Certificat de signature du profil et d'identité MDM iOS
- Certificat de la chaîne d'approbation de MDM iOS

Si vous ne prévoyez pas de déployer la gestion des appareils mobiles iOS, vous n'avez pas besoin de fournir ces certificats.

Certificat de Sécurité de Control Center

Le certificat de sécurité de Control Center est nécessaire pour identifier la console Web de Control Center comme étant un site Web de confiance dans le navigateur Web. Le Control Center utilise par défaut un certificat SSL signé parBitdefender. Ce certificat intégré n'est pas reconnu par les navigateurs Web et déclenche des avertissements de sécurité. Pour éviter les avertissements de sécurité du navigateur, ajoutez un certificat SSL signé par votre entreprise ou par une autorité de certification externe.

Pour ajouter ou remplacer le certificat de Control Center :

1. Rendez-vous sur la page **Configuration** et cliquez sur l'onglet **Certificats**.
2. Cliquez sur le nom du certificat.
3. Choisissez le type de certificat (avec une clé privée séparée ou incorporée).
4. Cliquez sur le bouton **Ajouter** à côté du champ **Certificat** et uploadez le certificat.
5. Pour les certificats avec une clé privée séparée, cliquez sur le bouton **Ajouter** à côté du champ **Clé privée** et uploadez la clé privée.
6. Si le certificat est protégé par mot de passe, saisissez le mot de passe dans le champ correspondant.
7. Cliquez sur **Enregistrer**.

Endpoint - Security Server certificat de sécurité communication

Ce certificat assure une communication sécurisée entre les agents de sécurité et la Security Server (Multi-Platforme) qu'ils ont assignée.

Pendant son déploiement, le Security Server génère un certificat auto-signé par défaut. Vous pouvez remplacer ce certificat intégré en ajoutant l'un de vos choix dans Control Center.

Pour ajouter ou remplacer un Endpoint - certificat de communication Security Server :

1. Rendez-vous sur la page **Configuration** et cliquez sur l'onglet **Certificats**.
2. Cliquez sur le nom du certificat.
3. Choisissez le type de certificat (avec une clé privée séparée ou incorporée).
4. Cliquez sur le bouton **Ajouter** à côté du champ **Certificat** et uploadez le certificat.
5. Pour les certificats avec une clé privée séparée, cliquez sur le bouton **Ajouter** à côté du champ **Clé privée** et uploadez la clé privée.
6. Si le certificat est protégé par mot de passe, saisissez le mot de passe dans le champ correspondant.
7. Cliquez sur **Enregistrer**. Un message d'avertissement peut apparaître si le certificat est auto-signé ou a expiré. S'il a expiré, veuillez renouveler votre certificat.
8. Cliquez sur **Oui** pour continuer à charger le certificat. Immédiatement une fois le téléchargement fini, Control Center envoie le certificat de sécurité aux Security Servers.

Si besoin, vous pouvez revenir au certificat intégré d'origine de chaque Security Server, comme suit :

1. Cliquez sur le nom de certificat sur la page **Certificats**.
2. Choisissez **Aucun certificat (utiliser celui par défaut)** comme type de certificat.
3. Cliquez sur **Enregistrer**.

Certificat du Serveur de Communication

Le certificat du serveur de communication est utilisé pour protéger les communications entre le serveur de communication et les appareils mobiles iOS.

Conditions :

- Ce certificat SSL peut être signé par votre entreprise ou par une autorité de certification externe.

  Avertissement
  Le certificat peut être reconnu comme invalide s'il n'a pas été délivré par une autorité de certification publique/fiable (par exemple, pour les certificats auto-signés).

- Le nom commun du certificat doit correspondre exactement au nom de domaine ou à l'adresse IP utilisée par les clients mobiles pour se connecter au Serveur de Communication. Cela est configuré en tant qu'adresse MDM externe dans l'interface de configuration de la console de l'appliance GravityZone.
- Les clients mobiles doivent faire confiance à ce certificat. Pour cela, vous devez également ajouter la Chaîne d'approbation de MDM iOS.

Pour ajouter ou remplacer le certificat du Serveur de communication :

1. Rendez-vous sur la page **Configuration** et cliquez sur l'onglet **Certificats**.
2. Cliquez sur le nom du certificat.
3. Choisissez le type de certificat (avec une clé privée séparée ou incorporée).
4. Cliquez sur le bouton **Ajouter** à côté du champ **Certificat** et uploadez le certificat.
5. Pour les certificats avec une clé privée séparée, cliquez sur le bouton **Ajouter** à côté du champ **Clé privée** et uploadez la clé privée.
6. Si le certificat est protégé par mot de passe, saisissez le mot de passe dans le champ correspondant.
7. Cliquez sur **Enregistrer**.

Certificat Push MDM Apple

Apple requiert un certificat Push MDM pour garantir une communication sécurisée entre le Serveur de communication et le Service de Notification Push d'Apple (APN) lors de l'envoi de notifications push. Les notifications push sont utilisées pour demander aux appareils de se connecter au Serveur de communication lorsque de nouvelles tâches ou modifications de politiques sont disponibles.

Apple délivre ce certificat directement à votre entreprise mais requiert que votre Demande de signature de certificat soit signée par Bitdefender. Control Center

fournit un assistant pour vous aider à obtenir facilement votre certificat push MDM Apple.

Important

- Vous avez besoin d'un identifiant Apple pour obtenir et gérer le certificat. Si vous n'avez pas d'identifiant Apple, vous pouvez en créer un sur la page web Mon identifiant Apple. Utilisez une adresse e-mail générique et non celle d'un employé pour obtenir l'identifiant Apple, puisque vous en aurez besoin par la suite pour renouveler le certificat.
- Le site web d'Apple ne fonctionne pas correctement avec Internet Explorer. Nous vous recommandons d'utiliser les dernières versions de Safari ou Chrome.
- Le certificat push MDM Apple est valide un an seulement. Lorsque le certificat est sur le point d'expirer, vous devez le renouveler et importer le certificat renouvelé dans Control Center. Si vous laissez le certificat expirer, vous devrez en créer un nouveau et réactiver tous vos appareils.

Ajouter un certificat push MDM Apple

Pour obtenir le certificat push MDM Apple et l'importer dans Control Center :

1. Rendez-vous sur la page **Configuration** et cliquez sur l'onglet **Certificats**.
2. Cliquez sur le nom du certificat et suivez l'assistant comme indiqué ci-dessous :

   Étape 1 - Obtenir une demande de signature de certificat signée par Bitdefender

   Sélectionnez l'option appropriée :

   - **J'ai besoin de générer une demande de signature de certificat signée par Bitdefender** (Recommandé)
     a. Indiquez le nom de votre entreprise, votre nom complet et votre adresse e-mail dans les champs correspondants.
     b. Cliquez sur **Générer** pour télécharger le fichier CSR signé par Bitdefender.
   - **J'ai déjà une demande de signature de certificat et j'ai besoin de la faire signer par Bitdefender**
     a. Uploadez votre fichier CSR et la clé privée associée en cliquant sur le bouton **Ajouter** à côté de leurs champs.

        Le Serveur de Communication a besoin d'une clé privée lors de l'authentification avec les serveurs APN.
     b. Spécifiez le mot de passe protégeant la clé privée, s'il y en a un.

c. Cliquez sur le bouton **Signer** pour télécharger le fichier CSR signé par Bitdefender.

Étape 2 - Demander un certificat push d'Apple

a. Cliquez sur le lien **Apple Push Certificates Portal** et connectez-vous à l'aide de votre identifiant Apple et de votre mot de passe.
b. Cliquez sur le bouton **Create a Certificate** et acceptez les conditions d'utilisation.
c. Cliquez sur **Choose file**, sélectionnez le fichier CSR puis cliquez sur **Upload**.

> **Note**
> Le bouton **Choose file** peut porter un nom différent tel que **Choose** ou **Browse**, en fonction du navigateur que vous utilisez.

d. Sur la page de confirmation, cliquez sur le bouton **>Download** pour recevoir votre certificat push MDM.
e. Retournez dans l'assistant dans Control Center.

Étape 3 - Importer le certificat push d'Apple

Cliquez sur le bouton **Ajouter un certificat** pour uploader le fichier du certificat à partir de votre ordinateur.

Vous pouvez consulter les détails du certificat dans le champ ci-dessous.

3. Cliquez sur **Enregistrer**.

Renouveler le certificat push MDM Apple

Pour renouveler le certificat MDM Apple et le mettre à jour dans Control Center :

1. Rendez-vous sur la page **Configuration** et cliquez sur l'onglet **Certificats**.
2. Cliquez sur le nom du certificat pour ouvrir l'assistant d'importation.
3. Obtenir une demande de signature de certificat signée par Bitdefender. La procédure est la même que pour obtenir un nouveau certificat.
4. Cliquez sur le lien **Portail des Certificats Push d'Apple** et connectez-vous avec l'identifiant Apple utilisé pour créer le certificat.
5. Localisez le certificat Push MDM de Bitdefender et cliquez sur le bouton **Renouveler** correspondant.
6. Cliquez sur **Choose file**, sélectionnez le fichier CSR puis cliquez sur **Upload**.
7. Cliquez sur **Télécharger** pour enregistrer le certificat sur votre ordinateur.
8. Retournez dans Control Center et importez le nouveau certificat push d'Apple.
9. Cliquez sur **Enregistrer**.

Certificat de signature du profil et d'identité MDM iOS

Le certificat de signature des profils et d'identité MDM iOS est utilisé par le serveur de communication pour signer les certificats d'identité et les profils de configuration envoyés aux appareils mobiles.

Conditions :

- Ce doit être un certificat intermédiaire ou un certificat d'entité finale, signé par votre entreprise ou par une autorité de certification externe.
- Les clients mobiles doivent faire confiance à ce certificat. Pour cela, vous devez également ajouter la Chaîne d'approbation de MDM iOS.

Pour ajouter ou remplacer le certificat de signature du profil et d'identité MDM iOS :

1. Rendez-vous sur la page **Configuration** et cliquez sur l'onglet **Certificats**.
2. Cliquez sur le nom du certificat.
3. Choisissez le type de certificat (avec une clé privée séparée ou incorporée).
4. Cliquez sur le bouton **Ajouter** à côté du champ **Certificat** et uploadez le certificat.
5. Pour les certificats avec une clé privée séparée, cliquez sur le bouton **Ajouter** à côté du champ **Clé privée** et uploadez la clé privée.
6. Si le certificat est protégé par mot de passe, saisissez le mot de passe dans le champ correspondant.
7. Cliquez sur **Enregistrer**.

Certificat de la chaîne d'approbation de MDM iOS

Les certificats de la chaîne d'approbation de MDM iOS sont requis sur les appareils mobiles pour garantir qu'ils font confiance au Certificat du serveur de communication et au certificat de signature du profil et d'identité MDM iOS. Le Serveur de communication envoie ce certificat aux appareils mobiles pendant l'activation.

La Chaîne d'approbation de MDM iOS doit comprendre tous les certificats intermédiaires y compris le certificat racine de votre entreprise ou le certificat intermédiaire émis par l'autorité de certification externe.

Pour ajouter ou remplacer les certificats de la chaîne d'approbation de MDM iOS :

1. Rendez-vous sur la page **Configuration** et cliquez sur l'onglet **Certificats**.
2. Cliquez sur le nom du certificat.

3. Cliquez sur le bouton **Ajouter** à côté du champ **Certificat** et uploadez le certificat.
4. Cliquez sur **Enregistrer**.

Dépôt

Cet onglet présente des informations sur les mises à jour de l'agent de sécurité, y compris les versions du produit stockées sur le Serveur de mise à jour et les versions disponibles sur le dépôt officiel de Bitdefender, les rings de mise à jour, la date et l'heure de la mise à jour et la dernière vérification de la disponibilité de nouvelles versions.

Note
Les versions du produit ne sont pas disponibles pour les serveurs de sécurité.

5.1.5. Gérer l'appliance GravityZone

L'appliance GravityZone dispose d'une interface de configuration basique, disponible depuis l'outil d'administration utilisé pour gérer l'environnement virtualisé où vous avez déployé l'appliance.

Voici les principales options disponibles après le premier déploiement de l'appliance GravityZone :

- Configurer les paramètres du Nom d'hôte
- Configurer les paramètres du réseau
- Définir les paramètres de proxy
- Serveur de communication MDM
- Paramètres avancés
- Configurer la langue

Utilisez les flèches et la touche `Tab` pour vous déplacer dans les menus et les options. Appuyez sur `Entrée` pour sélectionner une option spécifique.

Configurer les paramètres et le Nom d'hôte

La communication avec les rôles GravityZone s'effectue à l'aide de l'adresse IP ou du nom DNS de l'appliance sur laquelle ils sont installés. Par défaut, les composants de GravityZone communiquent en utilisant les adresses IP. Si vous souhaitez activer la communication via des noms DNS, vous devez configurer les appliances

GravityZone avec un nom DNS et vérifier que la résolution vers l'adresse IP configurée de l'appliance est correcte.

Prérequis :

- Configurez l'enregistrement DNS dans le serveur DNS.
- Le nom DNS doit effectuer correctement la résolution vers l'adresse IP configurée de l'appliance. Vous devez donc vous assurer que l'appliance est configurée avec l'adresse IP correcte.

Pour configurer les paramètres du Nom d'hôte :

1. Accédez à la console de l'appliance à partir de votre outil de gestion de la virtualisation (par exemple, vSphere Client).
2. Dans le menu principal, sélectionnez **Configurer les paramètres Nom d'hôte**.
3. Saisissez le Nom d'hôte de l'appliance et le nom de domaine de l'Active Directory (si nécessaire).
4. Sélectionnez **OK** pour enregistrer les modifications.

Configurer les paramètres du réseau

Vous pouvez configurer l'appliance afin qu'elle obtienne automatiquement les paramètres du réseau à partir du serveur DHCP ou vous pouvez configurer manuellement les paramètres du réseau. Si vous choisissez d'utiliser DHCP, vous devez configurer le serveur DHCP afin qu'il réserve une adresse IP spécifique à l'appliance.

Pour configurer les paramètres du réseau :

1. Accédez à la console de l'appliance à partir de votre outil de gestion de la virtualisation (par exemple, vSphere Client).
2. Dans le menu principal, sélectionnez **Configurer les paramètres réseau**.
3. Sélectionnez l'interface réseau (par défaut `eth0`).
4. Sélectionnez la méthode de configuration :
   - **Configurer les paramètres du réseau manuellement.** Vous devez indiquer l'adresse IP, le masque de réseau, l'adresse de la passerelle et les adresses du serveur DNS.

- **Obtenir les paramètres du réseau automatiquement par DHCP.** Utilisez cette option uniquement si vous avez configuré le serveur DHCP afin qu'il réserve une adresse IP spécifique à l'appliance.

5. Vous pouvez consulter les détails de la configuration IP actuelle ou l'état du lien en sélectionnant les options correspondantes.

Définir les paramètres de proxy

Si l'appliance se connecte à Internet via un serveur proxy, vous devez configurer les paramètres du proxy.

Note
Les paramètres du proxy peuvent également être configurés depuis la page Control Center, **Configuration > Proxy** Modifier les paramètres du proxy à un endroit les met automatiquement à jour à l'autre emplacement également.

Pour configurer les paramètres du proxy :

1. Accédez à la console de l'appliance à partir de votre outil de gestion de la virtualisation (par exemple, vSphere Client).
2. Dans le menu principal, sélectionnez **Configurer les paramètres du proxy**.
3. Sélectionnez **Définir paramètres proxy**.
4. Saisissez l'adresse du serveur proxy. Utilisez la syntaxe suivante :
   - Si le serveur proxy ne requiert pas d'authentification :

     ```
     http(s)://<IP/nom d'hôte>:<port>
     ```

   - Si le serveur proxy requiert une authentification :

     ```
     http(s)://<nom d'utilisateur>:<mot de passe>@<IP/nom d'hôte>:<port>
     ```

5. Sélectionnez **OK** pour enregistrer les modifications.

Sélectionnez **Afficher les informations du proxy** pour vérifier les configurations du proxy.

Serveur de communication MDM

Note
Cette configuration n'est nécessaire que pour la gestion des appareils mobiles, si votre clé de licence couvre le service Security for Mobile. L'option apparait dans le menu après avoir installé le rôle de serveur de communication.

Dans la configuration par défaut de GravityZone, les appareils mobiles peuvent être administrés uniquement lorsqu'ils sont connectés directement au réseau de l'entreprise (via Wifi ou VPN). Cela a lieu car lorsqu'on inscrit des appareils mobiles ils sont configurés pour se connecter à l'adresse locale de l'appliance du serveur de communication.

Pour pouvoir administrer les appareils mobiles sur Internet, quel que soit l'endroit où ils se trouvent, vous devez configurer le Serveur de communication avec une adresse publique.

Pour pouvoir administrer les appareils mobiles lorsqu'ils ne sont pas connectés au réseau de l'entreprise, les options suivantes sont disponibles :

- Configurez la redirection de port sur la passerelle de l'entreprise pour l'appliance exécutant le rôle du Serveur de Communication.
- Ajoutez une carte réseau supplémentaire à l'appliance exécutant le rôle du Serveur de communication et attribuez-lui une adresse IP publique.

Dans les deux cas, vous devez configurer le serveur de communication avec l'adresse externe à utiliser pour la gestion des appareils mobiles :

1. Accédez à la console de l'appliance à partir de votre outil de gestion de la virtualisation (par exemple, vSphere Client).
2. Dans le menu principal, sélectionnez **Serveur de communication MDM**.
3. Sélectionnez **Configurer l'adresse externe du Serveur MDM**.
4. Saisissez l'adresse externe.

   Utilisez la syntaxe suivante : `https://<IP/Domaine>:<Port>.`.

   - Si vous utilisez la redirection de port, vous devez saisir l'adresse IP publique ou le nom de domaine et le port ouvert sur la passerelle.
   - Si vous utilisez une adresse publique pour le Serveur de Communication, vous devez saisir l'adresse IP publique ou le nom de domaine et le port du Serveur de communication. Le port par défaut est le `8443`.

5. Sélectionnez **OK** pour enregistrer les modifications.
6. Sélectionnez **Afficher l'adresse externe du serveur MDM** pour vérifier les configurations.

Paramètres avancés

Les paramètres avancés couvrent plusieurs options de déploiement manuel, d'extension d'environnement et d'amélioration de la sécurité :

- Installation / désinstallation des rôles
- Installer le Security Server
- Configurer un mot de passe pour la nouvelle base de données
- Serveur de mise à jour
- Configurer les équilibreurs de rôle
- Jeu de réplicas
- Activer le Cluster de VPN sécurisés
- Se connecter à une base de données existante
- Se connecter à la Base de données existante (Cluster de VPN sécurisés)
- Vérifier le Cluster de VPN sécurisés

La disponibilité des options dépend des rôles installés et des services activés. Par exemple, si le rôle de Serveur de base de données n'est pas installé sur l'appliance, vous pouvez uniquement installer des rôles ou vous connecter à une base de données GravityZone déployée sur votre réseau. Une fois le rôle de Serveur de base de données déployé sur votre réseau, les options de connexion à une autre base de données apparaissent.

Installation / désinstallation des rôles

L'appliance GravityZone peut exécuter un, plusieurs ou l'ensemble des rôles suivants :

- **Serveur de base de données**
- **Serveur de mise à jour**
- **Console Web**
- **Serveur de communication**
- **Serveur des incidents**

Un déploiement de GravityZone nécessite d'exécuter une instance de chaque rôle. Ainsi, selon la façon dont vous préférez répartir les rôles de GravityZone, vous déploierez une à quatre appliances GravityZone. Le rôle du Serveur de base de données est le premier à être installé. Dans un scénario avec plusieurs appliances de GravityZone, vous installerez le rôle du Serveur de base de données sur la première appliance et configurerez toutes les autres appliances pour se connecter à l'instance de la base de données existante.

Note

Vous pouvez installer d'autres instances de certains rôles à l'aide des équilibreurs de rôle. Pour plus d'informations, reportez-vous à « Configurer les équilibreurs de rôle » (p. 107).

Pour installer les rôles GravityZone :

1. Accédez à la console de l'appliance à partir de votre outil de gestion de la virtualisation (par exemple, vSphere Client).
2. Dans le menu principal, sélectionnez **Paramètres avancés**.
3. Sélectionnez **Installation / désinstallation des rôles**.
4. Sélectionnez **Ajouter ou supprimer des rôles**.
5. Procédez selon la situation actuelle :
   - S'il s'agit du déploiement initial de l'appliance GravityZone, appuyez sur la `Barre d'espace` puis sur `Entrée` pour installer le rôle Serveur de base de données. Vous devez confirmer votre choix en appuyant à nouveau sur `Entrée`. Configurez le mot de passe base de données puis attendez que l'installation soit terminée.
   - Si vous avez déjà déployé une autre appliance avec le rôle Serveur de base de données, sélectionnez **Annuler** et retournez au menu **Ajouter ou supprimer des rôles**. Vous devez ensuite choisir **Configurer l'adresse de la base de données** et saisir l'adresse du serveur de la base de données. Assurez-vous que vous avez bien configuré votre mot de passe base de données avant d'accéder à cette option. Si vous ne connaissez pas le mot de passe base de données, configurez-en un nouveau en sélectionnant **Paramètres avancés > Configurer un nouveau mot de passe base de données** à partir du menu principal.

Utilisez la syntaxe suivante : `http://<IP/Nom d'hôte>:<Port>`. Le port de la base de données par défaut est le `27017`. Saisissez le mot de passe base de données précédent.

6. Installez les autres rôles en choisissant **Ajouter ou supprimer des rôles** dans le menu **Installer/Désinstaller Rôles** puis les rôles à installer. Pour chaque rôle que vous souhaitez installer ou désinstaller, appuyer sur la `Barre d'espace` pour sélectionner ou désélectionner le rôle puis appuyer sur `Entrée` pour continuer. Vous devez confirmer votre choix en appuyant de nouveau sur `Entrée` puis patienter jusqu'à la fin de l'installation.

Note
Chaque rôle est normalement installé en quelques minutes. Lors de l'installation, les fichiers nécessaires sont téléchargés à partir d'Internet. L'installation prend donc plus de temps si la connexion à Internet est lente. Si l'installation bloque, redéployez l'appliance.

Vous pouvez voir les rôles installés et leurs IP en sélectionnant l'une des options suivantes dans le menu **Installer/Désinstaller rôles** :

- **Afficher les rôles installés localement**, pour voir uniquement les rôles installés sur cette appliance.
- **Affichier tous les rôles installés**, pour voir tous les rôles installés dans votre environnement GravityZone.

Installer le Security Server

Note
Le Security Server sera disponible pour utilisation si votre clé de licence le permet.

Vous pouvez installer le Security Server à partir de l'interface de configuration de l'appliance GravityZone, directement sur l'appliance GravityZone, ou bien à partir de Control Center comme une appliance autonome. Les avantages d'installer le Security Server à partir de l'appliance :

- Convient aux déploiements de GravityZone avec une seule appliance possédant tous les rôles.
- Vous pouvez voir et utiliser le Security Server sans avoir à intégrer GravityZone dans une plateforme de virtualisation.

- Moins d'opérations de déploiement à effectuer.

Prérequis :

Le rôle Serveur base de données doit être installé sur l'appliance GravityZone, ou bien cette dernière doit être configurée pour se connecter à une base de données existante.

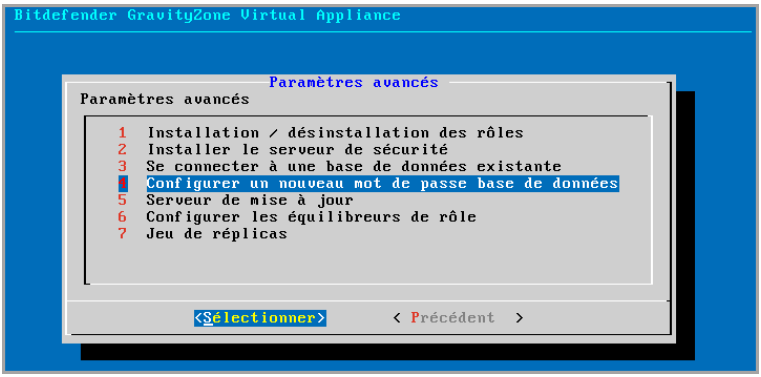
Pour installer Security Server à partir de l'interface de l'appliance :

1. Accédez à la console de l'appliance à partir de votre outil de gestion de la virtualisation (par exemple, vSphere Client).
2. Dans le menu principal, sélectionnez **Paramètres avancés**.
3. Sélectionnez **Installer Security Server**. Une message de confirmation s'affichera.
4. Appuyez sur `Entrée` pour continuer et attendez que l'installation soit terminée.

Note
Vous pouvez désinstaller ce Security Server uniquement à partir du menu **Paramètres avancés** de l'interface de l'appliance.

Configurer un mot de passe pour la nouvelle base de données

Lors de l'installation du rôle de Serveur de base de données, vous devez définir un mot de passe pour protéger la base de données. Si vous voulez le changer, configurez-en un nouveau en allant dans **Paramètres avancés > Configurer un nouveau mot de passe base de données** à partir du menu principal.



Interface de la console de l'appliance : Option Définir un nouveau mot de passe pour la base de données

Suivez les instructions pour définir un mot de passe complexe.

Configurer Update Server

L'appliance GravityZone est configurée par défaut pour se mettre à jour à partir d'Internet. Vous pouvez également, si vous préférez, configurer vos appliances installées pour qu'elles se mettent à jour à partir du serveur de mise à jour local Bitdefender (l'appliance GravityZone avec le rôle Update Server installé).

Pour configurer l'adresse du serveur de mise à jour :

1. Accédez à la console de l'appliance à partir de votre outil de gestion de la virtualisation (par exemple, vSphere Client).
2. Dans le menu principal, sélectionnez **Paramètres avancés**.
3. Sélectionner **Mise à jour du serveur**.
4. Sélectionnez **Configurer l'adresse de mise à jour**.
5. Saisissez l'adresse IP ou le nom d'hôte de l'appliance exécutant le rôle Update Server. Le port d'Update Server par défaut est le `7074`.

Configurer les équilibreurs de rôle

Pour garantir la fiabilité et l'extensibilité, vous pouvez installer plusieurs instances de rôles spécifiques (Serveur de communication, Console Web).

Pour garantir la fiabilité et l'extensibilité, vous pouvez installer plusieurs instances de rôles spécifiques (Serveur des incidents, Serveur de communication, Console Web).

Chaque instance de rôle est installée sur une appliance différente.

Toutes les instances d'un rôle spécifique doivent être connectées aux autres rôles via un équilibreur de rôles.

L'appliance GravityZone comprend des équilibreurs intégrés que vous pouvez installer et utiliser. Si vous avez déjà des logiciels ou du matériel d'équilibrage dans votre réseau, vous pouvez les utiliser au lieu des équilibreurs intégrés.

Les équilibreurs de rôle intégrés ne peuvent pas être installés avec des rôles sur une appliance GravityZone.

1. Accédez à la console de l'appliance à partir de votre outil de gestion de la virtualisation (par exemple, vSphere Client).
2. Dans le menu principal, sélectionnez **Paramètres avancés**.

3. Sélectionnez **Configurer les équilibreurs de rôle**.
4. Sélectionnez l'option souhaitée :
   - **Utiliser des équilibreurs externes.** Sélectionnez cette option si votre infrastructure réseau dispose déjà de logiciels ou de matériel d'équilibrage que vous pouvez utiliser. Vous devez saisir l'adresse de l'équilibreur pour chaque rôle que vous souhaitez équilibrer. Utilisez la syntaxe suivante :

     `http(s)://<IP/Nom d'hôte>:<Port>`.

   - **Utiliser les équilibreurs intégrés.** Sélectionnez cette option pour installer et utiliser le logiciel équilibreur intégré.

     Important
     To install multiple instances of the Incidents Server role you may only use the built-in balancer.

5. Sélectionnez **OK** pour enregistrer les modifications.

Jeu de réplicas

Cette option vous permet d'activer l'utilisation d'un replica set de la base de données au lieu d'une instance de base de données de serveur unique. Ce mécanisme permet de créer plusieurs instances de base de données dans un environnement GravityZone distribué, garantissant une haute disponibilité de la base de données en cas de panne.

Important
La réplication de la base de données est disponible uniquement pour les nouvelles installations de l'appliance GravityZone à partir de la version 5.1.17-441.

Configurer le replica set

Vous devez commencer par activer le Replica Set sur la première appliance GravityZone installée. Vous pourrez ensuite ajouter des membres du replica set en installant le rôle de base de données aux autres instances GravityZone du même environnement.

Important
- Le Replica Set requiert au moins trois membres pour fonctionner.

- Vous pouvez ajouter jusqu'à sept instances de rôles de base de données comme membres du replica set (limite MongoDB).
- Il est recommandé d'utiliser un nombre impair d'instances de base de données. Un nombre pair de membres consumera plus de ressources pour les mêmes résultats.

Pour activer la réplication de la base de données dans votre environnement GravityZone :

1. Installez le rôle de serveur base de données sur la première appliance GravityZone. Pour plus d'informations, reportez-vous à « Installation / désinstallation des rôles » (p. 103).
2. Configurez les autres appliances pour se connecter à la première instance base de données. Pour plus d'informations, reportez-vous à « Se connecter à une base de données existante » (p. 111).
3. Allez dans le menu principal de la première appliance, sélectionnez **Paramètres avancés** puis sélectionnez **Replica Set** pour l'activer. Une message de confirmation s'affichera.
4. Sélectionnez **Oui** pour confirmer.
5. Installez le rôle serveur de la base de données sur toutes les autres appliances GravityZone :

Dès que les étapes ci-dessus auront été effectuées, toutes les instances de base de données commenceront à fonctionner en tant que replica set :

- Une instance principale est choisie, la seule à accepter des opérations d'écriture.
- L'instance principale écrit toutes les modifications apportées à son jeu de données dans un journal.
- Les instances secondaires répliquent ce journal et appliquent les mêmes modifications à leurs jeux de données.
- Lorsque l'instance principale n'est pas disponible, le replica set choisit comme instance principale l'une des instances secondaires.
- Lorsqu'une instance principale ne communique pas avec les autres membres du jeu depuis plus de 10 secondes, le replica set tente de sélectionner un autre membre afin qu'il devienne la nouvelle instance principale.

Supprimer des membres du replica set

Pour supprimer des membres du replica set, sélectionnez simplement dans leur interface de la console de l'appliance (interface graphique) **Installer/Désinstaller des rôles > Ajouter ou supprimer des rôles** et décochez **Serveur de base de données**.

Note
Vous pouvez supprimer un membre du replica set uniquement si au moins quatre instances de la base de données ont été installées dans le réseau.

Activer le Cluster de VPN sécurisés

Les rôles de GravityZone ont plusieurs services internes qui communiquent exclusivement les uns avec les autres. Pour améliorer la sécurité de l'environnement, vous pouvez isoler ces services en les intégrant à un cluster VPN. Que ces services soient sur une ou plusieurs appliances, ils communiqueront ainsi via un canal sécurisé.

Important

- Cette fonctionnalité nécessite un déploiement standard de GravityZone, sans qu'aucun outil personnalisé ne soit installé.
- Une fois le cluster activé, il est impossible de le désactiver.

Pour sécuriser les services internes des appliances :

1. Accédez à la console de l'appliance à partir de votre outil de gestion de la virtualisation (par exemple, vSphere Client).
2. Dans le menu principal, sélectionnez **Paramètres avancés**.
3. Sélectionnez **Activer le Cluster de VPN sécurisés**.

   Un message vous informe des modifications qui seront apportées.
4. Choisissez **Oui** pour confirmer et poursuivre l'installation du VPN.

   Une fois le processus terminé, un message de confirmation apparait.

Dorénavant, tous les rôles de l'application sont installés en mode sécurisé et les services communiqueront via l'interface VPN. Toute nouvelle appliance ajoutée à l'environnement devra également être ajoutée au cluster VPN. Pour plus d'informations, reportez-vous à « Se connecter à la Base de données existante (Cluster de VPN sécurisés) » (p. 112).

Se connecter à une base de données existante

Dans une architecture distribuée de GravityZone, vous devez installer le rôle du Serveur de base de données sur la première appliance et configurerez toutes les autres appliances pour se connecter à l'instance de la base de données existante. De cette manière, toutes les appliances partageront la même base de données.

Important
Il est recommandé d'activer le cluster de VPN sécurisé et de se connecter à une base de données à l'intérieur du cluster. Pour plus d'informations, reportez-vous à :

- « Activer le Cluster de VPN sécurisés » (p. 110)
- « Se connecter à la Base de données existante (Cluster de VPN sécurisés) » (p. 112)

Pour connecter une appliance à une base de données GravityZone située hors du cluster VPN sécurisé :

1. Accédez à la console de l'appliance à partir de votre outil de gestion de la virtualisation (par exemple, vSphere Client).
2. Dans le menu principal, sélectionnez **Paramètres avancés**.
3. Sélectionner **Se connecter à une base de données existante**.

   Note
   Assurez-vous que vous avez bien configuré votre mot de passe base de données avant d'accéder à cette option. Si vous ne connaissez pas le mot de passe base de données, configurez-en un nouveau en allant dans **Paramètres avancés > Configurer un nouveau mot de passe base de données** à partir du menu principal.

4. Sélectionnez **Configurer l'adresse du serveur de la base de données**.
5. Saisissez l'adresse de la base de données, en utilisant la syntaxe suivante :

   `<IP/Nom d'hôte>:<Port>`

   Indiquer le port est facultatif. Le port par défaut est `27017`.
6. Saisissez le mot de passe base de données précédent.

Interface de la console de l'appliance : saisissez mot de passe base de données

7. Sélectionnez **OK** pour enregistrer les modifications.
8. Sélectionnez **Afficher l'adresse du serveur de la base de données** pour vérifier que l'adresse a été configurée correctement.

Se connecter à la Base de données existante (Cluster de VPN sécurisés)

Utilisez cette option lorsque vous devez étendre votre déploiement de GravityZone en ajoutant des appliances et que le cluster VPN sécurisé est activé. De cette manière, toutes les nouvelles appliances utiliseront la même base de données que le déploiement existant, et ce de manière sécurisée.

Pour plus d'informations sur le cluster VPN sécurisé, reportez-vous à « Activer le Cluster de VPN sécurisés » (p. 110).

Configuration nécessaire

Avant de poursuivre, vérifiez que vous disposez des éléments suivants :

- Adresse IP du serveur de la base de données
- Le mot de passe de l'utilisateur **bdadmin** sur appliance ayant le rôle de Serveur de base de données

Connexion à la base de données

Pour connecter une appliance à une base de données GravityZone située dans le cluster VPN sécurisé :

1. Accédez à la console de l'appliance à partir de votre outil de gestion de la virtualisation (par exemple, vSphere Client).
2. Dans le menu principal, sélectionnez **Paramètres avancés**.
3. Sélectionnez **Se connecter à la Base de données existante (Cluster de VPN sécurisés)**

   Vous serez informé des prérequis ainsi que d'alternatives si ces prérequis ne sont pas remplis.
4. Sélectionnez **OK** pour confirmer et continuer.
5. Saisissez l'adresse IP du Serveur de base de données, au sein du Cluster de VPN sécurisés.
6. Saisissez le mot de passe de l'utilisateur **bdadmin** sur appliance ayant le rôle de Serveur de base de données
7. Sélectionnez **OK** pour sauvegarder les changements et continuer.

Une fois le processus terminé, un message de confirmation apparait. La nouvelle appliance devient membre du cluster et elle communiquera avec les autres appliances de manière sécurisée. Toutes les appliances partageront la même base de données.

Vérifier l'état du Cluster de VPN sécurisés

Cette option n'est disponible qu'après avoir activé le cluster VPN sécurisé. Sélectionnez cette option pour vérifier quelles appliances de votre déploiement GravityZone n'ont pas encore suivi cette procédure de sécurisation des services. Vous aurez peut-être à vérifier que les appliances sont en ligne et accessibles.

Configurer la langue

Pour changer la langue de l'interface de configuration de l'appliance :

1. Sélectionnez **Configurer Langue** dans le menu principal.
2. Sélectionnez la langue dans les options disponibles : Une message de confirmation s'affichera.

   Note
   Vous devrez peut être faire dérouler la liste pour voir apparaître votre langue.

3. Sélectionnez **OK** pour enregistrer les modifications.

5.2. Gestion des licences

GravityZone ne comprend qu'une clé de licence pour tous les services de sécurité.

En plus des services de sécurité de base, GravityZone fournit également d'importantes fonctionnalités de protection sous forme d'extensions. Chaque extension est activée par une clé séparée et vous ne pouvez l'utiliser que si vous disposez d'une licence de base valide. Si la licence principale est invalide, vous pourrez voir les diverses options des fonctionnalités sans être en mesure de les utiliser.

Vous pouvez choisir de tester GravityZone et décider s'il s'agit de la solution adaptée à votre entreprise. Pour activer votre version d'évaluation, vous devez saisir la clé de licence de la version d'évaluation indiquée dans l'e-mail d'inscription de Control Center.

Note
Le Control Center est fourni gratuitement avec tout service de sécurité GravityZone.

Pour continuer à utiliser GravityZone après la fin de la période d'essai, vous devez acheter une clé de licence et l'utiliser pour enregistrer le produit.

Pour acheter une licence, contactez un revendeur Bitdefender ou contactez-nous par e-mail à info@bitdefender.fr.

La clé de licence de GravityZone peut être gérée à partir de la page **Licence** de Control Center. Quand votre clé de licence sera sur le point d'expirer, un message apparaîtra dans la console pour vous informer qu'elle doit être renouvelée. Pour saisir une nouvelle clé de licence ou afficher les détails de la licence actuelle, allez sur la page **Licence**.

5.2.1. Trouver un revendeur

Nos revendeurs vous fourniront toutes les informations dont vous avez besoin et vous aideront à choisir la meilleure option de licence pour vous.

Pour trouver un revendeur Bitdefender dans votre pays :

1. Rendez-vous sur la page Trouver un partenaire du site web de Bitdefender.
2. Sélectionnez le pays dans lequel vous habitez afin de voir les coordonnées des partenaires Bitdefender disponibles.
3. Si vous ne trouvez pas de revendeur Bitdefender dans votre pays, n'hésitez pas à nous contacter par e-mail à l'adresse channel-sales@bitdefender.fr.

5.2.2. Saisie de vos clés de licence

L'activation de la licence GravityZone peut être réalisée en ligne ou hors connexion (lorsqu'aucune connexion Internet n'est disponible). Vous devez fournir une clé de licence valide dans les deux cas.

Pour l'activation hors connexion, vous aurez également besoin du code d'activation hors connexion associé à la clé de licence.

Pour changer la clé de licence existante ou enregistrer une extension :

1. Connectez-vous au Control Center à l'aide d'un compte administrateur de l'entreprise.
2. Allez sur la page **Configuration > Licence**.
3. Cliquez sur le bouton **Ajouter** en haut du tableau.
4. Sélectionnez le type d'activation :
   - **en ligne**. Dans ce cas, saisissez une clé de licence valide dans le champs **Clé de licence**. La clé de licence sera vérifiée et validée en ligne.
   - **Hors connexion**, lorsqu'aucune connexion à Internet n'est disponible. Vous avez besoin dans ce cas d'indiquer la clé de licence ainsi que son code d'activation.

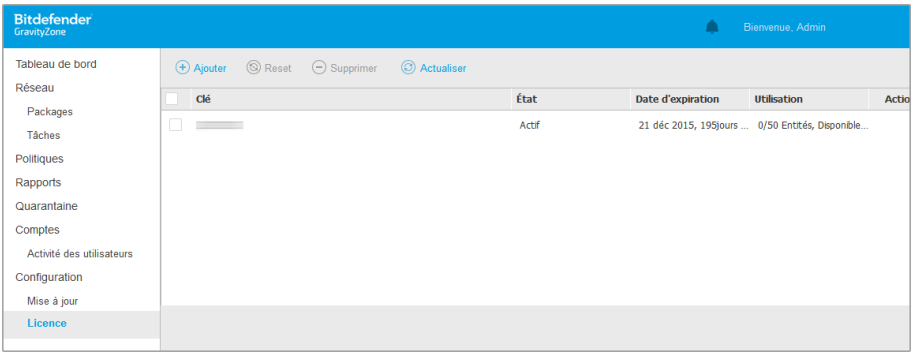
   Si la clé de licence n'est pas valide, une erreur de validation apparaît sous la forme d'une info-bulle sur le champ **Clé de licence**.
5. Cliquez sur **Ajouter**. La clé de licence sera ajoutée à la page **Licence**, où vous pourrez consulter ses détails.
6. Cliquez sur **Enregistrer** pour appliquer les modifications. Control Center redémarre et vous devez vous reconnecter pour pour voir les modifications.

Note
Vous pouvez utiliser les extensions tant que la licence de base compatible est valide. Sinon, vous pourrez voir les fonctionnalités sans être en mesure de les utiliser.

5.2.3. Vérification des détails de la licence actuelle

Pour afficher des informations sur votre licence :

1. Connectez-vous au Control Center à l'aide d'un compte administrateur de l'entreprise.
2. Allez sur la page **Configuration > Licence**.



La page Licence

3. Le tableau fournit des informations sur la clé de licence existante.
   - Clé de licence
   - État de la clé de licence
   - Date d'expiration et durée de validité de la licence restante

     Important
     Lorsque la licence expire, les modules de protection des agents installés sont désactivés. Par conséquent, les terminaux ne sont plus protégés et vous ne pouvez plus procéder à des tâches d'analyse. Tous les nouveaux agents installés seront soumis à une période d'essai.

   - Nombre d'utilisations de la licence

5.2.4. Réinitialisation du nombre d'utilisations de la licence

Vous pouvez trouver des informations sur le nombre d'utilisations de la clé de licence sur la page **Licence**, dans la colonne **Utilisation**.

Si vous avez besoin de mettre à jour les informations sur l'utilisation, sélectionnez la clé de licence et cliquez sur le bouton **Réinitialiser** en haut du tableau.

5.3. Installer la protection des postes de travail

Selon la configuration de la machine et l'environnement de réseau, vous pouvez choisir d'installer uniquement les agents de sécurité ou d'utiliser également un Security Server. Dans ce dernier cas, vous devez d'abord installer Security Server, puis les agents de sécurité.

Il est recommandé d'utiliser le Security Server dans des environnements virtualisés tels que Nutanix, VMware ou Citrix Xen, ou si les machines possèdent peu de ressources matérielles.

Important
Seuls Bitdefender Endpoint Security Tools et Bitdefender Tools supportent une connexion à Security Server. Pour plus d'informations, reportez-vous à « L'architecture de GravityZone » (p. 9).

5.3.1. Installation de Security Server

Security Server est une machine virtuelle dédiée qui déduplique et centralise une grande partie de la fonctionnalité antimalware des clients antimalwares, en agissant en tant que serveur d'analyse.

Le déploiement Security Server est spécifique à l'environnement dans lequel il est installé. Les procédures d'installation sont décrites ici :

- Security Server pour VMware NSX
- Security Server multiplateforme ou pour VMware vShield
- Security Server pour Amazon EC2
- Security Server pour Microsoft Azure

Installation de Security Server sur VMware NSX

Dans les environnements VMware NSX, vous devez déployer le service de Bitdefender sur chaque cluster à protéger. L'appliance se déploiera automatiquement sur tous les hôtes au sein du cluster. Toutes les machines virtuelles d'un hôte sont automatiquement connectées via l'Introspection en mode invité à l'instance du Security Server installée sur cet hôte.

Le déploiement Security Server doit être fait exclusivement à partir de vSphere Web Client.

Pour installer le service Bitdefender :

1. Connectez-vous à vSphere Web Client.
2. Allez dans **Réseau & Sécurité > Installation** puis cliquez sur l'onglet **Déploiements de service**.
3. Cliquez sur le bouton **Nouveau déploiement de service** (l'icône signe plus). La fenêtre de configuration s'affichera.

4. Sélectionnez **Introspection invité** et cliquez sur **Suivant**.
5. Sélectionnez le datacenter et les clusters sur lesquels déployer le service, puis cliquez sur **Suivant**.
6. Sélectionnez le réseau stockage et administration, cliquez sur **Suivant** puis **Terminer**.
7. Répétez les étapes 3 à 6, cette fois en choisissant le service **Bitdefender**.

   Avant de procéder à l'installation, assurez-vous que vous avez une connexion réseau entre le réseau sélectionné et GravityZone Control Center.

   Une fois le service Bitdefender est installé, il va déployer automatiquement le Security Server sur tous les hôtes ESXi dans les clusters sélectionnés.

Avertissement
Pour que les services fonctionnent correctement, il est très important de les installer dans cet ordre, d'abord Introspection invité puis Bitdefender, et non pas les deux en même temps.

Note
Pour plus d'informations sur l'ajout de services partenaires pour NSX, consultez le centre de documentation VMware NSX.
Si vous choisissez **Spécifié dans l'hôte** pour le stockage et la gestion du réseau, vérifiez que l'agent VM est configuré sur les hôtes pour l'Introspection invité et les services Bitdefender.

Security Server a des exigences spécifiques qui dépendent du nombre de machines virtuelles qu'il doit protéger. Pour régler la configuration hardware par défaut du Security Server :

1. Connectez-vous à VMware vSphere Web Client.
2. Allez dans **Hôtes et Clusters**.
3. Sélectionnez le cluster où Security Server est déployé, puis sélectionnez l'onglet **Objets connexes > Machines virtuelles**.
4. Éteignez l'appliance **Bitdefender**.
5. Cliquez droit sur le nom de l'appliance, puis choisissez **Modifier les paramètres...** dans le menu contextuel.
6. Dans l'onglet **Hardware virtuel** , ajustez les valeurs de CPU et RAM en fonction de vos besoins puis cliquez sur **OK** pour enregistrer les modifications.

7. Rallumez l'appliance.

Note
Pour mettre à niveau VMWare vShield vers NSX, référez-vous à cet article de support.

Installation de Security Server multiplateforme ou pour VMware vShield

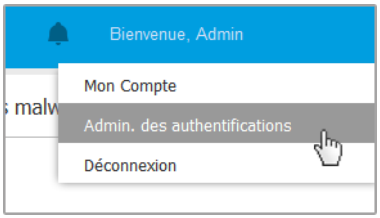
1. Se connecter à la plate-forme de virtualisation
2. Installer Security Server sur les hôtes

Connexion à la plate-forme de virtualisation

Pour accéder à l'infrastructure virtualisée intégrée à la Control Center, vous devez indiquer vos identifiants utilisateur pour chaque système de serveur de virtualisation disponible. Le Control Center utilise vos identifiants pour se connecter à l'infrastructure virtualisée, en affichant uniquement les ressources auxquelles vous avez accès (en fonction de ce qui est défini dans vCenter Server).

Pour spécifier les identifiants pour se connecter aux systèmes serveurs de virtualisation :

1. Cliquez sur votre nom d'utilisateur dans l'angle supérieur droit de la page et sélectionnez **Admin. des authentifications**.



Le menu Réseau > Packages

2. Allez dans l'onglet **Environnement Virtuel**.
3. Spécifiez les informations d'authentification requises.
   a. Sélectionnez un serveur dans le menu correspondant.

Note
Si le menu n'est pas disponible, c'est que l'intégration n'a pas encore été configurée ou que tous les authentifiants requis ont déjà été configurés.

b. Saisissez votre nom d'utilisateur et votre mot de passe ainsi qu'une description explicite.

c. Cliquez sur le bouton ⊕ **Ajouter**. Le nouveau jeu d'authentifiants apparaît dans le tableau.

Note
Si vous n'avez pas précisé vos informations d'authentification, on vous demandera de les saisir lorsque vous tenterez de parcourir l'inventaire de tout système vCenter Server. Les authentifiants que vous avez indiqués sont enregistrés dans votre Administrateur des authentifications afin que vous n'ayez pas besoin de les saisir la prochaine fois.

Installation de Security Server sur les hôtes

Vous devez installer Security Server sur les hôtes de la manière suivante :

- Dans les environnements VMware avec vShield Endpoint, vous devez installer l'appliance spécialement conçue sur tous les hôtes à protéger. Toutes les machines virtuelles d'un hôte sont automatiquement connectées via vShield Endpoint à l'instance du Security Server installée sur cet hôte.
- Dans les environnements Nutanix Prism Element, vous devez installer le Security Server sur chaque hôte, via la tâche d'installation à distance.
- Dans tous les autres environnements, vous devez installer Security Server sur un ou plusieurs hôtes en fonction du nombre de machines virtuelles à protéger. Vous devez prendre en compte le nombre de machines virtuelles protégées, les ressources disponibles pour Security Server sur les hôtes, ainsi que la connectivité réseau entre le Security Server et les machines virtuelles protégées. L'agent de sécurité installé sur les machines virtuelles se connecte au Security Server via TCP/IP, à l'aide des informations configurées lors de l'installation ou via une politique.

Si le Control Center est intégré à vCenter Server, XenServer et Nutanix Prism Element, vous pouvez déployer automatiquement Security Server sur les hôtes à partir du Control Center. Vous pouvez également télécharger les packages de Security Server pour une installation autonome à partir du Control Center.

Note
Pour les environnements VMware avec vShield Endpoint, vous pouvez déployer Security Server sur les hôtes exclusivement avec des tâches d'installation.

Installation locale

Dans tous les environnements virtualisés qui ne sont pas intégrés au Control Center, vous devez installer le Security Server sur les hôtes manuellement, à l'aide d'un package d'installation. Le package du Security Server peut être téléchargé à partir du Control Center dans différents formats compatibles avec les principales plateformes de virtualisation.

Téléchargement des packages d'installation du Security Server :

Pour télécharger des packages d'installation du Security Server :

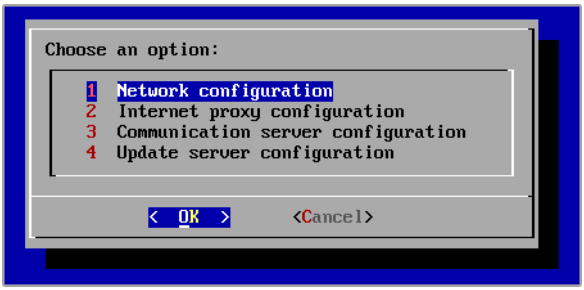
1. Accédez à la page **Réseau > Packages**.
2. Sélectionnez le package du Security Server par défaut.
3. Cliquez sur le bouton **Télécharger** en haut du tableau et sélectionnez le type de package dans le menu.
4. Enregistrez le package sélectionné à l'emplacement de votre choix.

Déploiement des packages d'installation du Security Server :

Lorsque vous avez le package d'installation, déployez-le sur l'hôte à l'aide de l'outil de déploiement de machines virtuelles de votre choix.

Après le déploiement, configurez le Security Server de la façon suivante :

1. Accédez à la console de l'appliance à partir de votre outil de gestion de la virtualisation (par exemple, vSphere Client). Vous pouvez également vous connecter à l'appliance via SSH.
2. Connectez-vous avec les identifiants par défaut.
   - Nom d'utilisateur : `root`
   - Mot de passe : `sve`
3. Exécutez la commande `sva-setup`. Vous accéderez à l'interface de configuration de l'appliance.



Interface de configuration de Security Server (menu principal)

Pour naviguer entre les menus et les options, utilisez l'`Onglet` et les flèches. Pour sélectionner une option spécifique, appuyez sur `Entrée`.

4. Configurez les paramètres du réseau.

   Security Server utilise le protocole TCP/IP pour communiquer avec les autres composants de GravityZone. Vous pouvez configurer l'appliance afin qu'elle obtienne automatiquement les paramètres du réseau à partir du serveur DHCP ou configurer manuellement les paramètres du réseau, comme indiqué ci-après :

   a. Dans le menu principal, sélectionnez **Configuration du réseau**.

   b. Sélectionnez l'interface réseau.

   c. Sélectionnez le mode de configuration de l'IP :

      - **DHCP**, si vous souhaitez que le Security Server obtienne automatiquement les paramètres réseau du serveur DHCP.
      - **Statique**, si un serveur DHCP est absent ou si une réservation de l'IP d'une appliance a été effectuée sur le serveur DHCP. Dans ce cas, vous devez configurer manuellement les paramètres du réseau.

        i. Indiquez le nom d'hôte, l'adresse IP, le masque de réseau, la passerelle et les serveurs DNS dans les champs correspondants.

        ii. Sélectionnez **OK** pour enregistrer les modifications.

Note
Si vous êtes connecté à l'appliance via un client SSH, modifier les paramètres réseau fermera immédiatement votre session.

5. Configurez les paramètres du proxy.

   Si un serveur proxy est utilisé dans le réseau, vous devez indiquer ses informations afin que le Security Server puisse communiquer avec GravityZone Control Center.

   Note
   Seuls les proxy avec l'authentification de base sont pris en charge.

   a. Dans le menu principal, sélectionnez **Configuration du proxy Internet**.
   b. Indiquez le nom d'hôte, le nom d'utilisateur, le mot de passe et le domaine dans les champs correspondants.
   c. Sélectionnez **OK** pour enregistrer les modifications.

6. Configurez l'adresse du serveur de communication.
   a. Dans le menu principal, sélectionnez **Configuration du serveur de communication**.
   b. Saisissez l'adresse du Serveur de Communication, dont le numéro de port 8443, au format suivant :

      ```
      https://Communication-Server-IP:8443
      ```

      Vous pouvez également utiliser le nom d'hôte du serveur de communication au lieu de l'adresse IP.
   c. Sélectionnez **OK** pour enregistrer les modifications.

Installation à distance

Le Control Center vous permet d'installer à distance Security Server sur les hôtes visibles en utilisant des tâches d'installation.

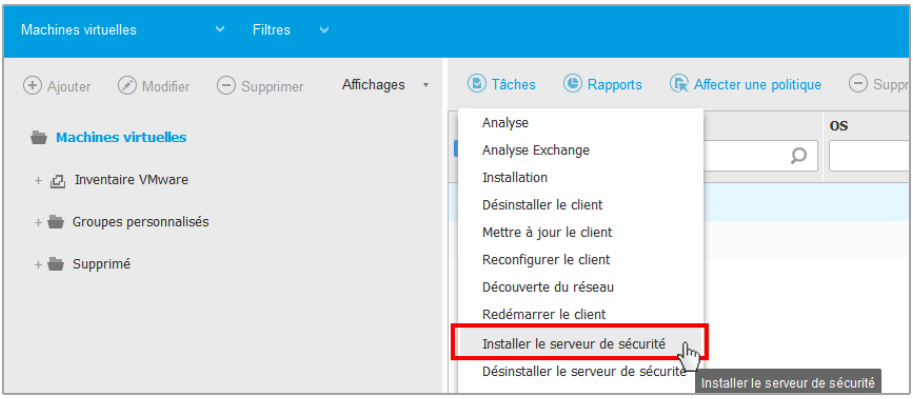
Pour installer Security Server à distance sur un ou plusieurs hôtes :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Machines virtuelles** dans le sélecteur d'affichage.
3. Parcourez l'inventaire VMware, Citrix ou Nutanix et cochez les cases correspondant aux hôtes ou conteneurs souhaités (Nutanix Prism, vCenter Server, XenServer ou datacenter). Pour une sélection rapide, vous pouvez sélectionner directement le conteneur root (Inventaire Nutanix, Inventaire

VMware ou Inventaire Citrix). Pour pourrez sélectionner les hôtes individuellement à partir de l'assistant d'installation.

Note
Vous ne pouvez pas sélectionner les hôtes de différents dossiers.

4. Cliquez sur le bouton **Tâches** en haut du tableau et sélectionnez **Installer Security Server** dans le menu. La fenêtre **installation de Security Server** s'affiche.



Installer Security Server à partir du menu Tâches

5. Sélectionnez les hôtes sur lesquels vous souhaitez installer les instances de Security Server.
6. Sélectionnez les paramètres de configuration que vous souhaitez utiliser.

Important
Utiliser des paramètres communs tout en déployant plusieurs instances Security Server simultanément nécessite que les hôtes partagent le même emplacement de stockage, aient leurs adresses IP affectées par un serveur DHCP et fassent partie du même réseau.

Si vous choisissez de configurer chaque Security Server différemment, vous pourrez définir les paramètres de votre choix pour chaque hôte à l'étape suivante de l'assistant. Les étapes indiquées ici s'appliquent dans le cas où l'option **Configurer chaque Security Server** est utilisée.

7. Cliquez sur **Suivant**.
8. Indiquez un nom explicite pour le Security Server.
9. Pour les environnements VMware, sélectionnez l'emplacement dans lequel vous souhaitez inclure le Security Server à partir du menu **Dossier de déploiement**.
10. Sélectionnez l'emplacement de stockage de destination.
11. Choisissez le type d'allocation d'espace disque. Il est recommandé de déployer l'appliance en utilisant l'allocation d'espace disque fixe.

    Important
    Si vous utilisez une allocation d'espace disque dynamique et que l'espace disque de la banque de données vient à manquer, le Security Server se bloquera, et l'hôte demeurera, par conséquent, non protégé.

12. Configurez l'allocation de ressources mémoire et processeur en fonction du ratio de consolidation de la VM sur l'hôte. Sélectionnez **Faible**, **Moyen** ou **Élevé** pour charger les paramètres d'allocation de ressources recommandés ou sur **Manuel** pour configurer l'allocation de ressources manuellement.
13. Vous devez définir un mot de passe administrateur pour la console Security Server. Définir un mot de passe d'administration écrase le mot de passe root par défaut (« sve »).
14. Configurez le fuseau horaire de l'appliance.
15. Sélectionnez le type de configuration réseau pour le réseau Bitdefender. L'adresse IP du Security Server ne doit pas changer puisqu'elle est utilisée par les agents Linux pour la communication.

    Si vous choisissez DHCP, veillez à configurer le serveur DHCP afin qu'il réserve une adresse IP à cette appliance.

    Si vous choisissez "statique", vous devez indiquer l'adresse IP, le masque de sous-réseau, la passerelle et les informations de DNS.
16. Sélectionnez le réseau vShield et saisissez les identifiants vShield. L'étiquette par défaut du réseau vShield est `vmservice-vshield-pg`.
17. Cliquez sur **Enregistrer**.

Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**.

Note
Pour mettre à niveau VMWare vShield vers NSX, référez-vous à cet article de support.

Important
L'installation de Security Server sur Nutanix par le biais de la tâche d'installation à distance peut échouer si le cluster Prism Element est enregistré dans Prism Central ou pour une autre raison. Dans ces situations, il est recommandé de réaliser un déploiement manuel de Security Server. Pour plus d'informations, consultez cet article de la base de connaissances :

Installation du Security Server sur Amazon EC2

Vous pouvez utiliser Security Server pour protéger vos instances Amazon EC2, en procédant de la manière suivante :

- Configurez le Security Server installé sur votre réseau local pour qu'il communique avec les instances Amazon EC2. Vous pourrez ainsi utiliser vos ressources locales, physiques ou virtuelles, pour protéger également votre inventaire EC2.
- Installez une ou plusieurs instances du Security Server dans votre environnement Amazon EC2, en fonction de vos besoins. Pour cela, suivez les instructions de cet article de la base de connaissances.

Important

- Pour que vos machines EC2 et les instances du Serveur de sécurité installées dans votre inventaire Amazon EC2 communiquent, vous devez configurer correctement vos connexions Amazon VPC (Virtual Private Cloud) et Amazon VPN. Pour plus d'informations, consultez la documentation sur les VPC Amazon.
- Nous vous recommandons d'installer le Security Server dans la région Amazon EC2 où se trouve les instances que vous voulez protéger.

Le mode d'analyse par défaut des instances EC2 est l'analyse locale (le contenu de sécurité est stockées dans l'agent de sécurité installé et l'analyse est exécutée localement sur la machine). Pour analyser vos instances EC2 à l'aide d'un Security Server, vous devez configurer le package d'installation de l'agent de sécurité et la politique appliquée en conséquence.

Installer Security Server pour Microsoft Azure

Vous pouvez utiliser Security Server pour protéger vos machines virtuelles Microsoft Azure de la manière suivante :

- Configurez le Security Server installé sur votre réseau local pour qu'il communique avec les machines virtuelles Microsoft Azure. Vous pourrez ainsi utiliser vos ressources locales, physiques ou virtuelles, pour protéger également l'inventaire Microsoft Azure.
- Installez une ou plusieurs instances du Security Server dans votre environnement Microsoft Azure, en fonction de vos besoins. Pour cela, suivez les instructions de cet article de la base de connaissances.

Important

- Pour que la communication entre vos machines virtuelles Microsoft Azure et les instances du Serveur de sécurité installées dans votre inventaire Microsoft Azure fonctionne, vous devez configurer correctement votre réseau/sous-réseau virtuel. Pour plus d'informations, reportez-vous à la Documentation sur le réseau virtuel Microsoft Azure.
- Nous vous recommandons d'installer le Security Server dans la même région Microsoft Azure que celle où se trouvent les machines virtuelles que vous souhaitez protéger.

Le mode d'analyse par défaut des machines virtuelles Microsoft Azure est l'analyse locale (le contenu de sécurité est stocké dans l'agent de sécurité installé et l'analyse est exécutée localement sur la machine). Pour analyser vos machines virtuelles Microsoft Azure à l'aide d'un Security Server, vous devez configurer le package d'installation de l'agent de sécurité et la politique appliquée en conséquence.

5.3.2. Installation des agents de sécurité

Pour protéger vos endpoints physiques et virtuels, vous devez installer un agent de sécurité sur chacun d'entre eux. Outre la gestion de la protection sur l'endpoint local, l'agent de sécurité communique également avec Control Center pour recevoir les commandes de l'administrateur et envoyer les résultats de ses actions.

Pour en savoir plus à propos des agents de sécurité, veuillez vous référer à « Agents de sécurité » (p. 11).

Sur les machines Windows et Linux, l'agent de sécurité peut avoir deux rôles, et vous pouvez l'installer comme suit :

1. En tant que simple agent de sécurité pour vos endpoints.
2. En tant que Relais, servant d'agent de sécurité et de serveur de communication, proxy et de mise à jour aux autres endpoints du réseau.

Vous pouvez installer les agents de sécurité sur des endpoints physiques et virtuels en exécutant des packages d'installation localement ou en exécutant des tâches d'installation à distance depuis Control Center.

Merci de lire attentivement et de respecter les instructions avant de préparer l'installation.

En mode normal, les agents de sécurité ont une interface utilisateur minimale. Il permet uniquement aux utilisateurs de consulter l'état de la protection et d'exécuter des tâches de sécurité de base (mises à jour et analyses) sans fournir d'accès aux paramètres.

Si l'administrateur réseau l'a permis via le package d'installation et la politique de sécurité, l'agent de sécurité peut également s'exécuter en mode Power User sur les endpoints Windows, ce qui autorise l'utilisateur de l'endpoint à afficher et modifier les paramètres de politique. Cependant, l'administrateur de Control Center peut toujours contrôler quels paramètres de politique s'appliquent, en écrasant le mode Power User.

Par défaut, la langue d'affichage de l'interface utilisateur sur les endpoints Windows protégés est définie au moment de l'installation en fonction de la langue de votre compte GravityZone.

Sur Mac, la langue d'affichage de l'interface utilisateur est définie au moment de l'installation en fonction de la langue du système d'exploitation de l'endpoint. Sur Linux, l'agent de sécurité ne possède pas d'interface utilisateur localisée.

Pour installer l'interface utilisateur dans une autre langue sur certains endpoints Windows, vous pouvez créer un package d'installation et définir la langue de votre choix dans ses options de configuration. Cette option n'est pas disponible pour les endpoints Mac et Linux. Pour plus d'informations sur la création de packages d'installation, reportez-vous à « Créer des packages d'installation » (p. 131).

Préparation de l'Installation

Avant l'installation, suivez ces étapes préparatoires pour vous assurer de son bon déroulement :

1. Vérifiez que les endpoints cibles disposent de la configuration système minimale requise. Pour certains endpoints, vous pouvez avoir besoin d'installer le dernier

service pack du système d'exploitation disponible ou de libérer de l'espace disque. Établissez une liste d'endpoints ne correspondant pas aux critères nécessaires afin de pouvoir les exclure de l'administration.

2. Désinstallez (ne vous contentez pas de désactiver) tout logiciel antimalware ou de sécurité Internet sur les endpoints cibles. Faire fonctionner simultanément l'agent de sécurité avec d'autres logiciels de sécurité installés sur un endpoint peut affecter leur fonctionnement et causer d'importants problèmes avec le système.

   Un grand nombre de programmes de sécurité incompatibles sont automatiquement détectés et supprimés au moment de l'installation.

   Pour plus d'informations et pour vérifier la liste du logiciel de sécurité détecté par Bitdefender Endpoint Security Tools pour les systèmes d'exploitation Windows actuels, reportez-vous à cet article de la base de connaissances.

   Important
   Si vous voulez déployer l'agent de sécurité sur un ordinateur sur lequel Bitdefender Antivirus for Mac 5.X est déjà installé, vous devez d'abord désinstaller celui-ci manuellement. Pour les instructions, veuillez vous référer à l'article de support.

3. L'installation requiert des privilèges d'administration et un accès à Internet. Si les endpoints cibles sont dans un domaine Active Directory, vous devriez utiliser des identifiants d'administrateur de domaine pour une installation à distance. Autrement, assurez-vous de disposer des identifiants nécessaires pour tous les endpoints.
4. Les endpoints doivent avoir une connectivité réseau avec l'appliance GravityZone.
5. Il est recommandé d'utiliser une adresse IP statique pour le serveur relais. Si vous ne configurez pas d'adresse IP statique, utilisez le nom d'hôte de la machine.
6. Lors du déploiement de l'agent via un relais Linux, les conditions additionnelles suivantes doivent être respectées :

   - L'endpoint relais doit avoir installé le package Samba (`smbclient`) version 4.1.0 ou supérieure et la procédure binaire/commande `net` pour déployer des agents Windows.

     Note
     La procédure binaire/commande `net` est habituellement contenue dans les packages samba-client et/ou samba-common. Sur certaines distributions

Linux (telles que CentOS 7.4), la commande `net` est uniquement installée lors de l'installation de la suite Samba complète (Common + Client + Server). Assurez-vous que la commande `net` est disponible sur votre endpoint relais.

- Le Partage administratif et le Partage réseau des endpoints cibles sous Windows doivent être activés.
- SSH doit être activé pour les endpoints Linux et Mac cibles.

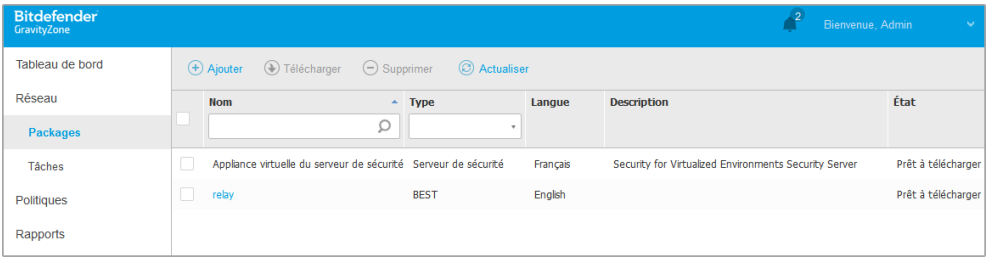
7. À partir de macOS High Sierra (10.13), après avoir installé Endpoint Security for Mac manuellement ou à distance, les utilisateurs sont invités à approuver les extensions de noyau Bitdefender sur leurs ordinateurs. Tant que les utilisateurs n'auront pas approuvé les extensions de noyau Bitdefender, certaines fonctionnalités de Endpoint Security for Mac ne fonctionneront pas. Afin d'éviter l'intervention des utilisateurs, vous pouvez pré-approuver les extensions de noyau Bitdefender en les inscrivant sur une liste blanche à l'aide d'un outil de gestion des appareils mobiles.
8. Lorsque vous déployez l'agent dans un inventaire Amazon EC2, configurez les groupes de sécurité associés aux instances que vous voulez protéger dans le **Tableau de bord Amazon EC2 > Réseau & Sécurité** :
   - Pour l'installation à distance, autorisez l'accès SSH* depuis l'instance EC2.
   - Pour l'installation locale, autorisez l'accès SSH* et par protocole RDP (Remote Desktop Protocol) sur l'ordinateur depuis lequel vous vous connectez.

   * Pour l'installation à distance sur des instances Linux, vous devez autoriser la connexion SSH à l'aide d'un nom d'utilisateur et d'un mot de passe.
9. Lorsque vous déployez l'agent dans un inventaire Microsoft Azure :
   - La machine virtuelle cible doit se trouver sur le même réseau virtuel que l'appliance GravityZone.
   - La machine virtuelle cible doit se trouver sur le même réseau virtuel qu'un Relais, qui communique avec l'appliance GravityZone lorsque celle-ci se trouve sur un autre réseau.

Installation locale

Il est possible d'installer l'agent de sécurité sur un endpoint en exécutant un package d'installation en local.

Vous pouvez créer et gérer des packages d'installation sur la page **Réseau > Packages**.



La page Packages

Une fois le premier client installé, il sera utilisé pour détecter d'autres endpoints du même réseau, à partir de la fonction Network Discovery. Pour plus d'informations sur la fonction Network Discovery, merci de vous référer à « Fonctionnement de Network Discovery » (p. 150).

Pour installer l'agent de sécurité en local sur un endpoint, procédez comme suit :

1. Créez un package d'installation en fonction de vos besoins.

   Note
   Cette étape n'est pas obligatoire si un package d'installation a déjà été créé pour le réseau sous votre compte.

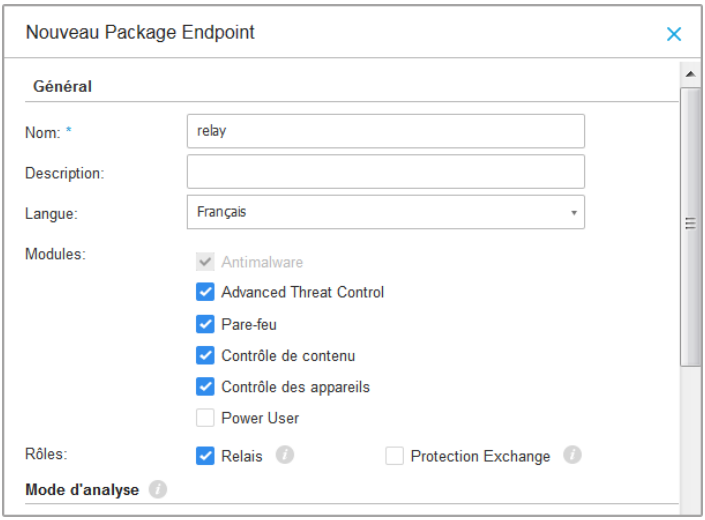
2. Téléchargez le package d'installation sur l'endpoint cible.

   Vous pouvez également envoyer les liens de téléchargement du package d'installation par e-mail à plusieurs utilisateurs de votre réseau.
3. Exécutez le package d'installation sur l'endpoint cible.

Créer des packages d'installation

Pour créer un package d'installation :

1. Connectez-vous et identifiez-vous sur le Control Center.
2. Accédez à la page **Réseau > Packages**.
3. Cliquez sur le bouton **Ajouter** en haut du tableau. Une fenêtre de configuration s'affichera.



Créer des packages - Options

4. Indiquez un nom et une description explicites pour le package d'installation que vous souhaitez créer.
5. Dans le champ **Langue**, sélectionnez la langue souhaitée pour l'interface du client.

> **Note**
> Cette option n'est disponible que pour les systèmes d'exploitation Windows.

6. Sélectionnez les modules de protection que vous voulez installer.

> **Note**
> Seuls les modules pris en charge pour chaque système d'exploitation seront installés. Pour plus d'informations, reportez-vous à « Agents de sécurité » (p. 11).

7. Sélectionnez le rôle de l'endpoint cible :
   - **Relais**, pour créer le package d'un endpoint avec le rôle Relais. Pour plus d'informations, reportez-vous à « Relais » (p. 12)

- **Serveur cache du module Gestion des patchs**, pour faire du Relais un serveur interne pour la distribution des patchs logiciels. Ce rôle est affiché lorsque le rôle de relais est sélectionné. Pour plus d'informations, reportez-vous à « Serveur de mise en cache des patchs » (p. 13)
- **Protection Exchange**, pour installer les modules de protection pour les Serveurs Microsoft Exchange Servers, y compris l'antimalware, l'antispam, le filtrage de contenu et des pièces jointes pour le trafic de messagerie Exchange et l'analyse antimalware à la demande des bases de données Exchange. Pour plus d'informations, reportez-vous à « Installer la protection Exchange » (p. 160).

8. **Suppression des concurrents**. Il est recommandé de laisser cette case cochée pour supprimer automatiquement tout logiciel de sécurité incompatible pendant que l'agent Bitdefender s'installe sur l'endpoint. En sélectionnant cette option, l'agent Bitdefender s'installera en plus de la solution de sécurité existante. Vous pouvez supprimer manuellement la solution de sécurité précédemment installée dans un second temps, à vos propres risques.

   Important
   Faire fonctionner simultanément l'agent de Bitdefender avec d'autres logiciels de sécurité installés sur un endpoint peut affecter leur fonctionnement et causer d'importants problèmes avec le système.

9. **Mode d'analyse**. Choisissez la technologie d'analyse qui correspond le mieux à votre environnement réseau et aux ressources de vos endpoints. Vous pouvez définir le mode d'analyse en sélectionnant l'un des types suivants :
   - **Automatique**. Dans ce cas, l'agent de sécurité détectera automatiquement la configuration de l'endpoint et adaptera la technologie d'analyse en conséquence :
     - Analyse centralisée dans le cloud public ou privé (avec Security Server), avec une analyse hybride de secours (Moteurs légers) pour les ordinateurs physiques peu performants et pour les machines virtuelles. Ce cas nécessite le déploiement d'au moins un Security Server dans le réseau.
     - Analyse locale (avec des moteurs complets) pour les ordinateurs physiques très performants.

– Analyse locale pour les instances EC2 et les machines virtuelles Microsoft Azure.

> **Note**
> On considère comme ordinateurs a faibles performances ceux ayant une fréquence de processeur inférieure à 1,5 GHz, ou moins de 1 Go de mémoire vive.

- **Paramètres**. Vous pouvez dans ce cas configurer le mode d'analyse en choisissant entre plusieurs technologies d'analyse pour les machines physiques et virtuelles :
  – Analyse centralisée dans le cloud public ou privé (avec Security Server), avec en solution de secours* une analyse locale (avec des moteurs complets) ou une analyse hybride (avec des moteurs légers).
  – Analyse hybride (avec des moteurs légers)
  – Analyse locale (avec des moteurs complets)

  Le mode d'analyse par défaut des instances EC2 est l'analyse locale (le contenu de sécurité est stockées dans l'agent de sécurité installé et l'analyse est exécutée localement sur la machine). Pour analyser vos instances EC2 à l'aide d'un Security Server, vous devez configurer le package d'installation de l'agent de sécurité et la politique appliquée en conséquence.

  Le mode d'analyse par défaut des machines virtuelles Microsoft Azure est l'analyse locale (le contenu de sécurité est stocké dans l'agent de sécurité installé et l'analyse est exécutée localement sur la machine). Pour analyser vos machines virtuelles Microsoft Azure à l'aide d'un Security Server, vous devez configurer le package d'installation de l'agent de sécurité et la politique appliquée en conséquence.

  * Lorsqu'on utilise une analyse à double moteur, si le premier moteur n'est pas disponible, le moteur de secours est utilisé. La consommation des ressources et l'utilisation du réseau dépendront des moteurs utilisés.

  Pour plus d'informations sur les technologies d'analyse disponibles référez-vous à« Moteurs d'analyse » (p. 3)

10. **Déployer un endpoint avec vShield lorsqu'un environnement VMware intégré à vShield est détecté**. Cette option peut être utilisée lorsque le package d'installation est déployé sur une machine virtuelle d'un environnement VMware

intégré à vShield. Dans ce cas, VMware vShield Endpoint sera installé sur la machine cible au lieu de l'agent de sécurité Bitdefender.

Important
Cette option est seulement pour les déploiements à distance, pas les installations locales. Lors de l'installation locale dans un environnement VMWare intégré dans vShield, vous pouvez télécharger le package intégré dans vShield.

11. Lorsque vous personnalisez les moteurs d'analyse à l'aide de l'analyse Cloud Public ou Privé (Security Server), l'on vous demande de sélectionner les Security Server installés en local que vous souhaitez utiliser et de configurer leur priorité dans la section **Affectation du Security Server** :
    a. Cliquez sur la liste de Security Server dans l'en-tête du tableau. La liste des Security Server détectés s'affiche.
    b. Sélectionnez une entité.
    c. Cliquez sur le bouton ⊕ **Ajouter** de l'en-tête de la colonne **Actions**.
    Le Security Server est ajouté à la liste.
    d. Procédez de la même façon pour ajouter plusieurs serveurs de sécurité, si possible. Vous pouvez dans ce cas configurer leur priorité l'aide des flèches ⌃ vers le haut et ⌄ vers le bas se trouvant à droite de chaque élément. Lorsque le premier Security Server n'est pas disponible, le suivant est utilisé et ainsi de suite.
    e. Pour retirer un élément de la liste, cliquez sur le bouton ⊗ **Supprimer** correspondant en haut du tableau.

    Vous pouvez choisir de crypter la connexion à Security Server en sélectionnant l'option **Utiliser SSL**.
12. **Divers**. Vous pouvez configurer les options suivantes sur plusieurs types de fichiers en quarantaine des endpoints cibles :
    - **Soumettre des vidages sur incident**. Sélectionnez cette option afin que les fichiers de vidage mémoire soient envoyés aux Laboratoires Bitdefender afin d'y être analysés en cas de plantage de l'agent de sécurité. Les vidages sur incident aideront nos ingénieurs à découvrir la cause du problème et à éviter qu'il ne se reproduise. Aucune donnée personnelle ne sera envoyée.
    - **Envoyer les fichiers en quarantaine aux Laboratoires Bitdefender toutes les (heures)**. Par défaut, les fichiers en quarantaine sont automatiquement

envoyés aux Laboratoires Bitdefender toutes les heures. Vous pouvez modifier la fréquence d'envoi des fichiers en quarantaine. Les échantillons seront analysés par les spécialistes malwares de Bitdefender. Si la présence de malwares est confirmée, une signature est publiée afin de permettre de les supprimer.

- **Soumettre des exécutables suspects à Bitdefender**. Sélectionnez cette option afin que les fichiers qui n'ont pas l'air fiables ou qui ont un comportement suspect soient envoyés aux Laboratoires Bitdefender pour analyse.

13. Sélectionnez **Analyser avant l'installation** si vous souhaitez vous assurer que les machines sont saines avant d'y installer le client. Une analyse rapide dans le cloud sera réalisée sur les machines cibles avant de commencer l'installation.
14. Bitdefender Endpoint Security Tools est installé dans le répertoire d'installation par défaut. Sélectionnez **Utiliser le chemin d'installation personnalisé** si vous souhaitez installer l'agent de Bitdefender à un emplacement différent. Si le dossier spécifié n'existe pas, il sera créé lors de l'installation.

    - Sur Windows, le chemin par défaut est `C:\Program Files\`. Pour installer Bitdefender Endpoint Security Tools dans le dossier de votre choix, respectez la convention Windows lors de la saisie du chemin. Par exemple, `D:\dossier`.
    - Sur Linux, Bitdefender Endpoint Security Tools est installé par défaut dans le dossier `/opt`. Pour installer l'agent Bitdefender dans le dossier de votre choix, respectez la convention Linux lors de la saisie du chemin. Par exemple, `/dossier`.

      Bitdefender Endpoint Security Tools ne peut pas être installé dans les chemins personnalisés suivants :
      - Tout chemin ne commençant pas par une barre oblique (/). Seule exception : l'emplacement `%PROGRAMFILES%` de Windows, que l'agent de sécurité interprète comme le dossier par défaut de Linux : `/opt`.
      - Tout emplacement situé dans `/tmp` ou `/proc`.
      - Tout chemin contenant les caractères spéciaux suivants : `$, !, *, ?, ", ', `, \, (,), [,], {, }`.
      - Le spécificateur `systemd` (%).

Sur Linux, l'installation dans un dossier personnalisé nécessite glibc 2.21 ou supérieur.

Important
Lors de l'utilisation d'un chemin personnalisé, vérifiez que vous avec le package d'installation adapté pour chaque système d'exploitation.

15. Vous pouvez, si vous le souhaitez, définir un mot de passe pour empêcher les utilisateurs de supprimer la protection. Sélectionnez **Mot de passe de désinstallation** et indiquez le mot de passe souhaité dans les champs correspondants.
16. Si les endpoints cibles sont dans le Répertoire réseau sous **Groupes personnalisés**, vous pouvez choisir de les déplacer dans un dossier spécifié immédiatement après que le déploiement de l'agent de sécurité soit terminé.

    Sélectionnez **Utiliser dossier personnalisé** et choisissez un dossier dans le tableau correspondant.
17. Sous la section **Système de déploiement**, sélectionnez l'entité à laquelle les endpoints cibles se connecteront pour installer et mettre à jour le client :
    - L'**appliance GravityZone**, lorsque les endpoints se connecteront directement à l'appliance GravityZone.

      Dans ce cas, vous pouvez également définir :
      - Un serveur de communication personnalisé en indiquant son IP ou nom d'hôte, si nécessaire.
      - Les paramètres du proxy, si les endpoints cibles communiquent avec l'appliance GravityZone via un proxy. Dans ce cas, sélectionnez **Utiliser le proxy pour la communication** et saisissez les paramètres du proxy requis dans les champs ci-dessous.
    - **Relais Endpoint Security**, si vous souhaitez connecter les endpoints à un client relais installé dans votre réseau. Toutes les machines avec le rôle relais détectés dans votre réseau apparaîtront dans le tableau ci-dessous. Choisissez la machine relais de votre choix. Les endpoints connectés communiqueront avec Control Center uniquement via le relais spécifié.

      Important
      Le port 7074 doit être ouvert pour que le déploiement via Bitdefender Endpoint Security Tools Relay fonctionne.

18. Cliquez sur **Enregistrer**.

Le nouveau package créé sera ajouté à la liste de packages.

Note
Les paramètres configurés dans un package d'installation s'appliqueront aux endpoints immédiatement après l'installation. Dès qu'une politique sera appliquée au client, les paramètres configurés dans la politique s'appliqueront et remplaceront certains paramètres du package d'installation (comme les serveurs de communication ou les paramètres du proxy.

Téléchargement de packages d'installation

Téléchargez les packages d'installation des agents de sécurité :

1. Identifiez-vous auprès de Control Center à partir de l'endpoint sur lequel vous souhaitez installer la protection.
2. Accédez à la page **Réseau > Packages**.
3. Sélectionnez le package d'installation que vous souhaitez télécharger.
4. Cliquez sur le bouton **Télécharger** en haut du tableau et sélectionnez le type de programme d'installation que vous souhaitez utiliser. Deux types de fichiers d'installation sont disponibles :
   - **Programme de téléchargement** . Le downloader commence par télécharger le kit d'installation complet sur les serveurs cloud de Bitdefender avant de lancer l'installation. Il est peu volumineux et peut être exécuté à la fois sur les systèmes 32 et 64 bits (ce qui facilite sa distribution). Il requiert par contre une connexion active à Internet.
   - **Kit complet**. Les kits d'installation complets sont plus volumineux et doivent être exécutés sur le type de système d'exploitation spécifique.

     Le kit complet est à utiliser pour installer la protection sur les endpoints avec une connexion Internet lente ou sans connexion. Téléchargez ce fichier sur un endpoint connecté à Internet puis transmettez-le à d'autres endpoints à l'aide de supports de stockage externes ou d'un partage réseau.

     Note
     Versions du kit complet disponibles :
     - **OS Windows :** systèmes 32 et 64 bits
     - **OS Linux:** systèmes 32 et 64 bits

– **macOS :** seulement les systèmes 64-bits
Veillez à utiliser la version adaptée au système sur lequel vous l'installez.

5. Enregistrez le fichier sur l'endpoint.

Avertissement

- L'exécutable du downloader ne doit pas être renommé car il ne pourra sinon plus télécharger les fichiers d'installation à partir du serveur de Bitdefender.

6. En outre, si vous avez choisi le programme de téléchargement, vous pouvez créer un package MSI pour les endpoints Windows. Pour plus d'informations, veuillez consulter cet article KB.

Envoyer les liens de téléchargement des packages d'installation par e-mail

Vous pouvez avoir besoin d'informer rapidement d'autres utilisateurs qu'un package d'installation peut être téléchargé. Dans ce cas, suivez les étapes décrites ci-après :

1. Accédez à la page **Réseau > Packages**.
2. Sélectionnez le package d'installation que vous souhaitez.
3. Cliquez sur le bouton **Envoyer le lien de téléchargement** en haut du tableau. Une fenêtre de configuration s'affichera.
4. Indiquez l'adresse e-mail de chaque utilisateur à qui vous souhaitez envoyer le lien de téléchargement du package d'installation. Appuyez sur `Entrée` après chaque e-mail.

   Veuillez vérifier que chaque adresse e-mail indiquée est valide.
5. Si vous souhaitez afficher les liens de téléchargement avant de les envoyer par e-mail, cliquez sur le bouton **Liens d'installation**.
6. Cliquez sur **Envoyer**. Un e-mail contenant le lien d'installation est envoyé à chaque adresse e-mail spécifiée.

Exécution de packages d'installation

Pour que l'installation fonctionne, le package d'installation doit être lancé à l'aide des privilèges administrateur.

Le package s'installe différemment sur chaque système d'exploitation, comme suit :

- Sur les systèmes d'exploitation Windows et macOS :
  1. Sur l'endpoint cible, téléchargez le dossier d'installation à partir de la Control Center ou copiez-le à partir d'un réseau de partage.
  2. Si vous avez téléchargé le kit complet, extraire les fichiers à partir des archives.
  3. Exécutez le Fichier Exécutable.
  4. Suivez les instructions à l'écran.

  Note
  Sur macOS, après avoir installé Endpoint Security for Mac, les utilisateurs sont invités à approuver les extensions de noyau Bitdefender sur leurs ordinateurs. Tant que les utilisateurs n'auront pas approuvé les extensions de noyau Bitdefender, certaines fonctionnalités de l'agent de sécurité ne fonctionneront pas. Pour plus d'informations, consultez cet article de la base de connaissances :

- Sur les systèmes d'exploitation Linux :
  1. Connectez-vous et identifiez-vous sur le Control Center.
  2. Téléchargez ou copiez le package d'installation sur l'endpoint cible.
  3. Si vous avez téléchargé le kit complet, extraire les fichiers à partir des archives.
  4. Obtenez des privilèges root, en exécutant la commande `sudo su`.
  5. Changez les permissions du dossier d'installation afin de pouvoir l'exécuter :

     ```
     # chmod +x installer
     ```

  6. Exécutez le fichier d'installation :

     ```
     # ./installer
     ```

7. Pour vérifier que l'agent a bien été installé sur l'endpoint, exécutez cette commande :

```
$ service bd status
```

Une fois l'agent de sécurité installé, l'endpoint apparaît comme étant administré dans Control Center (page **Réseau**) après quelques minutes.

Important
Si vous utilisez le système VMware Horizon View Persona Management, nous vous conseillons de configurer la politique de groupe Active Directory de manière à exclure les processus suivants de Bitdefender (sans indiquer le chemin complet) :

- `bdredline.exe`
- `epag.exe`
- `epconsole.exe`
- `epintegrationservice.exe`
- `epprotectedservice.exe`
- `epsecurityservice.exe`
- `epupdateservice.exe`
- `epupdateserver.exe`

Ces exclusions doivent s'appliquer tant que l'agent de sécurité s'exécute sur le endpoint. Pour plus d'informations, consultez cette page de la documentation VMware Horizon.

Installation à distance

Control Center vous permet d'installer à distance l'agent de sécurité sur les endpoints dans les environnements intégrés dans Control Center et autres endpoints détectés dans le réseau en utilisant des tâches d'installation. Dans les environnements VMWare, l'installation à distance se base sur les outils VMWare, alors que pour les environnements Citrix XenServer et Nutanix Prism Element, elle se base sur les partages administratifs Windows et sur SSH.

Une fois l'agent de sécurité installé sur un endpoint, quelques minutes peuvent être nécessaires pour que les autres endpoints du réseau deviennent visibles dans Control Center.

Bitdefender Endpoint Security Tools comprend un mécanisme de découverte du réseau automatique qui lui permet de détecter les endpoints qui ne sont pas dans

Active Directory. Les endpoints détectés apparaissent comme étant **non administrés** sur la page **Réseau**, dans l'affichage **Ordinateurs**, sous **Groupes personnalisés**. Control Center supprime automatiquement les endpoints Active Directory de la liste des endpoints détectés.

Pour activer la découverte du réseau, Bitdefender Endpoint Security Tools doit être déjà installé sur au moins un endpoint du réseau. Cet endpoint sera utilisé pour analyser le réseau et installer Bitdefender Endpoint Security Tools sur les endpoints non protégés.

Pour plus d'informations sur la fonction Network Discovery, merci de vous référer à « Fonctionnement de Network Discovery » (p. 150).

Configuration requise pour l'installation à distance

Pour que l'installation à distance fonctionne :

- Sous Windows:
  - Le partage administratif `admin$` doit être activé. Configurez chaque poste de travail cible afin qu'il n'utilise pas le partage de fichiers avancé.
  - Configurer le Contrôle de compte d'utilisateur (UAC) en fonction du système d'exploitation présent sur les endpoints cibles. Si les endpoints sont dans un domaine Active Directory, vous pouvez utiliser une politique de groupe pour configurer le Contrôle de compte d'utilisateur. Pour plus d'informations, consultez cet article de la base de connaissances :
  - Désactivez le pare-feu Windows ou configurez-le pour autoriser le trafic au moyen du protocole de Partage de fichiers et d'imprimantes.

  Note
  Le déploiement à distance ne fonctionne que sur les systèmes d'exploitation modernes, à partir de Windows 7 / Windows Server 2008 R2, pour lesquels Bitdefender propose une assistance complète. Pour plus d'informations, reportez-vous à « Systèmes d'exploitation pris en charge » (p. 26).

- Sur Linux : SSH doit être activé.
- Sur macOS : la connexion à distance et le partage de fichiers doivent être activés.

Exécution de tâches d'installation à distance

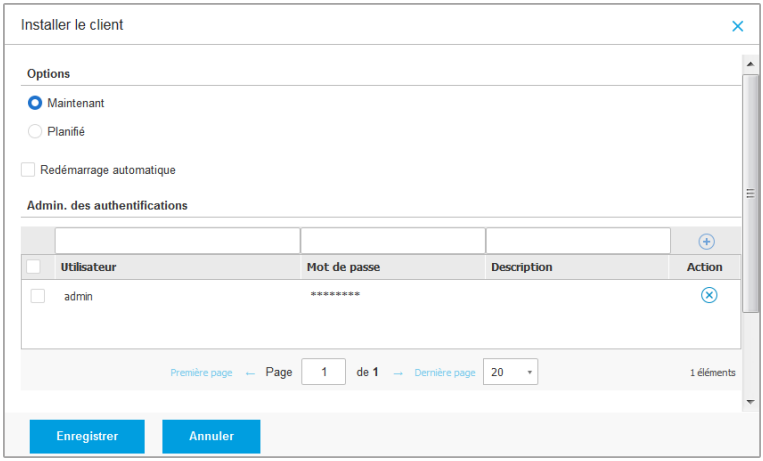
Pour exécuter une tâche d'installation à distance :

1. Connectez-vous et identifiez-vous sur le Control Center.
2. Allez sur la page **Réseau**.
3. Sélectionnez **Ordinateur / Machine virtuelle** dans le sélecteur d'affichage.
4. Sélectionnez le groupe souhaité dans le panneau de gauche. Les entités contenues dans le groupe sélectionné apparaissent dans le tableau du panneau de droite.

   Note
   Vous pouvez aussi appliquer des filtres pour afficher uniquement les endpoints non administrés. Cliquez sur le menu **Filtres** et sélectionnez les options suivantes : **Non administré** dans l'onglet **Sécurité** et **Tous les éléments de manière récurrente** dans l'onglet **Profondeur**.

5. Sélectionnez les entités (endpoints ou groupes d'endpoints) sur lesquelles vous souhaitez installer la protection.
6. Cliquez sur le bouton **Tâches** en haut du tableau et sélectionnez **Installer**

   L'assistant **Installer le client** apparaît.



Installer Bitdefender Endpoint Security Tools à partir du menu des Tâches

7. Configurez l'heure d'installation dans la section **Options** :

- **Maintenant**, afin de lancer immédiatement le déploiement.
- **Planifié**, afin de planifier un déploiement à intervalle régulier. Dans ce cas, sélectionnez le temps d'intervalle désiré (par heure, par jour ou par semaine) et configurez le selon vos besoin.

  Note
  Par exemple, lorsque certaines opérations sont nécessaires sur une machine cible avant l'installation du client (comme désinstaller d'autres logiciels et redémarrer l'OS), vous pouvez planifier les tâches de déploiement afin qu'elle s'exécute toutes les deux heures. La tâche va commencer sur chacune des cibles toutes les deux heures jusqu'à ce que déploiement soit un succès.

8. Si vous souhaitez que les endpoints cibles redémarrent automatiquement pour terminer l'installation, sélectionnez **Redémarrer automatiquement (si nécessaire)**.
9. Dans la section **Admin. des authentifications**, indiquez les identifiants d'administration requis pour l'authentification à distance sur les endpoints sélectionnés. Vous pouvez ajouter les identifiants en saisissant l'utilisateur et le mot de passe de tous les systèmes d'exploitation cibles.

   Important
   Pour les postes de travail Windows 8.1, vous devez indiquer les identifiants du compte administrateur intégré ou d'un compte administrateur de domaine. Pour en savoir plus, reportez-vous à cet article KB.

   Pour ajouter les identifiants du système d'exploitation requis :

   a. Saisissez le nom d'utilisateur et le mot de passe d'un compte administrateur dans les champs correspondants à partir de l'en-tête.

      Si les ordinateurs sont dans un domaine, il suffit d'indiquer les identifiants de l'administrateur du domaine.

      Utilisez les conventions Windows lorsque vous saisissez le nom (d'un compte utilisateur).

      - pour les machines Active Directory, utilisez ces syntaxes : `username@domain.com` and `domain\username`. Pour vous assurer que les identifiants saisis fonctionneront, ajoutez-les dans les deux formes (`username@domain.com` et `domain\username`).

- Pour les machines Workgroup, il suffit de saisir le nom d'utilisateur, sans le nom du groupe de travail.

Vous pouvez également ajouter une description qui vous aidera à identifier chaque compte plus facilement.

b. Cliquez sur le bouton ⊕ **Ajouter**. Le compte est ajouté à la liste des identifiants.

> **Note**
> Les identifiants spécifiés sont enregistrés automatiquement dans votre Administrateur des authentifications afin que vous n'ayez pas à les saisir la prochaine fois. Pour accéder à l'Administrateur des authentifications, pointez simplement sur votre nom d'utilisateur dans l'angle supérieur droit de la console.

> **Important**
> Si les identifiants indiqués ne sont pas valides, le déploiement du client échouera sur les endpoints correspondants. Veillez à mettre à jour les identifiants du système d'exploitation saisis dans l'Administrateur des authentifications lorsque ceux-ci sont modifiés sur les endpoints cibles.

10. Cochez les cases correspondant aux comptes que vous souhaitez utiliser.

> **Note**
> Un message d'avertissement s'affiche tant que vous n'avez sélectionné aucun identifiant. Cette étape est obligatoire pour installer à distance l'agent de sécurité sur les endpoints.

11. Sous la section **Système de déploiement**, sélectionnez l'entité à laquelle les endpoints cibles se connecteront pour installer et mettre à jour le client :

- L'**appliance GravityZone**, lorsque les endpoints se connecteront directement à l'appliance GravityZone.

  Dans ce cas, vous pouvez également définir :

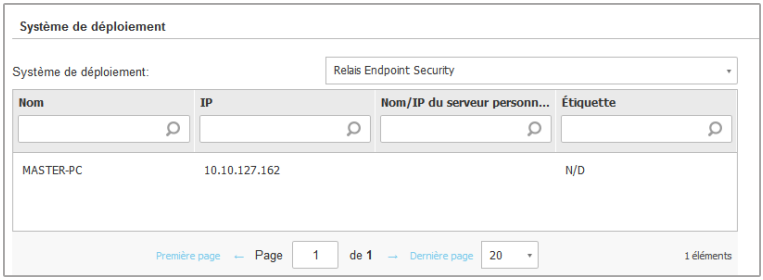
  – Un serveur de communication personnalisé en indiquant son IP ou nom d'hôte, si nécessaire.

  – Les paramètres du proxy, si les endpoints cibles communiquent avec l'appliance GravityZone via un proxy. Dans ce cas, sélectionnez **Utiliser**

le proxy pour la communication et saisissez les paramètres du proxy requis dans les champs ci-dessous.

- **Relais Endpoint Security**, si vous souhaitez connecter les endpoints à un client relais installé dans votre réseau. Toutes les machines avec le rôle relais détectés dans votre réseau apparaîtront dans le tableau ci-dessous. Choisissez la machine relais de votre choix. Les endpoints connectés communiqueront avec Control Center uniquement via le relais spécifié.

  Important
  Le port 7074 doit être ouvert pour que le déploiement via l'agent relais fonctionne.



12. Utilisez la section **Cibles supplémentaires** si vous souhaitez déployer le client sur certaines machines de votre réseau qui n'apparaissent pas dans l'inventaire du réseau. Développez la section et saisissez les adresses IP ou les noms d'hôtes de ces machines dans le champ prévu à cet effet, en les séparant par des virgules. Vous pouvez ajouter autant d'IP que nécessaire.
13. Vous devez sélectionner un package d'installation pour le déploiement actuel. Cliquez sur la liste **Utiliser le package** et sélectionnez le package d'installation de votre choix. Vous y trouverez tous les packages d'installation créés pour votre compte ainsi que le package d'installation disponible par défaut avec Control Center.
14. Si besoin, vous pouvez modifier certains paramètres du package d'installation sélectionné en cliquant sur le bouton **Personnalisé** à côté du champ **Utiliser le package**.

    Les paramètres du package d'installation apparaîtront ci-dessous et vous pouvez effectuer toutes les modifications dont vous avez besoin. Pour plus

d'informations sur la modification des packages d'installation référez-vous à « Créer des packages d'installation » (p. 131).

Si vous souhaitez enregistrer les modifications en tant que nouveau package, sélectionnez l'option **Enregistrer en tant que package** en bas de la liste des paramètres du package et indiquez un nom pour le nouveau package d'installation.

15. Cliquez sur **Enregistrer**. Une message de confirmation s'affichera.

Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**.

Important
Si vous utilisez le système VMware Horizon View Persona Management, nous vous conseillons de configurer la politique de groupe Active Directory de manière à exclure les processus suivants de Bitdefender (sans indiquer le chemin complet) :

- `bdredline.exe`
- `epag.exe`
- `epconsole.exe`
- `epintegrationservice.exe`
- `epprotectedservice.exe`
- `epsecurityservice.exe`
- `epupdateservice.exe`
- `epupdateserver.exe`

Ces exclusions doivent s'appliquer tant que l'agent de sécurité s'exécute sur le endpoint. Pour plus d'informations, consultez cette page de la documentation VMware Horizon.

Préparation des systèmes Linux pour l'analyse à l'accès

Bitdefender Endpoint Security Tools pour Linux intègre des fonctionnalités d'analyse à l'accès qui fonctionnent avec des distributions et des versions de noyaux spécifiques. Pour en apprendre plus, consultez la configuration recommandée.

Vous apprendre ensuite comment compiler manuellement le module DazukoFS.

Compiler manuellement le module DazukoFS

Veuillez suivre les étapes suivantes pour compiler DazukoFS pour la version Kernel du système puis chargez le module :

1. Téléchargez les headers du kernel correspondant.

- Sur les systèmes **Ubuntu**, lancez cette commande :

```
$ sudo apt-get install linux-headers-`uname -r`
```

- Sur les systèmes **RHEL/CentOS**, lancez cette commande :

```
$ sudo yum install kernel-devel kernel-headers-`uname -r`
```

2. Sur les systèmes **Ubuntu**, vous avez besoin de `build-essential`:

```
$ sudo apt-get install build-essential
```

3. Copiez et décompressez le code source DazukoFS dans un répertoire favori :

```
# mkdir temp
# cd temp
# cp /opt/BitDefender/share/modules/dazukofs/dazukofs-source.tar.gz
# tar -xzvf dazukofs-source.tar.gz
# cd dazukofs-3.1.4
```

4. Compilez le module :

```
# make
```

5. Installez et chargez le module :

```
# make dazukofs_install
```

Conditions requises à l'utilisation de l'analyse à l'accès avec DazukoFS

Pour que DazukoFS et l'analyse à l'accès fonctionnent ensemble, différentes conditions doivent être remplies. Veuillez vérifier que l'une des affirmations ci-dessous s'applique à votre système Linux et suivez les recommandations pour éviter les problèmes.

- La politique SELinux doit être désactivée ou réglée sur **permissive**. Pour consulter et ajuster la configuration de la politique SELinux, éditez le fichier `/etc/selinux/config`.
- Bitdefender Endpoint Security Tools est compatible exclusivement avec la version de DazukoFS incluse dans le package d'installation. Si DazukoFS est déjà installé sur le système, supprimez-le avant d'installer Bitdefender Endpoint Security Tools.
- DazukoFS supporte certaines versions de noyau. Si le package DazukoFS fourni avec Bitdefender Endpoint Security Tools n'est pas compatible avec la version du noyau du système, le module ne pourra pas se charger. Vous pouvez dans ce cas mettre à jour le noyau vers la version supportée ou recompiler le module DazukoFS pour votre version de noyau. Le package DazukoFS se trouve dans le répertoire d'installation de Bitdefender Endpoint Security Tools :

  `/opt/BitDefender/share/modules/dazukofs/dazukofs-modules.tar.gz`
- Lors du partage de fichiers à l'aide de serveurs dédiés tels que NFS, UNFSv3 ou Samba, vous devez lancer les services dans l'ordre suivant :

  1. Activez l'analyse à l'accès par politique à partir de Control Center.

     Pour plus d'informations, veuillez vous référer au Guide Administrateur de GravityZone.
  2. Lancez le service de partage réseau.

     Pour NFS :

     ```
     # service nfs start
     ```

     Pour UNFSv3 :

     ```
     # service unfs3 start
     ```

     Pour Samba :

     ```
     # service smbd start
     ```

Important
Pour le service NFS, DazukoFS est compatible uniquement avec le serveur NFS User Server.

Fonctionnement de Network Discovery

Outre l'intégration à Active Directory, GravityZone inclut également un mécanisme de découverte du réseau automatique conçu pour détecter les ordinateurs du groupe de travail.

GravityZone s'appuie sur le service **Explorateur d'ordinateurs de Microsoft** et sur l'outil **NBTscan** pour réaliser la découverte du réseau.

Le service Explorateur d'ordinateurs est une technologie de réseau utilisée par les ordinateurs Windows pour maintenir des listes actualisées de domaines, groupes de travail et les ordinateurs qui s'y trouvent et pour fournir ces listes aux ordinateurs clients sur demande. Les ordinateurs détectés dans le réseau par le service Explorateur d'ordinateurs peuvent être consultés en exécutant la commande **net view** dans une fenêtre d'invite de commandes.

La commande Net view

L'outil NBTscan analyse les réseaux en utilisant NetBIOS. Il envoie des requêtes à chaque endpoint du réseau et récupère des informations telles que l'adresse IP, le nom NetBIOS et l'adresse MAC.

Pour activer la découverte automatique du réseau, Bitdefender Endpoint Security Tools Relay doit être déjà installé sur au moins un ordinateur du réseau. Cet ordinateur sera utilisé pour analyser le réseau.

Important
Control Center n'utilise pas les informations réseau d'Active Directory ou de la fonctionnalité de cartographie du réseau. Le mappage réseau exploite une technologie

de découverte du réseau différente : le protocole LLTD (Link Layer Topology Discovery).

Control Center n'est pas impliqué activement dans le fonctionnement du service Explorateur d'ordinateurs. Bitdefender Endpoint Security Tools demande uniquement au service Explorateur d'ordinateurs la liste des postes de travail et serveurs visibles dans le réseau (nommée liste de parcours) puis l'envoie à Control Center. Le Control Center gère la liste de parcours, en ajoutant les ordinateurs détectés récemment à sa liste d'**Ordinateurs non administrés**. Les ordinateurs détectés auparavant ne sont pas supprimés après une nouvelle requête de découverte du réseau, vous devez donc exclure & supprimer manuellement les ordinateurs qui ne sont plus dans le réseau.

La requête initiale de la liste de parcours est effectuée par le premier Bitdefender Endpoint Security Tools installé dans le réseau.

- Si le relais est installé sur l'ordinateur d'un groupe de travail, seuls les ordinateurs de ce groupe de travail seront visibles dans Control Center.
- Si le relais est installé sur l'ordinateur d'un domaine, seuls les ordinateurs de ce domaine seront visibles dans Control Center. Les ordinateurs d'autres domaines peuvent être détectés s'il y a une relation d'approbation avec le domaine dans lequel le relais est installé.

Les requêtes de découverte du réseau suivantes sont réalisées régulièrement à chaque heure. Pour chaque nouvelle requête, Control Center divise l'espace des ordinateurs administrés en des zones de visibilité puis désigne un relais dans chaque zone pour effectuer la tâche. Une zone de visibilité est un groupe d'ordinateurs qui se détectent les uns les autres. Une zone de visibilité est généralement définie par un groupe de travail ou domaine, mais cela dépend de la topologie et de la configuration du réseau. Dans certains cas, une zone de visibilité peut consister en de multiples domaines et groupes de travail.

Si le relais sélectionné ne parvient pas à effectuer la requête, Control Center attend la requête suivante planifiée, sans choisir d'autre relais pour réessayer.

Pour une visibilité complète du réseau, le relais doit être installé sur au moins un ordinateur de chaque groupe de travail ou domaine de votre réseau. Idéalement, Bitdefender Endpoint Security Tools devrait être installé sur au moins un ordinateur de chaque sous-réseau.

Plus d'informations sur le service Explorateur d'ordinateurs de Microsoft

Présentation rapide du service Explorateur d'ordinateurs :

- Fonctionne indépendamment d'Active Directory.
- Fonctionne exclusivement sur les réseaux IPv4 et opère de manière indépendante, dans les limites d'un groupe LAN (groupe de travail ou domaine). Une liste de parcours est établie et gérée pour chaque groupe LAN.
- Utilise généralement des diffusions de serveurs sans connexion pour communiquer entre les nœuds.
- Utilise NetBIOS sur TCP/IP (NetBT).
- Nécessite une résolution de noms NetBIOS. Il est recommandé d'avoir une infrastructure WINS (Windows Internet Name Service) opérationnelle dans le réseau.
- N'est pas activé par défaut dans Windows Server 2008 et 2008 R2.

Pour des informations détaillées sur le service Explorateur d'ordinateurs, consultez le sujet technique Computer Browser Service sur Microsoft Technet.

Configuration requise pour la découverte du réseau

Afin de découvrir tous les ordinateurs (serveurs et postes de travail) qui seront administrés depuis le Control Center, les conditions suivantes doivent être remplies :

- Les ordinateurs doivent faire partie d'un groupe de travail ou d'un domaine et être connectés via un réseau local IPv4. Le service Explorateur d'ordinateurs ne fonctionne pas sur les réseaux IPv6.
- Plusieurs ordinateurs dans chaque groupe LAN (groupe de travail ou domaine) doivent exécuter le service Explorateur d'ordinateurs. Les contrôleurs principaux de domaine doivent également exécuter le service.
- NetBIOS sur TCP/IP (NetBT) doit être activé sur les ordinateurs. Le pare-feu local doit autoriser le trafic NetBT.
- En cas d'utilisation d'un relais Linux pour découvrir d'autres endpoints Linux et Mac, vous devez soit installer Samba sur les endpoints cibles, ou les joindre dans Active Directory et utiliser le DHCP. De cette manière, leur NetBIOS sera automatiquement configuré.
- Le partage de fichiers doit être activé sur les ordinateurs. Le pare-feu local doit autoriser le partage de fichiers.

- Une infrastructure WINS (Windows Internet Name Service) doit être installée et opérationnelle.
- La découverte du réseau doit être activée (**Panneau de configuration > Centre Réseau et partage > Modifier les paramètres de partage avancés**).

  Pour activer cette fonctionnalité, les services suivants doivent être activés :
  - DNS Client
  - Function Discovery Resource Publication
  - SSDP Discovery
  - UPnP Device Host
- Dans les environnements avec plusieurs domaines, il est recommandé d'établir des relations d'approbation entre les domaines afin que les ordinateurs puissent accéder aux listes de parcours d'autres domaines.

Les ordinateurs à partir desquels Bitdefender Endpoint Security Tools demande le service Explorateur d'ordinateurs doivent être capables de résoudre les noms NetBIOS.

Note
Le mécanisme de découverte du réseau fonctionne pour tous les systèmes d'exploitation supportés, y compris les versions Windows Embedded, à condition de disposer de la configuration requise.

5.4. Installer Sandbox Analyzer On-Premises

Pour vous assurer que l'installation se déroule sans problème, procédez comme suit :

1. Préparer l'installation
2. Déployez l'appliance virtuelle de Sandbox Analyzer
3. Déployer l'appliance virtuelle de sécurité du réseau

5.4.1. Préparer l'installation

Avant d'installer Sandbox Analyzer On-Premises, vérifiez les points suivants :

- L'hyperviseur VMWare ESXi est installé et configuré. Pour en apprendre plus, consultez la documentation vSphere Installation and Setup, section 2 : « Installing and Setting Up ESXi ».
- L'appliance virtuelle de Bitdefender GravityZone est déployée et configurée.

Note
En ce qui concerne l'hyperviseur VMWare ESXi, vérifiez les points suivants :

- La version d'ESXi est 6.5 ou supérieure.
- La version du datastore VMFS est 5.
- SSH est activé **Startup policy** avec la configuration **Start and stop with host**.
- Le service NTP est actif et configuré.

La clé de licence de Sandbox Analyzer On-Premises contrôle la limite maximale de détonations simultanées. Comme chaque détonation utilise une instance de machine virtuelle en cours d'exécution, le nombre de détonations simultanées se reflète dans le nombre de machines virtuelles créées. Pour en apprendre plus sur l'ajout de clés de licence dans GravityZone Control Center, consultez « Saisie de vos clés de licence » (p. 115).

5.4.2. Déployez l'appliance virtuelle de Sandbox Analyzer

Pour déployer l'appliance virtuelle de Sandbox Analyzer :

1. Connectez-vous à GravityZone Control Center.
2. Accédez à la page **Réseau > Packages**.
3. Cochez la case **Sandbox Analyzer** dans le tableau.
4. Cliquez sur le bouton **Télécharger** en haut à gauche de la page. Sélectionnez l'option **Appliance de sécurité (ESXi autonome)**.
5. Utilisez votre outil de gestion de la virtualisation (par exemple, le client vSphere) pour importer le fichier OVA téléchargé dans votre environnement virtuel.

   Note
   Lors du déploiement du fichier OVA, configurez les réseaux comme suit :

   - **Réseau Bitdefender** - il s'agit du réseau auquel sont connectés les autres composants Bitdefender (interface `eth0`). Sandbox Analyzer et l'appliance GravityZone doivent être sur le même réseau et doivent communiquer via `eth0`.
   - **Réseau de détonation privé** - Sandbox Analyzer utilise ce réseau pour la communication interne (interface `eth1`). Ce réseau doit être isolé de tous les autres segments de réseau.

- **Réseau d'accès à Internet** - Sandbox Analyzer utilise ce réseau pour obtenir les dernières mises à jour (interface `eth2`). L'interface `eth2` ne doit pas avoir la même IP ou le même réseau que `eth0`.

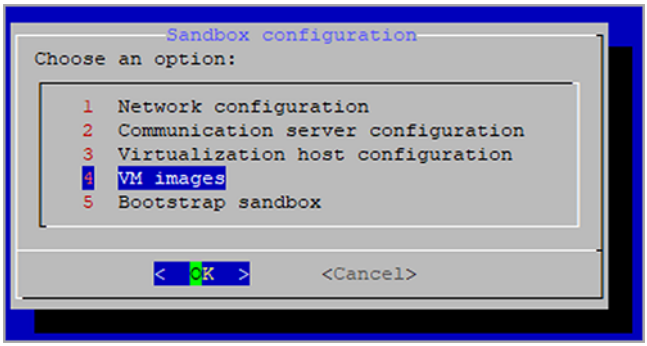
6. Allumez l'appliance.
7. Depuis l'outil de gestion de la virtualisation, accédez à l'interface de la console de l'appliance virtuelle Sandbox Analyzer.
8. Lorsqu'il vous sera demandé de vous identifier, entrez le nom d'utilisateur `root` et le mot de passe `sve`.
9. Ouvrez le menu de configuration en exécutant la commande suivante :

```
/opt/bitdefender/bin/sandbox-setup
```

10. Dans le menu **Configuration de la sandbox**, sélectionnez les paramètres suivants :
    a. **Configuration réseau**. Sélectionnez cette option pour configurer la carte réseau d'administration. Sandbox Analyzer utilisera cette interface réseau pour communiquer avec GravityZone.

       L'adresse IP peut être attribuée manuellement ou automatiquement via DHCP.

       Note
       Si l'appliance GravityZone est sur un réseau différent de `eth0`, vous devez ajouter un routage statique dans **Configuration du réseau > Réseau BitDefender > Routes** pour que Sandbox Analyzer fonctionne correctement.



Console de l'appliance Sandbox Analyzer

b. **Configuration du proxy Internet**. Sandbox Analyzer nécessite une connexion à Internet pour être installé. Le cas échéant, vous pouvez configurer Sandbox Analyzer pour passer par un proxy en indiquant les informations suivantes :

   - **Hôte** - IP ou FQDN du serveur proxy. Utilisez la syntaxe suivante : `http://<IP/Nom d'hôte>:<Port>`.
   - **Nom d'utilisateur et mot de passe** - vous devez saisir deux fois le mot de passe.
   - **Domaine** - le domaine Active Directory, le cas échéant.

c. **Configuration du serveur de communication**. Indiquez l'adresse IP ou le nom d'hôte de l'appliance exécutant le rôle Communicatino Server.

   Utilisez la syntaxe suivante : `http://<IP/Nom d'hôte>:<Port>`. Le port par défaut est le `8443`.

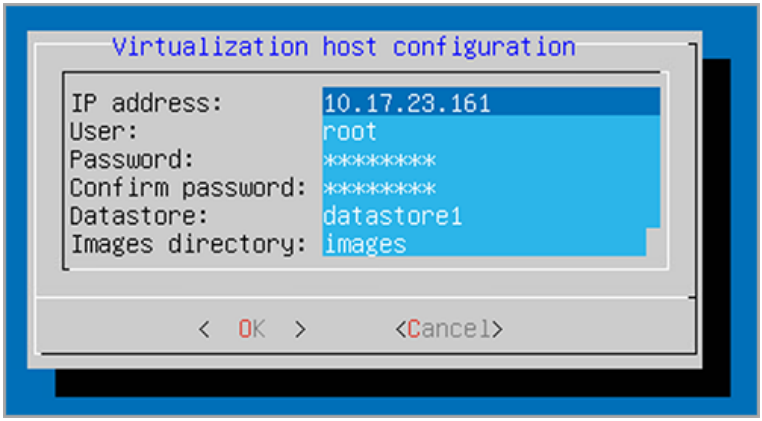
   Note
   Après avoir saisi une adresse IP ou un nom d'hôte et enregistré les modifications, l'instance de Sandbox Analyzer deviendra visible dans la GravityZone Control Center, sur la page**Sandbox Analyzer > Infrastructure**.

d. **Configuration de l'hôte virtualisé** Sandbox Analyzer utilise le serveur ESXi pour procéder au provisionning de l'infrastructure d'analyse des malwares. En utilisant **Configuration de l'hôte virtualisé**, vous connectez l'appliance Sandbox Analyzer à l'hôte ESXi en indiquant les informations suivantes :

- L'adresse IP du serveur ESXi.
- Informations d'authentification root pour accéder à l'hôte ESXi.
- Datastore dédié à Sandbox Analyzer.

  Saisissez le nom du datastore tel qu'il apparait dans ESXi.
- Nom du dossier utilisé dans le datastore pour stocker les images de machines virtuelles.

  Si ce dossier n'existe pas, vous devez le créer sur le datastore avant d'enregistrer la configuration de Sandbox Analyzer.



Console de l'appliance Sandbox Analyzer

e. **Images VM**. Pour créer des machines virtuelles de détonation pour Sandbox Analyzer, vous devez copier les fichiers VMDK contenant les images désirées dans le dossier **Images** indiqué dans le menu **Configuration de l'hôte virtualisé**. Depuis le menu **Images VM**, vous pouvez modifier les paramètres suivants pour chaque image :

   i. Dans le menu **Configuration de l'image**, indiquez le nom de l'image (tel qu'il apparaitra dans GravityZone Control Center) et dans le système d'exploitation.

      Note
      Le dossier contenant les images VM est régulièrement analysé et les nouvelles entrées sont détectées dans GravityZone. Ces entrées sont

visibles dans Control Center, sur la page **Sandbox Analyzer > Infrastructure > Gestion des images**.

Dans certaines situations, en utilisant Sandbox Analyzer, vous rencontrerez peut-être des problèmes avec les machines virtuelles de détonation. Pour corriger ces problèmes, vous devez désactiver l'option Anti-fingerprinting. Pour plus d'informations, veuillez consulter « Techniques Anti-fingerprinting » (p. 158)

ii. Dans le menu **Hôtes DMZ**, vous pouvez passer en liste blanche les noms d'hôtes dont les services et composants embarqués dans les machines virtuelles ont besoin pour communiquer avec Sandbox Manager. Pour plus d'informations, veuillez consulter « Hôtes DMZ » (p. 159)

iii. Dans le menu **Nettoyage**, vous pouvez supprimer les images VM dont vous n'avez plus besoin.

f. **Bootstrap sandbox**. Une fois les détails de configuration de Sandbox Analyzer ajoutés, poursuivez l'installation en sélectionnant cette option. Le statut de l'installation apparaitra dans la GravityZone Control Center, sur la page **Sandbox Analyzer > Infrastructure**.

Techniques Anti-fingerprinting

Par défaut, pendant le processus de création d'images, Sandbox Analyzer activera plusieurs techniques Anti-fingerprinting. Certains types de malwares sont capables de déterminer s'ils sont exécutés dans un environnement de sandbox et en ce cas de ne pas activer leur routine malveillante.

L'objectif de l'Anti-fingerprinting est de simuler diverses conditions afin d'imiter un environnement réel. Compte tenu des combinaisons théoriquement illimitées de logiciels déployés et de configurations de l'environnement, il est impossible de prévoir et de contrôler à l'avance une combinaison, et il est possible que certaines techniques ne soient pas compatibles avec les logiciels installés sur l'image maitresse. Ces situations rares s'accompagnent des symptômes suivants :

- Erreurs pendant le processus de création de l'image.
- Erreurs à l'exécution du logiciel à l'intérieur de l'image.
- Messages d'erreur renvoyés lors de la détonation des échantillons.
- Logiciel sous licence ne fonctionnant plus pour cause de clés de licence invalides.

Une solution rapide à ces problèmes rares consiste à recréer l'image en désactivant les techniques Anti-fingerprinting. Pour cela, suivez ces étapes :

1. Connectez-vous à GravityZone Control Center et supprimez l'image.
2. Connectez-vous à l'appliance Sandbox Analyzer et lancez la console de l'appliance Sandbox Analyzer en exécutant la commande suivante :

```
/opt/bitdefender/bin/sandbox-setup
```

3. Rendez-vous dans **VM Images> Image Configuration**.
4. Sélectionnez l'image posant problème.
5. Recherchez l'option **Anti-fingerprinting**.
6. Décochez la case pour désactiver les techniques Anti-fingerprinting.

Hôtes DMZ

Pendant le processus de création d'une image, une infrastructure virtuelle sera créée pour faciliter la communication entre Sandbox Manager et les machines virtuelles. Du point de vue réseau, il s'agit d'un environnement réseau isolé qui contiendra toutes les communications potentielles qu'un échantillon pourrait créer lors de la détonation.

Le menu Serveurs DMZ permet de passer en liste blanche les noms d'hôtes dont les services et composants de tierces parties embarqués dans les machines virtuelles ont besoin pour communiquer et fonctionner correctement.

Par exemple, les serveurs de licence KMS utilisés par Windows si une licence de volume est appliquée aux machines virtuelles fournies.

5.5. Installer le Chiffrement complet du disque

Le Chiffrement complet du disque dur est un service GravityZone qui doit être activé via une clé de licence. Pour cela, rendez-vous dans **Configuration >License** et entrez la clé de licence.

Pour plus d'informations sur les clés de licence, consultez « Gestion des licences » (p. 114).

Les agents de sécurité de Bitdefender prennent en charge le Chiffrement complet du disque dur à partir des versions 6.2.22.916 sur Windows et 4.0.0173876 sur

Mac. Pour vérifier que les agents sont pleinement compatibles avec ce module, vous avez deux options :

- Installez les agents de sécurité avec le module de Chiffrement inclus.
- Utilisez la fonction **Reconfigurer**.

Pour plus d'informations sur l'utilisation du Chiffrement complet du disque dur sur votre réseau, consultez le chapitre **Politiques de sécurité > Chiffrement** du Guide de l'administrateur de GravityZone.

5.6. Installer la protection Exchange

Security for Exchange s'intègre automatiquement aux Serveurs Exchange, en fonction du rôle du serveur. Pour chaque rôle, seules les fonctionnalités compatibles sont installées, comme indiqué ici :

Caractéristiques	Microsoft Exchange 2019/2016/2013		Microsoft Exchange 2010/2007		
	Rôle serveur de transport Edge	Boîte de messagerie	Rôle serveur de transport Edge	Hub	Boîte de messagerie
Niveau du transport					
Filtrage Antimalware	x	x	x	x	
Filtrage antispam	x	x	x	x	
Filtrage du contenu	x	x	x	x	
Pièces jointes	x	x	x	x	
Base Exchange					
Analyse antimalware à la demande		x			x

5.6.1. Préparation de l'Installation

Avant d'installer Security for Exchange, veillez à respecter l'ensemble de la configuration requise ; Bitdefender Endpoint Security Tools pourrait sinon être installé sans le module de Protection Exchange.

Pour que le module Protection Exchange fonctionne correctement et pour éviter les conflits et les résultats indésirables, désinstallez tout agent antimalware ou de filtrage de messagerie.

Bitdefender Endpoint Security Tools détecte et désinstalle automatiquement la plupart des produits antimalware et désactive l'agent antimalware intégré à Exchange Server depuis la version 2013. Pour plus d'informations sur la liste des logiciels de sécurité détectés, référez-vous à cet article KB.

Vous pouvez réactiver manuellement l'agent antimalware intégré à Exchange à tout moment, bien que cela ne soit pas recommandé.

5.6.2. Installation de la protection sur les serveurs Exchange

Pour protéger vos serveurs Exchange, vous devez installer Bitdefender Endpoint Security Tools avec le rôle Protection Exchange sur chacun d'entre eux.

Vous pouvez déployer Bitdefender Endpoint Security Tools sur les serveurs Exchange de différentes façons :

- Par une installation locale, en téléchargeant et en exécutant le package d'installation sur le serveur.
- Par une installation à distance, en exécutant une tâche **Installation**.
- À distance, en exécutant la tâche **Reconfigurer le client** si Bitdefender Endpoint Security Tools fournit déjà une protection du système de fichiers sur le serveur.

Pour les étapes d'installation détaillées, référez-vous à « Installation des agents de sécurité » (p. 127).

5.7. Installer la Protection de stockage

Security for Storage est un service de Bitdefender conçu pour protéger les serveurs de stockage en réseau (NAS) et les systèmes de partage de fichiers conformes à l'ICAP (Internet Content Adaptation Protocol). Pour consulter la liste des systèmes de partage de fichiers, voir « Protection de stockage » (p. 48).

Pour utiliser Security for Storage avec votre solution GravityZone

1. Installez et configurez au moins deux Security Server dans votre environnement pour faire office de serveurs CAP. Les Security Server de Bitdefender analysent les fichiers, envoient des verdicts aux systèmes de stockage et prennent les mesures appropriées si nécessaire. En cas de surcharge, le premier Security Server renvoie le surplus de données au second.

   Note
   En terme de bonnes pratiques, installez des Security Server dédiés à la protection de stockage de manière séparée des Security Server utilisés pour d'autres rôles, tels que l'analyse antimalware.

   Pour en apprendre plus sur la procédure d'installation de Security Server, consultez la section **Installer Security Server** du présent guide.

2. Configurez le module **Protection de stockage** depuis les paramètres de politique GravityZone.

   Pour en apprendre plus, consultez le Guide de l'administrateur GravityZone, chapitre **Politiques de sécurité > Ordinateurs et Machines virtuelles > Protection de stockage**.

Pour en apprendre plus sur la configuration et la gestion des serveurs ICAP sur un NAS ou système de partage de fichier particulier, consultez la documentation de la plateforme concernée.

5.8. Installation de la protection pour appareils mobiles

Security for Mobile est une solution de gestion des appareils mobiles conçue pour les appareils iPhone, iPad et Android. Pour une liste complète des versions de système d'exploitation supportées, consultez la configuration système requise.

Pour gérer Security for Mobile à partir de Control Center, vous devez ajouter des appareils mobiles aux utilisateurs d'Active Directory ou personnalisés, avant d'installer l'application GravityZone Mobile Client sur les appareils. Une fois le service configuré, vous pouvez exécuter des tâches d'administration sur les appareils mobiles.

Avant de commencer, veillez à configurer une adresse publique (externe) pour le serveur de communication.

Pour installer Security for Mobile :

1. Si vous ne disposez pas de l'intégration à Active Directory, vous devez créer des utilisateurs pour les propriétaires d'appareils mobiles.

2. Ajouter des appareils aux utilisateurs.
3. Installez GravityZone Mobile Client sur les appareils et activez-le.

5.8.1. Configurer l'adresse externe du serveur de communication

Dans la configuration par défaut de GravityZone, les appareils mobiles peuvent être administrés uniquement lorsqu'ils sont connectés directement au réseau de l'entreprise (via Wifi ou VPN). Cela a lieu car lorsqu'on inscrit des appareils mobiles ils sont configurés pour se connecter à l'adresse locale de l'appliance du serveur de communication.

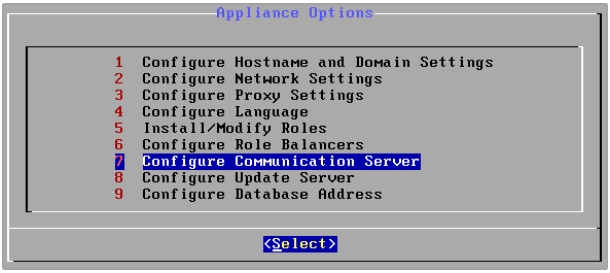
Pour pouvoir administrer les appareils mobiles sur Internet, quel que soit l'endroit où ils se trouvent, vous devez configurer le Serveur de communication avec une adresse publique.

Pour pouvoir administrer les appareils mobiles lorsqu'ils ne sont pas connectés au réseau de l'entreprise, les options suivantes sont disponibles :

- Configurez la redirection de port sur la passerelle de l'entreprise pour l'appliance exécutant le rôle du Serveur de Communication.
- Ajoutez une carte réseau supplémentaire à l'appliance exécutant le rôle du Serveur de communication et attribuez-lui une adresse IP publique.

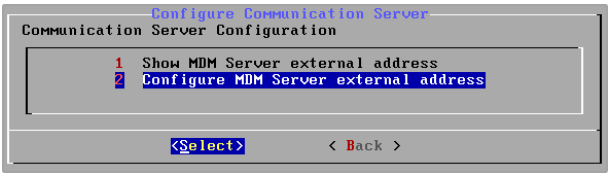
Dans les deux cas, vous devez configurer le serveur de communication avec l'adresse externe à utiliser pour la gestion des appareils mobiles :

1. Accédez à la console de l'appliance à partir de votre outil de gestion de la virtualisation (par exemple, vSphere Client).
2. Dans le menu principal, sélectionnez **Configurer le serveur de communication**.



Fenêtre Options de l'application

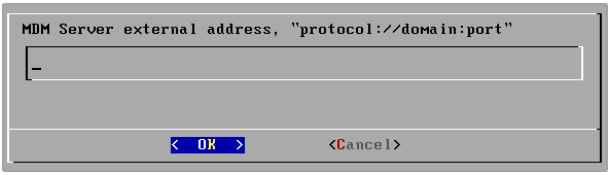
3. Sélectionnez **Configurer l'adresse externe du Serveur MDM**.



Configurez la fenêtre Serveur de communication

4. Saisissez l'adresse externe.

   Utilisez la syntaxe suivante : `https://<IP/Domaine>:<Port>.`.



Fenêtre de saisie de l'adresse externe du Serveur MDM

   - Si vous utilisez la redirection de port, vous devez saisir l'adresse IP publique ou le nom de domaine et le port ouvert sur la passerelle.
   - Si vous utilisez une adresse publique pour le Serveur de Communication, vous devez saisir l'adresse IP publique ou le nom de domaine et le port du Serveur de communication. Le port par défaut est le `8443`.

5. Sélectionnez **OK** pour enregistrer les modifications.

5.8.2. Créer et organiser des utilisateurs personnalisés

Sans Active Directory, vous devez commencer par créer des utilisateurs personnalisés afin d'avoir un moyen d'identifier les propriétaires d'appareils mobiles. Les utilisateurs d'appareils mobiles spécifiés ne sont liés d'aucune manière à Active Directory ou à d'autres utilisateurs définis dans le Control Center.

Créer des utilisateurs personnalisés

Pour créer un utilisateur personnalisé :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Appareils mobiles** dans le sélecteur de vues.
3. Dans le panneau de gauche, sélectionnez **Groupes personnalisés**.
4. Cliquez sur l'icône **Ajouter un utilisateur** de la barre d'outils d'actions. Une fenêtre de configuration s'affichera.
5. Spécifiez les informations requises de l'utilisateur :
   - Un nom d'utilisateur explicite (par exemple, le nom complet de l'utilisateur)
   - L'adresse e-mail de l'utilisateur

   Important
   - Veillez à indiquer une adresse e-mail valide. L'utilisateur recevra les instructions d'installation par e-mail lorsque vous ajouterez un appareil.
   - Chaque adresse e-mail peut être associée uniquement à un utilisateur.

6. Cliquez sur **OK**.

Organiser des utilisateurs personnalisés

Pour organiser des utilisateurs personnalisés :

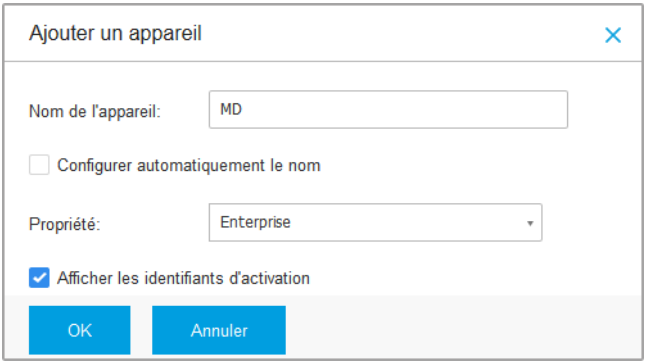
1. Créez des groupes personnalisés.
   a. Sélectionnez **Groupes personnalisés** dans le panneau de gauche et cliquez sur l'icône **Ajouter** de la barre d'outils d'actions (au-dessus du panneau).
   b. Indiquez un nom explicite pour le groupe et cliquez sur **OK**. Le nouveau groupe apparaît sous **Groupes personnalisés**.
2. Déplacez les utilisateurs personnalisés dans les groupes personnalisés appropriés.
   a. Sélectionnez les utilisateurs dans le panneau de droite.
   b. Glissez-déposez la sélection sur le groupe souhaité du panneau de gauche.

5.8.3. Ajouter des appareils aux utilisateurs

Pour ajouter un appareil à un utilisateur :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Appareils mobiles** dans le sélecteur de vues.

3. Recherchez l'utilisateur dans les dossiers Active Directory ou dans Groupes personnalisés.
4. Cliquez sur l'icône ⊕ **Ajouter un appareil** en haut du tableau. Une fenêtre de configuration s'affichera.



Ajouter un appareil mobile à un utilisateur.

5. Indiquez un nom explicite pour l'appareil.
6. Utilisez l'option **Configurer automatiquement le nom** si vous souhaitez que le nom de l'appareil soit généré automatiquement. Lorsqu'il est ajouté, l'appareil a un nom générique. Lorsque l'appareil est activé, il est automatiquement renommé avec les informations correspondantes du fabricant et du modèle.
7. Indiquez si l'appareil appartient à l'entreprise ou est personnel.
8. Sélectionnez l'option **Afficher les identifiants d'activation** après avoir cliqué sur le bouton **OK** si vous pensez installer GravityZone Mobile Client sur l'appareil de l'utilisateur.
9. Cliquez sur **OK**. L'utilisateur reçoit immédiatement un e-mail comportant les instructions d'installation et les détails de l'activation à configurer sur l'appareil. Les détails de l'activation comprennent le jeton d'activation et l'adresse du serveur de communication (ainsi que le code QR correspondant).

Note

- Vous pouvez voir les détails de l'activation d'un appareil à tout moment en cliquant sur son nom dans le Control Center.

- Vous pouvez également ajouter des appareils mobiles à une sélection d'utilisateurs et de groupes. Dans ce cas, la fenêtre de configuration permettra de définir uniquement le type d'appareils dont il s'agit. Les appareils mobiles créés par une sélection multiple recevront par défaut un nom générique. Dès qu'un appareil est enregistré, son nom change automatiquement, y compris les étiquettes correspondant au fabricant et au modèle.

5.8.4. Installer GravityZone Mobile Client sur les appareils

L'application GravityZone Mobile Client est distribuée exclusivement via Apple App Store et Google Play.

Pour installer GravityZone Mobile Client sur un appareil :

1. Recherchez l'application sur l'app store officiel.
   - Lien Google Play
   - Lien vers Apple App Store
2. Téléchargez et installez l'application sur l'appareil.
3. Lancez l'application et effectuez la configuration requise :
   a. Sur les appareils Android, cliquez sur **Activer** pour activer GravityZone Mobile Client comme administrateur de l'appareil. Lisez attentivement les informations fournies.

      Note

      - Pour les appareils Android (version 7.0 ou supérieure), la tâche Verrouiller force l'utilisation du mot de passe défini dans votre console GravityZone uniquement si aucune autre protection par verrouillage n'est configurée sur l'appareil. Le cas contraire, les options existantes de verrouillage de l'écran telles que Schéma, PIN, Mot de passe, Empreinte digitale ou Smart Lock seront utilisées pour protéger l'appareil.
      - La tâche Déverrouiller n'est plus disponible pour les appareils Android (version 7.0 ou supérieure).
      - En raison de limitations techniques, les tâches Verrouiller et Effacer ne sont pas disponibles sur Android 11.

   b. Saisissez le jeton d'activation et l'adresse du serveur de communication ou scannez le code QR reçu par e-mail.

c. Appuyez sur **Faire confiance** lorsqu'il vous sera demandé d'accepter le certificat de Communication Server. De cette manière, GravityZone Mobile Client valide le Communication Server et n'acceptera que les messages en sa provenance, empêchant ainsi les attaques de l'homme du milieu.

d. Cliquez sur **Activer**.

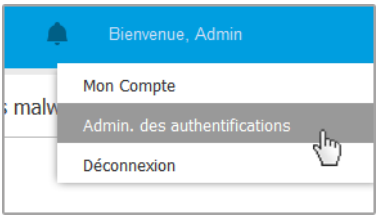
e. Sur les appareils iOS, vous êtes invité à installer le profil MDM. Si votre appareil est protégé par mot de passe, l'on vous demandera de l'indiquer. En outre, vous devez autoriser GravityZone à accéder aux paramètres de votre appareil, sinon le processus d'installation revient à l'étape précédente. Veuillez suivre les instructions à l'écran pour terminer l'installation du profil.

Note
Les utilisateurs doivent autoriser la localisation des appareils en arrière-plan, et pas seulement pendant l'utilisation de l'application, pour que la fonctionnalité Localiser fonctionne correctement.

5.9. Admin. des authentifications

L'Administrateur des authentifications vous aide à définir les identifiants requis pour accéder aux inventaires vCenter Server disponibles et pour l'authentification à distance sur différents systèmes d'exploitation de votre réseau.

Pour ouvrir l'Administrateur des authentifications, cliquez sur votre nom d'utilisateur dans l'angle supérieur droit de la page et sélectionnez **Admin. des authentifications**.



Le menu Admin. des authentifications

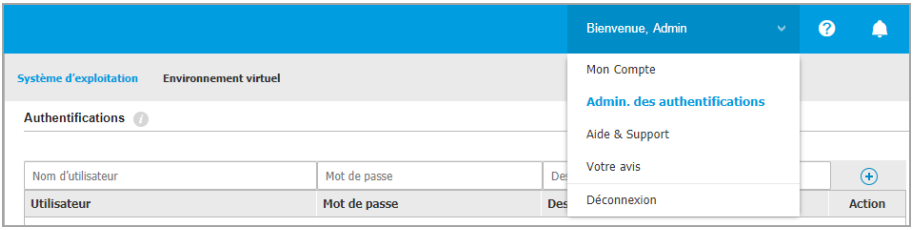
La fenêtre **Admin. des authentifications** comporte deux onglets :

- Système d'exploitation
- Environnement virtuel

5.9.1. Système d'exploitation

L'onglet **Système d'exploitation** vous permet de gérer les identifiants de l'administrateur requis pour l'authentification à distance lors des tâches d'installation envoyées aux ordinateurs et aux machines virtuelles de votre réseau.

Pour ajouter un ensemble d'identifiants :



Admin. des authentifications

1. Saisissez le nom d'utilisateur et le mot de passe d'un compte administrateur de tous les systèmes d'exploitation cibles dans les champs correspondants en haut du titre du tableau. Vous pouvez également ajouter une description qui vous aidera à identifier chaque compte plus facilement. Si les ordinateurs sont dans un domaine, il suffit d'indiquer les identifiants de l'administrateur du domaine.

   Utilisez les conventions Windows lorsque vous saisissez le nom (d'un compte utilisateur).

   - pour les machines Active Directory, utilisez ces syntaxes : `username@domain.com` and `domain\username`. Pour vous assurer que les identifiants saisis fonctionneront, ajoutez-les dans les deux formes (`username@domain.com` et `domain\username`).
   - Pour les machines Workgroup, il suffit de saisir le nom d'utilisateur, sans le nom du groupe de travail.

2. Cliquez sur le bouton ⊕ **Ajouter** à droite du tableau. Le nouveau jeu d'authentifiants est ajouté au tableau.

   Note
   Si vous n'avez pas spécifié les informations d'authentification, vous serez invité à les saisir lorsque vous lancerez des tâches d'installation. Les identifiants

spécifiés sont enregistrés automatiquement dans votre Administrateur des authentifications afin que vous n'ayez pas à les saisir la prochaine fois.

5.9.2. Environnement virtuel

L'onglet Environnement virtuel vous permet de gérer les identifiants des systèmes de serveurs virtualisés disponibles.

Pour accéder à l'infrastructure virtualisée intégrée à Control Center, vous devez indiquer vos identifiants utilisateur pour chaque système de serveur virtualisé disponible. Control Center utilise vos identifiants pour se connecter à l'infrastructure virtualisée, en affichant uniquement les ressources auxquelles vous avez accès (en fonction de ce qui est défini dans le serveur virtualisé).

Pour spécifier les identifiants requis pour se connecter à un serveur virtualisé :

1. Sélectionnez le serveur dans le menu correspondant.

   Note
   Si le menu n'est pas disponible, c'est que l'intégration n'a pas encore été configurée ou que tous les authentifiants requis ont déjà été configurés.

2. Saisissez votre nom d'utilisateur et votre mot de passe ainsi qu'une description explicite.
3. Cliquez sur le bouton ⊕ **Ajouter**. Le nouveau jeu d'authentifiants est ajouté au tableau.

   Note
   Si vous ne configurez pas vos informations d'authentification dans l'Administrateur des authentifications, on vous demandera de les saisir lorsque vous tenterez de parcourir l'inventaire de tout système de serveur virtualisé. Les authentifiants que vous avez indiqués sont enregistrés dans votre Administrateur des authentifications afin que vous n'ayez pas besoin de les saisir la prochaine fois.

   Important
   Lorsque vous changez le mot de passe utilisateur de votre serveur virtualisé, pensez à l'actualiser dans l'Administrateur des authentifications.

5.9.3. Supprimer les identifiants de l'Administrateur des authentifications

Pour supprimer des identifiants obsolètes de l'Administrateur des authentifications :

1. Pointez sur la ligne du tableau contenant les identifiants que vous souhaitez supprimer.
2. Cliquez sur le bouton ⊗ **Supprimer** à droite de la ligne du tableau correspondante. Le compte sélectionné sera supprimé.

6. MISE À JOUR GRAVITYZONE

Bitdefender publie l'ensemble des mises à jour de produits et contenus de sécurité, par le biais des serveurs Bitdefender sur Internet. Toutes les mises à jour sont chiffrées et numériquement signées pour qu'elles ne puissent pas être altérées.

GravityZone comprend un rôle Update Server, conçu pour servir de point de distribution des mises à jour centralisé pour le déploiement de GravityZone. Update Server recherche et télécharge toutes les mises à jour de GravityZone disponibles sur les serveurs de mise à jour de Bitdefender sur Internet et les rend disponibles dans le réseau local. Les composants de GravityZone peuvent être configurés pour se mettre automatiquement à jour à partir du serveur de mise à jour local plutôt qu'à partir d'Internet.

Lorsqu'une nouvelle mise à jour est disponible, l'appareil GravityZone, l'agent de sécurité ou le Security Server vérifient la signature numérique de la mise à jour et le contenu du package, afin d'en contrôler respectivement l'authenticité et l'intégrité. Ensuite, chaque mise à jour est analysée et la nouvelle version est comparée à celle qui est déjà installée. Les fichiers les plus récents sont téléchargés localement et comparés à leur empreinte MD5, afin de s'assurer qu'ils n'ont pas été modifiés.

Si une vérification s'avère défaillante, la procédure de mise à jour s'arrêtera et renverra un message d'erreur. Dans le cas contraire, la mise à jour sera considérée valide et prête à être installée.

Pour mettre à jour les appliances GravityZone installées dans votre environnement et les packages d'installation des composants GravityZone, connectez-vous avec un compte administrateur de l'entreprise et allez sur la page **Configuration > Mise à jour**.

6.1. Mise à jour des appliances GravityZone

Via les mises à jour de l'appliance GravityZone, Bitdefender propose de nouvelles fonctionnalités ou des améliorations des fonctionnalités existantes. Celles-ci sont visibles dans Control Center.

Avant d'exécuter une mise à jour, il est recommandé de vérifier les points suivants :

- L'état de la mise à jour
- Toutes les informations ou tous les avertissements pouvant apparaitre.
- Le journal des modifications

Pour contrôler l'état de la mise à jour :

1. Rendez-vous sur la page **Configuration > Mise à jour > Rôles GravityZone**.
2. Dans la section **Statut actuel**, vous pouvez consulter les messages traitant de l'état général de votre déploiement. Si GravityZone doit être mis à jour, le bouton **Mettre à jour** devient disponible.
3. Dans la section **Infrastructure**, vérifiez les informations de chaque rôle GravityZone déployé sur votre réseau. Les rôles se mettant à jour de manière indépendante, pour chaque rôle vous pouvez voir : le nom de l'appliance qui l'héberge, son adresse IP, la version actuelle, la dernière version disponible, et le statut de la mise à jour.

Pour consulter le journal des modifications :

1. Rendez-vous sur la page **Configuration > Mise à jour > Rôles GravityZone**.
2. Cliquez sur le lien **Afficher le journal des modifications**. Une popup affiche une liste de toutes les versions et des modifications qu'elles ont apportées.

   Les notes de publication pour chaque nouveau produit ont également été publiées dans le Bitdefender Support Center.

Vous pouvez mettre à jour GravityZone de deux manières :

- Manuellement
- Automatiquement

6.1.1. Mise à jour manuelle

Choisissez cette méthode si vous voulez avoir le contrôle total sur le moment du déploiement de la mise à jour.

Pour mettre à jour GravityZone manuellement :

1. Rendez-vous sur la page **Configuration > Mise à jour > Rôles GravityZone**.
2. Cliquez sur le bouton **Mettre à jour** (s'il est disponible).

   La mise à jour peut prendre un certain temps. Patientiez jusqu'à la fin de la procédure.
3. Effacer le cache du navigateur.

Pendant la mise à jour, Control Center déconnecte tous les utilisateurs et les informe qu'une mise à jour est en cours. Vous pourrez voir en détail la progression de la procédure de mise à jour.

Une fois la mise à jour terminée, Control Center affiche la page de connexion.

6.1.2. Mise à jour automatique

En installant les mises à jour automatiquement, vous pouvez être certain que GravityZone est toujours à jour, avec les derniers patchs de sécurité et les dernières fonctionnalités.

GravityZone dispose de deux types de mise à jour automatique :

- Mises à jour du produit
- Mises à jour de logiciels de tierces parties

Mises à jour du produit

Ces mises à jour apportent de nouvelles fonctionnalités à GravityZone et résolvent les problèmes résultant de celles-ci.

Les mises à jour étant gênantes pour les utilisateurs de GravityZone, elles ont été pensées pour s'exécuter à des horaires prédéfinis. Vous pouvez programmer les mises à jour pour qu'elles soient exécutées au moment qui vous arrange. Par défaut, les mises à jour automatiques du produit sont désactivées.

Pour activer et programmer les mises à jour du produit :

1. Rendez-vous sur la page **Configuration > Mise à jour > Rôles GravityZone**.
2. Cochez la case **Activer les mises à jour automatiques du produit GravityZone**.
3. Définissez la **récurrence** sur **Quotidienne**, **Hebdomadaire** (sélectionnez un ou plusieurs jours de la semaine) ou **Mensuellement**.
4. Définissez un **intervalle**. Vous pouvez planifier une heure pour le début du processus de mise à jour lorsqu'une nouvelle mise à jour est disponible.

Par défaut, GravityZone fait apparaitre un message d'avertissement à tous les utilisateurs de Control Center 30 minutes avant le début de la mise à jour automatique. Pour désactiver cet avertissement, décochez la case **Alerte de 30 minutes de pause avant la mise à jour**.

Mises à jour de logiciels de tierces parties

L'appliance virtuelle GravityZone embarque un ensemble de produits logiciels créés par d'autres développeurs. Ce type de mise à jour vise à corriger ces logiciels aussi rapidement que possible pour éviter les risques de sécurité potentiels.

Ces mises à jour sont réalisées silencieusement, sans interrompre le travail sur Control Center.

Cette option est activée par défaut. Pour désactiver cette option :

1. Rendez-vous sur la page **Configuration > Mise à jour > Rôles GravityZone**.
2. Cochez la case **Activer les mises à jour de sécurité automatiques pour les composants GravityZone de tierces parties**

   Les patchs de logiciels de tiers seront ainsi publiés en une fois avec la mise à jour du produit GravityZone.

6.2. Configuration d'Update Server

Par défaut, Update Server télécharge des mises à jour à partir d'Internet toutes les heures. Nous vous recommandons de modifier les paramètres d'Update Server par défaut.

Pour vérifier et configurer les paramètres d'Update Server :

1. Allez sur la page **Mise à jour** dans Control Center et cliquez sur l'onglet **Composants**.
2. Cliquez sur le bouton **Paramètres** en haut du panneau du côté gauche pour afficher la fenêtre **Paramètres du serveur de mise à jour**.
3. **Configuration du serveur de mise à jour** vous permet de vérifier et de configurer les principaux paramètres.
   - **Adresse des packages.** L'adresse à partir de laquelle les packages sont téléchargés.
   - **Adresse de mise à jour.** UpdateServer est configuré pour rechercher et télécharger des mises à jour depuis `upgrade.bitdefender.com:80`. Il s'agit d'une adresse générique qui est résolue automatiquement pour correspondre au serveur le plus proche stockant les mises à jour de Bitdefender dans votre zone géographique.
   - **Port.** Lorsque les différents composants de GravityZone sont configurés pour se mettre à jour à partir d'UpdateServer, vous devez indiquer ce port. Le port par défaut est `7074`.
   - **IP.** L'adresse IP du serveur de mise à jour.

- **Période de mise à jour (heures).** Pour modifier la fréquence des mises à jour, tapez une nouvelle valeur dans ce champ. La valeur par défaut est 1.

4. Vous pouvez configurer le serveur de mise à jour de façon à ce qu'il télécharge automatiquement le Security Server et les kits d'endpoint.
5. UpdateServer peut agir en tant que passerelle pour les données envoyées par les produits clients Bitdefender installés dans le réseau aux serveurs Bitdefender. Ces données peuvent comprendre des rapports anonymes concernant l'activité des virus, les rapports de plantage du produit et les données utilisées pour l'inscription en ligne. Activer les rôles de passerelle est utile pour le contrôle de trafic dans les réseaux n'ayant pas accès à Internet.

   Note
   Vous pouvez désactiver à tout moment les modules du produit qui envoient des données statistiques ou sur les plantages aux Laboratoires Bitdefender. Vous pouvez utiliser des politiques pour contrôler ces options à distance sur les ordinateurs et les machines virtuelles administrés par le Control Center.

6. Cliquez sur **Enregistrer**.

6.3. Téléchargement des mises à jour de produits

Vous pouvez voir des informations sur les packages de composants GravityZone existants dans l'onglet **Composants**. Les informations disponibles comprennent la version en cours, la version de la mise à jour (le cas échéant) et l'état des opérations de mise à jour que vous lancez.

Pour mettre à jour un composant de GravityZone :

1. Allez sur la page **Mise à jour** dans Control Center et cliquez sur l'onglet **Composants**.
2. Cliquez sur le composant que vous souhaitez mettre à jour dans la liste **Produits**. Toutes les versions disponibles seront affichées dans le tableau **Packages**. Cochez la case correspondant à la version que vous souhaitez télécharger.

   Note
   Les nouveaux packages seront **Non téléchargés**. Une fois qu'une nouvelle version est publiée par Bitdefender, la version non téléchargée la plus ancienne sera supprimée du tableau.

3. Cliquez sur **Actions** en haut du tableau et sélectionnez **Publier** La version sélectionnée sera téléchargée et le statut changera en fonction. Actualisez le contenu du tableau en cliquant sur le bouton **Actualiser** et vérifiez l'état correspondant.

Important
L'appliance GravityZone ne comprend pas les packages du Security Server par défaut. Vous devez télécharger manuellement les packages du Security Server nécessaires à votre environnement.

6.4. Mise à jour produit hors ligne

GravityZone utilise par défaut un système de mise à jour connecté à Internet. Pour ls réseaux isolés, Bitdefender offre une alternative, rendant les mises à jour composants et contenus de sécurité disponibles également hors ligne.

6.4.1. Configuration nécessaire

Pour utiliser les mises à jour hors ligne, vous devez :

- Une instance GravityZone installée sur un réseau avec accès à Internet ("instance en ligne"). L'instance en ligne doit avoir :
  - Accès direct à Internet
  - Accès aux ports 80 et 443. Pour plus d'informations concernant les ports utilisés par GravityZone, reportez-vous à cet article de la base de connaissances.
  - Uniquement les rôles installés de Serveur de base de données et de Serveur de mise à jour
- Une ou plusieurs instances GravityZone installées sur un réseau sans accès à Internet ("instances hors ligne")
- Les deux instances GravityZone doivent disposer de la même version de l'appliance

6.4.2. Configuration de l'instance en ligne GravityZone

Pendant cette phase, vous déploierez une instance GravityZone sur un réseau disposant d'un accès à Internet, puis vous la configurerez pour qu'elle fonctionne en tant que serveur de mise à jour hors ligne.

1. Déployer GravityZone sur une machine disposant d'une connexion à Internet.
2. Installer uniquement les rôles de Serveur de base de données et de Serveur de mise à jour.
3. Accédez au terminal TTY de la machine dans votre environnement virtuel (ou connectez-y-vous via SSH).
4. Connectez-vous à l'aide du nom d'utilisateur `bdadmin` et du mot de passe que vous avez défini.
5. Exécutez la commande `sudo su` pour obtenir des privilèges **root**.
6. Exécutez les commandes suivantes pour installer le package hors ligne `gzou-mirror` :

```
# apt update # gzcli update # apt install gzou-mirror
```

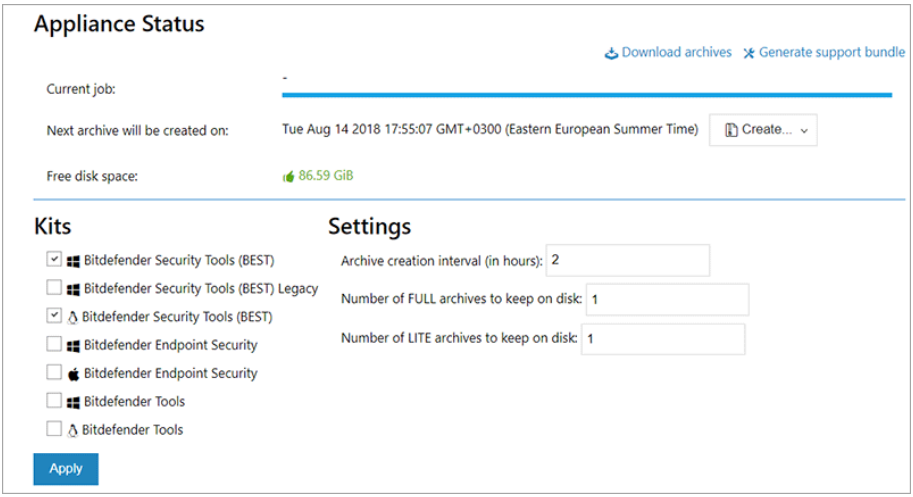
Le `gzou-mirror` a les rôles suivants :

- Configurez le Serveur de mise à jour pour générer des archives de mise à jour automatiquement hors ligne.
- Installez un service web sur l'instance en ligne, en indiquant les options de configuration et de téléchargement pour les archives de mise à jour hors ligne.

6.4.3. Configurer et télécharger les fichiers de mise à jour initiaux

Pendant cette phase, vous configurerez les paramètres des archives de mise à jour via le service web installé sur l'instance en ligne, puis créerez les fichiers d'archive requis pour configurer l'instance hors ligne. Ensuite, il vous faudra télécharger les fichiers de mise à jour et les placer sur un support de données portable (clé USB).

1. Accédez au service web via l'URL suivante : `https://Online-Instance-Update-Server-IP-or-Hostname`, avec le nom d'utilisateur `bdadmin` et le mot de passe que vous avez défini.



L'instance en ligne - Service web

2. Configurez l'archive de mise à jour hors ligne de la manière suivante :
   - Dans **Kits** : sélectionnez les kits agent de l'endpoint que vous souhaitez inclure dans l'archive de mise à jour hors ligne.
   - Dans **Paramètres**, modifiez vos préférences en matière d'archives de mise à jour.

     Une tâche CRON installée sur l'instance en ligne vérifiera toutes les minutes si de nouveaux fichiers de mise à jour sont disponibles et si l'espace disque disponible est supérieur à 10 Go. Lors de chaque période définie par l'option **Intervalle de création des archives (en heures)**, la tâche CRON créera les fichiers suivants :

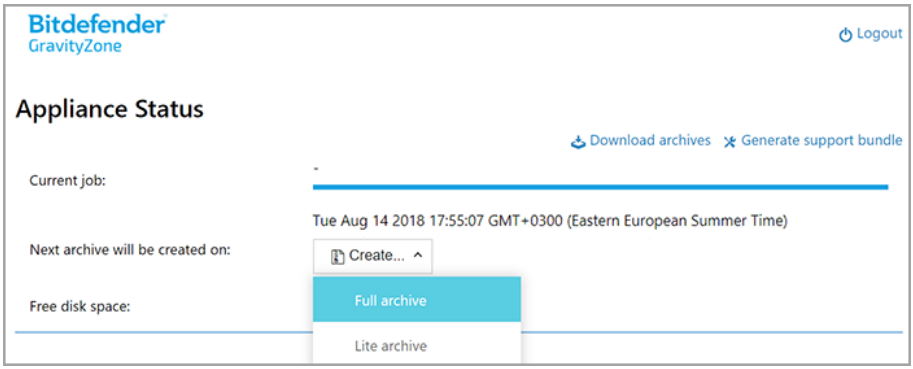
     – **Archive complète (produit + contenu de sécurité)**, lorsque de nouveaux fichiers de mise à jour sont disponibles

     – **Archive légère** (contenu de sécurité uniquement), lorsqu'il n'y a aucun nouveau fichier de mise à jour

     Les archives seront créées à l'emplacement suivant :

     `https://Online-Instance-Update-Server-IP-or-Hostname/snapshots`

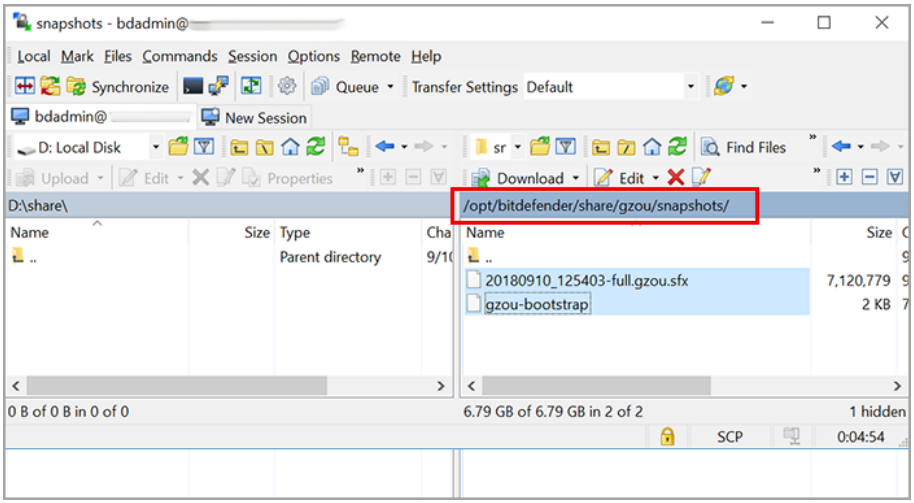
3. Cliquez sur **Créer > Archive** complète pour créer la première archive complète. Patientez jusqu'à ce que l'archive ait été créée.



L'instance en ligne - Service web : Création de l'archive

4. Téléchargez l'archive de mise à jour complète et le fichier `gzou-bootstrap` à partir de l'instance en ligne. Plusieurs possibilités s'offrent à vous :
   - Via le Service web : cliquez sur **Télécharger des archives** pour accéder à la page contenant les liens vers les fichiers de mise à jour. Cliquez sur les liens de l'archive de mise à jour complète et du fichier `gzou-bootstrap` pour les télécharger sur votre endpoint.
   - Utilisez le client SCP/SCTP de votre choix (WinSCP, par exemple) pour établir une session SCP avec l'instance en ligne et transférer les fichiers précédemment cités vers n'importe quel emplacement de votre réseau en ligne. Le chemin par défaut de l'instance en ligne est :

     `/opt/bitdefender/share/gzou/snapshots`



Transférer des fichiers de mise à jour en utilisant SCP

- Via le partage SAMBA. Utilisez un partage SAMBA en lecture seule pour récupérer les archives de mise à jour hors ligne à partir de l'emplacement suivant :

  `\\Online-Instance-update-Server-IP-or-Hostname\gzou-snapshots`

  Note
  Les identifiants pour accéder au partage SAMBA, s'ils vous sont demandés, sont les mêmes que les identifiants pour l'instance en ligne (nom d'utilisateur `bdadmin` et mot de passe).

6.4.4. Configuration de l'instance hors ligne GravityZone

Pendant cette étape, vous déploierez et configurerez l'instance hors ligne pour recevoir des mises à jour via les archives générées par l'instance en ligne. Sauf contre-indication, toutes les commandes doivent être exécutées comme **root**.

1. Déployer GravityZone sur une machine de l'environnement isolé.
2. Installer uniquement les rôles de Serveur de base de données et de Serveur de mise à jour.

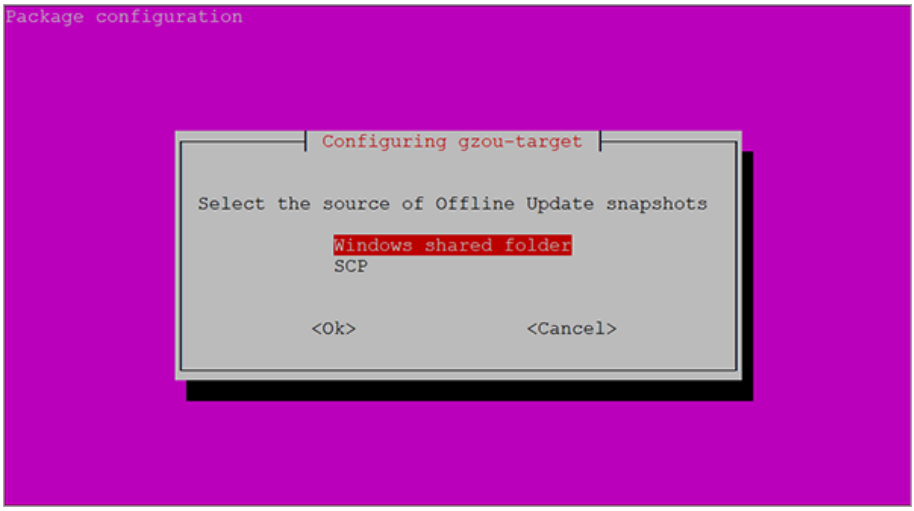
3. Transférez l'archive de mise à jour et le fichier `gzou-bootstrap` téléchargés depuis l'instance en ligne vers le `/home/bdadmin directory` de l'instance hors ligne à l'aide d'un support de données portable (clé USB).

   Important
   Afin que la mise à jour hors ligne fonctionne, vérifiez que :
   - L'archive de mise à jour et le `gzou-bootstrap` se trouvent dans le même dossier.
   - L'archive de mise à jour est une archive **complète**.

4. Exécutez le fichier `gzou-bootstrap` de la manière suivante :
   a. Accédez au terminal TTY de la machine dans votre environnement virtuel (ou connectez-y-vous via SSH).
   b. Transformez `gzou-bootstrap` en exécutable :

   ```
   #
   chmod +x gzou-bootstrap
   ```

   c. Exécutez : `./gzou-bootstrap`
5. Choisissez la méthode de transfert des archives de mise à jour vers l'instance hors ligne :
   - Sélectionnez **Dossier Windows partagé** (partage Samba). Dans ce cas, il vous faudra spécifier le chemin vers un partage Windows du réseau isolé, auquel l'instance hors ligne sera automatiquement connectée pour récupérer les archives de mise à jour. Saisissez les identifiants requis pour accéder à l'emplacement spécifié.
   - Sélectionnez SCP si vous transférerez manuellement les fichiers vers le dossier `/opt/bitdefender/share/gzou/snapshots/` de l'instance hors ligne via SCP.



Instance GravityZone hors ligne - Configurer le mode de transfert des fichiers de mise à jour

Note
Si vous souhaitez modifier ultérieurement la méthode de transfert :

a. Accédez au terminal TTY de l'instance hors ligne dans votre environnement virtuel (ou connectez-y-vous via SSH).
b. Connectez-vous à l'aide du nom d'utilisateur `bdadmin` et du mot de passe que vous avez défini.
c. Exécutez la commande `sudo su` pour obtenir des privilèges root.
d. Lancement :

```
# rm -f /opt/bitdefender/etc/gzou-target.json # dpkg-recon
```

La boîte de dialogue Configuration apparaîtra, à partir de laquelle vous pourrez effectuer les changements que vous souhaitez.

6. Passez à la ligne de commande de la console GravityZone hors ligne et installez le reste des rôles.
7. Accédez à la console hors ligne à partir de votre navigateur et saisissez votre clé de licence (mode hors ligne).

6.4.5. Utilisation de mises à jour hors ligne

Une fois que vous avez configuré les instances GravityZone, suivez ces étapes afin de mettre à jour votre installation hors ligne :

1. Téléchargez la dernière archive de mise à jour hors ligne à partir de l'instance en ligne vers le partage réseau de votre choix. Pour plus d'informations, reportez-vous à « Configurer et télécharger les fichiers de mise à jour initiaux » (p. 178).
2. Utilisez une clé USB pour transférer l'archive de mise à jour vers le partage Samba configuré du réseau isolé. Pour plus d'informations, reportez-vous à « Configuration de l'instance hors ligne GravityZone » (p. 181).

   Les fichiers seront automatiquement transférés dans le répertoire de l'instance hors ligne suivant :

   ```
   /opt/bitdefender/share/gzou/snapshots/
   ```

6.4.6. Utilisation de la console web

Accédez à la console web en saisissant l'IP/le nom d'hôte de l'appliance dans le navigateur. Vous pouvez modifier les options disponibles :

- Le Centre de Contrôle
- Paramètres généraux

Le Centre de Contrôle

Le **Statut appliance** affiche les détails de la dernière tâche effectuée (type d'archive, date et heure) et la prochaine tâche programmée.

Vous avez l'option de :

- **Créer une archive du contenu de sécurité**
- **Créer archive complète**

Dans la rubrique **Archives créées** vous pouvez télécharger les contenus de sécurité et les archives complètes.

Sélectionnez la(les) archive(s) dans la liste disponible, puis cliquez sur le bouton **Télécharger**.

Vous pouvez également voir l'espace disponible sur le lecteur de l'appliance.

Paramètres généraux

Vous pouvez définir un programme pour les kits GravityZone.

1. Cliquez sur le bouton **Modifier paramètres**.
2. Sélectionnez un ou plusieurs kits dans la liste **Kits disponibles**.
3. Dans la section **Planifier**, vous pouvez définir un intervalle de création des archives, ainsi qu'une quantité d'archives à conserver sur le disque.
4. Cliquez sur le bouton **Appliquer** pour enregistrer vos modifications.

7. DÉSINSTALLATION DE LA PROTECTION

Vous pouvez désinstaller et réinstaller les composants GravityZone dans certains cas, comme lorsque vous avez besoin d'utiliser une clé de licence sur une autre machine, de corriger des erreurs ou lors d'une mise à niveau.

Pour désinstaller correctement la protection des endpoints de Bitdefender de votre réseau, suivez les instructions décrites dans ce chapitre.

- Désinstallation de la Protection Endpoint
- Désinstallation de la Protection Exchange
- Désinstallation de la protection pour appareils mobiles
- Désinstaller des rôles serveur de GravityZone

7.1. Désinstallation de la Protection Endpoint

Pour désinstaller en toute sécurité la protection de Bitdefender, vous devez d'abord désinstaller les agents de sécurité, puis le Security Server, si besoin. Si vous souhaitez désinstaller seulement le Security Server, vérifiez que ses agents sont bien connectés à un autre Security Server.

- Désinstallation des agents de sécurité
- Désinstallation de Security Server

7.1.1. Désinstallation des agents de sécurité

Vous avez deux options pour désinstaller les agents de sécurité :

- À distance depuis la Control Center
- Manuellement sur la machine cible

Avertissement
Les agents de sécurité et les Serveurs de Sécurité sont essentiels pour protéger vos endpoints. C'est pourquoi les désinstaller peut mettre votre réseau en danger.

Désinstallation à distance

Pour désinstaller la protection de Bitdefender depuis n'importe quel endpoint administré à distance :

1. Allez sur la page **Réseau**.

2. Sélectionnez **Ordinateur / Machine virtuelle** dans le sélecteur d'affichage.
3. Sélectionnez l'emplacement souhaité dans le panneau de gauche. Tous les ordinateurs du conteneur sélectionné apparaissent dans le tableau du panneau de droite.
4. Sélectionnez les endpoints dont vous souhaitez désinstaller l'agent de sécurité de Bitdefender.
5. Cliquez sur le bouton **Tâches** en haut du tableau et sélectionnez **Désinstaller le client**. Une fenêtre de configuration s'affiche.
6. Dans la fenêtre de tâche de **désinstallation de l'agent** vous pouvez choisir de conserver les fichiers mis en quarantaine sur le endpoint ou de les supprimer.

   Pour les environnements intégrés à VMware vShield, vous devez sélectionner les identifiants requis pour chaque machine, car sinon la désinstallation échoue. Sélectionnez **Utiliser des identifiants pour l'intégration à vShield**, puis ajoutez toutes les données requises dans le tableau Admin. des authentifications qui apparaît en-dessous.
7. Cliquez sur **Enregistrer** pour créer la tâche. Une message de confirmation s'affiche.

Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**.

Si vous souhaitez réinstaller les agents de sécurité, veuillez vous référer à « Installer la protection des postes de travail » (p. 116).

Désinstallation locale

Pour désinstaller manuellement l'agent de sécurité Bitdefender sur une machine Windows :

1. Selon votre système d'exploitation :
   - Sous Windows 7, allez dans **Démarrer> Panneau de configuration > Désinstaller un programme** dans le menu**Programmes**.
   - Sous Windows 8, allez dans **Paramètres> Panneau de configuration > Désinstaller un programme** dans le menu**Programmes**.
   - Sous Windows 8.1, faites un clic droit sur le bouton **Démarrer** puis choisissez **Panneau de configuration > Programmes et fonctionnalités**.
   - Sous Windows 10, allez dans **Démarrer > Paramètres > Système > Applications & fonctionnalités**.

2. Sélectionnez l'agent Bitdefender dans la liste des programmes.
3. Cliquez sur **Désinstaller**.
4. Saisissez le mot de passe de Bitdefender, si l'option est activée dans les politiques de sécurité. Durant la désinstallation, vous pouvez voir la progression de la tâche.

Pour désinstaller manuellement l'agent de sécurité de Bitdefender sur une machine Linux :

1. Ouvrez le terminal.
2. Obtenez l'accès root en utilisant les commandes `su` ou `sudo su`.
3. Naviguez en utilisant la commande `cd` vers le chemin suivant : `/opt/BitDefender/bin`
4. Exécutez le script :

```
# ./remove-sve-client
```

5. Saisissez le mot de passe de Bitdefender pour continuer, si l'option est activée dans les politiques de sécurité.

Pour désinstaller manuellement l'agent de Bitdefender sur un Mac :

1. Allez dans le **Finder > Applications**.
2. Ouvrez le dossier de Bitdefender.
3. Double-cliquez sur **Bitdefender Mac Uninstall**.
4. Dans la fenêtre de confirmation, cliquez à la fois sur **Vérifier** et **Désinstaller** pour continuer.

Si vous souhaitez réinstaller les agents de sécurité, veuillez vous référer à « Installer la protection des postes de travail » (p. 116).

7.1.2. Désinstallation de Security Server

Vous pouvez désinstaller le Security Server de la même façon qu'il a été installé, soit depuis la Control Center, soit depuis l'interface de l'appliance virtuelle GravityZone.

Pour désinstaller le Security Server depuis la Control Center :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Machines virtuelles** dans le sélecteur d'affichage.
3. Sélectionnez le datacenter ou le dossier contenant l'hôte sur lequel le Security Server est installé. Les endpoints sont affichés dans le volet de droite.
4. Cochez la case correspondant à l'hôte sur lequel est installé le Security Server.
5. Dans le menu **Tâches**, sélectionnez **Désinstaller le Security Server**.
6. Saisissez les identifiants vShield (le cas échéant) et cliquez sur **Oui** pour créer la tâche.

Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**.

Quand le Security Server est installé sur la même appliance virtuelle que les autres rôles GravityZone, vous pouvez le supprimer en utilisant l'interface en ligne de commande de l'appliance. Suivez ces étapes :

1. Accédez à la console de l'appliance à partir de votre outil de gestion de la virtualisation (par exemple, vSphere Client).

   Utilisez les flèches et la touche `Tab` pour vous déplacer dans les menus et les options. Appuyez sur `Entrée` pour sélectionner une option spécifique.
2. Dans le menu des **options de l'appliance**, allez dans **Paramètres avancés**.
3. Sélectionnez **Désinstaller le Serveur de Sécurité**. Une fenêtre de confirmation s'affiche.
4. Appuyez sur la touche `Y`, ou appuyez sur `Entrée` tout en ayant sélectionné l'option **Oui**, afin de continuer. Patientez jusqu'à la fin de la désinstallation.

7.2. Désinstallation de la Protection Exchange

Vous pouvez désinstaller la protection Exchange de n'importe quel serveur Microsoft Exchange sur lequel Bitdefender Endpoint Security Tools est installé avec ce rôle. Vous pouvez réaliser la désinstallation depuis la Control Center.

1. Allez sur la page **Réseau**.
2. Sélectionnez **Ordinateur / Machine virtuelle** dans le sélecteur d'affichage.
3. Sélectionnez l'emplacement souhaité dans le panneau de gauche. Les entités seront affichées dans le volet de droite du tableau.
4. Sélectionnez l'endpoint dont vous souhaitez désinstaller la protection Exchange.

5. Cliquez sur **Reconfigurer le client** dans le menu **Tâches**, dans le volet de droite du tableau. Une fenêtre de configuration s'affiche.
6. Dans la section **Général**, décochez la case **Protection Exchange**.

   Avertissement
   Dans la fenêtre de configuration, vérifiez que tous les autres rôles sélectionnés sont actifs sur l'endpoint. Sinon, ils seront aussi désinstallés.

7. Cliquez sur **Enregistrer** pour créer la tâche.

Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**.

Si vous souhaitez réinstaller la protection Exchange, veuillez vous référer à « Installer la protection Exchange » (p. 160).

7.3. Désinstaller Sandbox Analyzer On-Premises

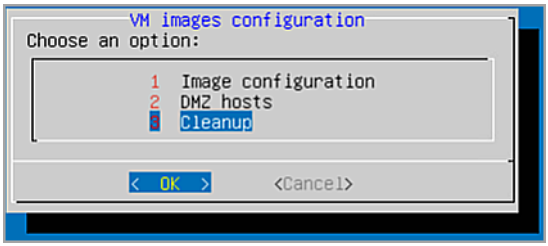
Pour désinstaller Sandbox Analyzer On-Premises :

1. Supprimer les images de machine virtuelle (VM) de la console de l'appliance Sandbox Analyzer.
   a. Connectez-vous à l'interface de l'appliance Sandbox Analyzer.

      Utilisez les flèches et la touche `Tab` pour vous déplacer dans les menus et les options.

      Appuyez sur `Entrée` pour sélectionner une option spécifique.

   b. Dans le menu **Configuration de la sandbox**, recherchez l'option **Images VM**.
   c. Dans le menu **Configuration des images VM**, recherchez l'option **Nettoyage**.



Console de l'appliance Sandbox Analyzer - Configuration de la sandbox - Nettoyage

d. Confirmez que vous voulez supprimer les images de machine virtuelle installées.

   Patientez jusqu'à la fin de l'action. En faisant cela, les données associées aux images de machine virtuelle seront également supprimées.

2. Supprimer l'appliance virtuelle de Sandbox Analyzer :
   a. Désactivez l'appliance virtuelle de Sandbox Analyzer.
   b. Supprimez l'appliance de l'inventaire ESXi.

7.4. Désinstallation de la protection pour appareils mobiles

Lorsque vous supprimez la protection de Bitdefender depuis un appareil mobile, vous devez le faire depuis l'appareil et la Control Center.

Lorsque vous supprimez un appareil de Control Center :

- Le client mobile GravityZone est dissocié mais n'est pas supprimé de l'appareil.
- Tous les journaux liés à l'appareil supprimé sont toujours disponibles.
- Vos informations personnelles et applications ne sont pas affectées.
- Pour les appareils iOS, le Profil MDM est supprimé. Si l'appareil n'est pas connecté à Internet, le Profil MDM demeure installé jusqu'à ce qu'une nouvelle connexion soit disponible.

Avertissement

- Vous ne pouvez pas restaurer les appareils mobiles supprimés.
- Veuillez vérifier que l'appareil cible n'est pas verrouillé avant la suppression. Si vous supprimez par erreur un appareil verrouillé, vous devez restaurer ses paramètres d'usine pour le déverrouiller.

1. Allez sur la page **Réseau**.
2. Sélectionnez **Appareils mobiles** dans le sélecteur de vues.
3. Cliquez sur **Filtres** en haut du volet réseau et sélectionnez **Appareils** dans la catégorie **Afficher**. Cliquez sur **Enregistrer**.
4. Sélectionnez l'emplacement souhaité dans le panneau de gauche. Toues les appareils sont affichés dans le volet de droite du tableau.

5. Cochez la case de l'appareil dont vous souhaitez désinstaller la protection.
6. Cliquez sur ⊖ **Supprimer** en haut du tableau.

Ensuite, vous devez désinstaller l'application de l'appareil.

Pour désinstaller la protection de Bitdefender sur un appareil Android :

1. Allez dans **Sécurité > Administrateurs de l'appareil**.
2. Décochez la case GravityZone. Une fenêtre de confirmation s'affichera.
3. Cliquez sur **Désactiver**. Un message d'alerte est affiché, vous informant que les fonctionnalités antivol ne fonctionneront plus et que vous perdrez l'accès à vos données et réseaux.
4. Désinstallez le client mobile GravityZone comme toute autre application.

Pour désinstaller la protection de Bitdefender sur un appareil iOS :

1. Cliquez sur l'icône du client mobile GravityZone de Bitdefender pendant quelques secondes.
2. Cliquez sur le × cercle associé quand il apparaît. L'application est désinstallée.

Si vous souhaitez réinstaller la protection des appareils mobiles, veuillez vous référer à« Installation de la protection pour appareils mobiles » (p. 162)

7.5. Désinstallation des rôles de l'appliance virtuelle GravityZone

Vous pouvez désinstallé les rôles de l'appliance virtuelle GravityZone via l'interface graphique. Même si vous supprimez l'un d'entre eux, votre réseau est toujours protégé. Néanmoins, vous avez besoin d'au moins une instance de chaque rôle pour faire fonctionner correctement GravityZone.

Dans un scénario avec une seule appliance ayant tous les rôles GravityZone, lorsque vous supprimez un rôle, les endpoints continueront d'être protégés, même si certaines des fonctionnalités de l'appliance ne seront plus disponibles, en fonction de chaque rôle.

Dans un scénario avec plusieurs appliances GravityZone , vous pouvez désinstaller un rôle en toute sécurité tant qu'une autre instance avec le même rôle est disponible. Plusieurs instances de rôles de Serveur de Communication et de Console Web peuvent être installés sur différentes appliances et connectées aux autres rôles

via un "role balancer". Par conséquent, si vous désinstallez une instance d'un rôle spécifique, sa fonction est prise en charge par d'autres.

En cas de besoin, vous pouvez désinstaller le Serveur de Communication depuis une appliance tout en attribuant sa fonction à une autre instance de ce rôle. Pour intégration rapide, suivez ces étapes :

1. Dans la Control Center, allez sur la page **Politiques**.
2. Sélectionnez une politique existante ou cliquez sur **Ajouter** pour en créer une nouvelle.
3. Dans la section **Général**, allez dans **Communication**.
4. Dans le tableau **Affectation des serveurs de communication aux postes de travail**, cliquez sur le champ **Nom**. La liste des serveurs de communication détectés s'affiche.
5. Sélectionnez le Serveur de Communication que vous souhaitez rattacher aux endpoints.
6. Cliquez sur le bouton **Ajouter** à droite du tableau. Si vous avez plus d'un Serveur de Communication dans la liste, vous pouvez configurer leur priorité en utilisant les flèches haut et bas à droite de chaque entité.
7. Cliquez sur **Enregistrer** pour créer la politique. Les endpoints communiqueront avec la Control Center via le Serveur de Communication spécifié.
8. Dans l'interface en ligne de commande GravityZone, désinstallez l'ancien rôle du Serveur de Communication.

Avertissement
Si vous désinstaller l'ancien Serveur de Communication sans paramétrer la politique auparavant, la communication sera perdue de façon permanente et vous devrez réinstaller les agents de sécurité.

Pour désinstaller les rôles de l'appliance virtuelle GravityZone :

1. Conectez-vous à l'interface de la console à partir de votre outil de gestion de la virtualisation (par exemple, vSphere Client). Utilisez les flèches et la touche `Tab` pour vous déplacer dans les menus et les options. Appuyez sur `Entrée` pour sélectionner une option spécifique.
2. Sélectionnez **Paramètres avancés**.

3. Sélectionnez **Installation / désinstallation des rôles**.
4. Allez dans **Ajouter ou supprimer des rôles**.
5. En utilisant la barre `Espace`, désélectionnez tout rôle que vous souhaitez désinstaller, puis appuyez sur `Entrée`. Une fenêtre de confirmation apparaît, vous informant que le rôle va être supprimé.
6. Appuyez sur `Entrée` pour continuer et attendez que la désinstallation soit terminée.

SI vous souhaitez réinstaller un rôle, veuillez vous référer à « Installation / désinstallation des rôles » (p. 103).

8. OBTENIR DE L'AIDE

Bitdefender fait le maximum pour apporter à ses clients une aide fiable, rapide et efficace. Si vous rencontrez le moindre problème ou si avez une question à poser concernant votre produit Bitdefender, consultez notre Centre d'assistance en ligne. Il propose de la documentation que vous pouvez utiliser pour trouver rapidement une solution ou obtenir une réponse. Si vous le désirez, vous pouvez également contacter l'équipe du Service Clients de Bitdefender. Nos membres du support technique répondront à vos questions aussi rapidement que possible et vous fourniront l'assistance dont vous avez besoin.

Note
Vous trouverez des informations sur les services d'aide et de support que nous fournissons ainsi que des détails sur notre politique d'assistance.

8.1. Centre de support de Bitdefender

Le Centre de support de Bitdefender fournit toute l'assistance dont vous avez besoin concernant votre produit Bitdefender.

Vous pouvez utiliser différentes ressources pour trouver rapidement une solution ou une réponse :

- Articles de connaissances de base
- Forum du Support Bitdefender
- Documentations produits

Vous pouvez également utiliser votre moteur de recherche favori pour obtenir plus d'informations sur la sécurité informatique, les produits et l'entreprise Bitdefender.

Articles de connaissances de base

La base de connaissances de Bitdefender est un ensemble d'informations en ligne concernant les produits Bitdefender. Il contient, dans un format facilement accessible, les rapports d'incidents survenus, ainsi que les bugs constatés, par le support technique de Bitdefender. Vous y découvrirez également des articles généraux sur la prévention des antivirus, sur la gestion, en détail, des solutions Bitdefender et beaucoup d'autres articles.

La base de connaissances de Bitdefender est accessible au public et peut être consultée gratuitement. Cet ensemble d'informations est une autre manière de

fournir aux clients de Bitdefender les informations techniques dont ils ont besoin. Toutes les requêtes valides d'informations ou de rapports de bugs provenant de clients Bitdefender trouvent une réponse dans la base de connaissances de Bitdefender, comme les rapports de corrections de bugs, les solutions de rechange ou les articles d'informations venant compléter les fichiers d'aide des produits.

La base de connaissances des produits pour Entreprises de Bitdefender est accessible à tout moment à l'adresse http://www.bitdefender.fr/support/business.html.

Forum du Support Bitdefender

Le Forum du Support Bitdefender fournit aux utilisateurs de Bitdefender une manière simple d'obtenir de l'aide et d'aider les autres. Vous pouvez poster tout problème ou toute question concernant votre produit Bitdefender.

Les techniciens du support Bitdefender surveillent le forum à la recherche de nouvelles publications afin de vous aider. Vous pouvez également obtenir une réponse ou une solution d'un utilisateur Bitdefender plus expérimenté.

Avant de publier un problème ou une question, recherchez s'il existe une rubrique similaire ou connexe dans le forum.

Le forum de support de Bitdefender est disponible à https://forum.bitdefender.com/index.php?showforum=59, dans 5 langues différentes : français, anglais, allemand, espagnol et roumain. Cliquez sur le lien **Protection des entreprises** pour accéder à la section dédiée aux produits pour entreprises.

Documentations produits

La documentation de votre produit est la source d'informations la plus riche.

La manière la plus simple de consulter la documentation est de se rendre sur la page **Aide & Support** de la Control Center. Cliquez sur votre nom d'utilisateur en haut à droite de la console, sélectionnez **Aide & Support** puis le guide qui vous intéresse. Le guide s'ouvrira dans un nouvel onglet de votre navigateur.

Vous pouvez également consulter et télécharger la documentation sur le Centre de support, dans la section **Documentation** disponible sur la page de support de chaque produit.

8.2. Demande d'aide

Vous pouvez demander de l'aide par le biais de notre Centre de support en ligne. Remplissez le formulaire de contact et envoyez-le.

8.3. Utiliser l'Outil de Support

L'Outil de Support GravityZone est conçu pour aider les utilisateurs et les techniciens du support à obtenir facilement les informations dont ils ont besoin pour la résolution des problèmes. Exécutez l'Outil de Support sur les ordinateurs affectés et envoyez l'archive créée avec les informations de résolution de problèmes au représentant du support Bitdefender.

8.3.1. Utiliser l'outil de support sur les systèmes d'exploitation Windows

Exécution de l'application Outil support

Pour générer le journal sur l'ordinateur affecté, suivez l'une de ces méthodes :

- Ligne de commande

  Pour tout problème lorsque BEST est installé sur l'ordinateur.

- Problème d'installation

  Si BEST n'est pas encore installé sur l'ordinateur et que l'installation échoue.

Méthode en ligne de commande

La ligne de commande permet de collecter des fichiers directement depuis l'ordinateur affecté. Cette méthode est à privilégier dans les cas où vous ne pouvez pas accéder au Centre de contrôle GravityZone où lorsque l'ordinateur ne communique pas avec la console.

1. Ouvrez une Invite de commande avec les privilèges administrateur.
2. Rendez-vous dans le dossier d'installation du produit. Le chemin par défaut est le suivant :

   ```
   C:\Program Files\Bitdefender\Endpoint Security
   ```

3. Récupérez et sauvegardez les journaux en exécutant la commande suivante :

```
Product.Support.Tool.exe collect
```

Par défaut, les journaux sont enregistrés dans `C:\Windows\Temp`.

Si vous le voulez, vous pouvez enregistrer le journal de l'Outil Support dans le dossier de votre choix, en utilisant le chemin optionnel :

```
Product.Support.Tool.exe collect [path="<path-to-file>"]
```

Exemple :

```
Product.Support.Tool.exe collect path="D:\Test"
```

Une fois la commande exécutée, une barre de progression apparait à l'écran. Lorsque la procédure est terminée, le nom de l'archive contenant les fichiers journaux et son emplacement apparaissent à l'écran.

Pour envoyer les fichiers journaux à l'équipe de support Bitdefender dédiée aux entreprises, accédez au dossier `C:\Windows\Temp` ou à l'emplacement choisi et sélectionnez le fichier d'archive nommé `ST_[nomordinateur]_[datedujour]`. Joignez l'archive à votre ticket de support pour que la procédure de dépannage puisse se poursuivre.

Problème d'installation

1. Pour télécharger l'Outil Support BEST, cliquez ici.
2. Exécuter le fichier en tant qu'administrateur. Une fenêtre s'ouvre.
3. Choisissez l'emplacement où enregistrer l'archive des fichiers journaux.

   Pendant la collecte des fichiers une barre de progression s'affichera sur l'écran. Une fois le processus achevé, le nom de l'archive et son emplacement apparaissent à l'écran.

Pour envoyer les fichiers journaux à l'équipe de support Bitdefender dédiée aux entreprises, accédez à l'emplacement choisi et sélectionnez le fichier d'archive nommé `ST_[nomordinateur]_[datedujour]`. Joignez l'archive à votre ticket de support pour que la procédure de dépannage puisse se poursuivre.

8.3.2. Utiliser l'outil de support sur les systèmes d'exploitation Linux

Pour les systèmes d'exploitation Linux, l'Outil de Support est intégré à l'agent de sécurité de Bitdefender.

Pour recueillir des informations sur le système Linux à l'aide de l'Outil de Support, exécutez la commande suivante :

```
# /opt/BitDefender/bin/bdconfigure
```

en utilisant les options disponibles suivantes :

- `--help` pour dresser la liste de toutes les commandes de l'Outil de Support
- `enablelogs` pour activer les journaux du module de communication et du produit (tous les services seront redémarrés automatiquement)
- `disablelogs` pour désactiver les journaux du module de communication et du produit (tous les services seront redémarrés automatiquement)
- `deliverall` pour créer :
  - Une archive contenant les journaux du module de communication et du produit, dans le dossier `/tmp` au format suivant : `bitdefender_machineName_timeStamp.tar.gz`.

    Une fois l'archive créée :

    1. L'on vous demandera si vous souhaitez désactiver les journaux. Si nécessaire, les services sont redémarrés automatiquement.
    2. L'on vous demandera si vous souhaitez supprimer les journaux.
- `deliverall -default` fournit les mêmes informations que l'option précédente, mais les actions par défaut s'appliqueront aux journaux, sans que l'utilisateur ne soit consulté (les journaux sont désactivés et supprimés).

Vous pouvez également exécuter la commande `/bdconfigure` directement depuis le package BEST (complet ou downloader) sans que le produit soit installé.

Pour signaler un problème GravityZone affectant vos systèmes Linux, procédez comme indiqué ci-dessous, en utilisant les options décrites précédemment :

1. Activez les journaux du module de communication et du produit.

2. Essayez de reproduire le problème.
3. Désactivez les journaux.
4. Créez l'archive des journaux.
5. Ouvrez un ticket de support par e-mail à l'aide du formulaire disponible sur la page **Aide & Support** de Control Center, avec une description du problème et en joignant l'archive des journaux.

L'Outil de Support pour Linux fournit les informations suivantes :

- Les dossiers `etc`, `var/log`, `/var/crash` (si disponible) et `var/epag` de `/opt/BitDefender`, contenant les journaux et les paramètres de Bitdefender
- Le fichier `/var/log/BitDefender/bdinstall.log`, contenant des informations sur l'installation
- Le fichier `network.txt`, contenant des informations sur la connectivité de la machine / les paramètres du réseau
- Le fichier `product.txt`, y compris le contenu de tous les fichiers `update.txt` dans `/opt/BitDefender/var/lib/scan` et une liste récursive complète de tous les fichiers dans `/opt/BitDefender`
- Le fichier `system.txt`, contenant des informations générales sur le système (versions de la distribution et du noyau, mémoire RAM disponible et espace libre sur le disque dur).
- Le fichier `users.txt`, contenant des informations sur les utilisateurs
- Autres informations concernant le produit liées au système, telles que les connexions externes de processus et l'utilisation du processeur.
- Journaux système

8.3.3. Utiliser l'outil de support sur les systèmes d'exploitation Mac

Lorsque vous envoyez une requête à l'équipe de support locale Bitdefender, vous devez fournir :

- Décrivez de façon détaillée le problème que vous rencontrez.
- Une capture d'écran (si possible) du message d'erreur exact.

- Le Journal Outil suppport.

Pour rassembler des informations sur le système Mac à l'aide de l'Outil support :

1. Téléchargez l'archive ZIP qui contient l'Outil support.
2. Extrayez le fihcier **BDProfiler.tool** de l'archive.
3. Ouvrir une fenêtre de terminal.
4. Naviguez vers l'emplacement du fichier **BDProfiler.tool**.

   Par exemple :

   ```
   cd /Users/Bitdefender/Desktop;
   ```

5. Ajouter des permissions d'exécution au fichier :

   ```
   chmod +x BDProfiler.tool;
   ```

6. Exécutez l'outil.

   Par exemple :

   ```
   /Users/Bitdefender/Desktop/BDProfiler.tool;
   ```

7. Appuyez sur `Y` et saisissez le mot de passe lorsqu'on vous demande de saisir le mot de passe administrateur.

   Attendez quelques minutes que l'outil finisse de générer le journal. Vous trouverez le fichier d'archive qui en résulte (**Bitdefenderprofile_output.zip**) sur votre Bureau.

8.4. Contact

Une communication efficace est la clé d'une relation réussie. Au cours des 18 dernières années, Bitdefender s'est bâti une réputation incontestable dans sa recherche constante d'amélioration de la communication pour dépasser les attentes de ses clients et de ses partenaires. N'hésitez pas à nous contacter pour toute question.

8.4.1. Adresses Web

Ventes : channel-sales@bitdefender.fr
Centre de support en ligne :http://www.bitdefender.fr/support/business.html
Documentation : gravityzone-docs@bitdefender.com
Distributeurs Locaux : https://www.bitdefender.fr/partenaires/trouver-un-partenaire.html
Programme Partenaires : channel-sales@bitdefender.fr
Relations Presse : communication@bitdefender.fr
Virus Submissions: virus_submission@bitdefender.com
Spam Submissions: spam_submission@bitdefender.com
Report Abuse: abuse@bitdefender.com
Site Internet : http://www.bitdefender.com

8.4.2. Distributeurs Locaux

Les distributeurs locaux Bitdefender se tiennent prêts à répondre à vos questions concernant leur zone d'opération, à propos de sujets commerciaux ou généraux.

Pour trouver un distributeur Bitdefender dans votre pays :

1. Allez à https://www.bitdefender.fr/partenaires/trouver-un-partenaire.html.
2. Allez dans **Trouver un partenaire**.
3. Les informations de contact des distributeurs locaux de Bitdefender devraient s'afficher automatiquement. Si ce n'est pas le cas, sélectionnez votre pays de résidence pour afficher les informations.
4. Si vous ne trouvez pas de distributeur Bitdefender dans votre pays, n'hésitez pas à nous contacter par e-mail à l'adresse channel-sales@bitdefender.fr.

8.4.3. Bureaux de Bitdefender

Les bureaux de Bitdefender se tiennent prêts à répondre à vos questions concernant leur zone d'opération, à propos de sujets commerciaux ou généraux. Leur adresse respective et contacts sont listés ci-dessous.

Etats-Unis

Bitdefender, LLC
PO Box 667588
Pompano Beach, Fl 33066

United States
Téléphone (Service commercial et support technique) : 1-954-776-6262
Ventes : sales@bitdefender.com
Site Web : http://www.bitdefender.com
Centre de support en ligne : http://www.bitdefender.com/support/business.html

France

Bitdefender
49, Rue de la Vanne
92120 Montrouge
Fax : +33 (0)1 47 35 07 09
Téléphone : +33 (0)1 47 35 72 73
E-mail : b2b@bitdefender.fr
Site Web : http://www.bitdefender.fr
Centre de support en ligne : http://www.bitdefender.fr/support/business.html

Espagne

Bitdefender España, S.L.U.
Avda. Diagonal, 357, 1º 1ª
08037 Barcelona
España
Fax : (+34) 93 217 91 28
Téléphone (services administratif et commercial) : (+34) 93 218 96 15
Téléphone (support technique) : (+34) 93 502 69 10
Ventes : comercial@bitdefender.es
Site Web : http://www.bitdefender.es
Centre de support en ligne : http://www.bitdefender.es/support/business.html

Allemagne

Bitdefender GmbH
Technologiezentrum Schwerte
Lohbachstrasse 12
D-58239 Schwerte
Deutschland
Téléphone (services administratif et commercial) : +49 (0) 2304 94 51 60
Téléphone (support technique) : +49 (0) 2304 99 93 004
Ventes : firmenkunden@bitdefender.de

Site Web : http://www.bitdefender.de
Centre de support en ligne : http://www.bitdefender.de/support/business.html

Royaume-Uni et Irlande

Genesis Centre Innovation Way
Stoke-on-Trent, Staffordshire
ST6 4BF
UK
Téléphone (Service commercial et support technique) : (+44) 203 695 3415
E-mail : info@bitdefender.co.uk
Ventes : sales@bitdefender.co.uk
Site Web : http://www.bitdefender.co.uk
Centre de support en ligne : http://www.bitdefender.co.uk/support/business.html

Roumanie

BITDEFENDER SRL
Orhideea Towers
15A Orhideelor Street
060071 Bucharest, Sector 6
Fax : +40 21 2641799
Téléphone (Service commercial et support technique) : +40 21 2063470
Ventes : sales@bitdefender.ro
Site Web : http://www.bitdefender.ro
Centre de support en ligne : http://www.bitdefender.ro/support/business.html

Émirats arabes unis

Bitdefender FZ-LLC
Dubai Internet City, Building 17
Office # 160
Dubai, UAE
Téléphone (Service commercial et support technique) : 00971-4-4588935 / 00971-4-4589186
Fax : 00971-4-44565047
Ventes : sales@bitdefender.com
Site Web : http://www.bitdefender.com
Centre de support en ligne : http://www.bitdefender.com/support/business.html

A. Annexes

A.1. Types de fichiers pris en charge

Les moteurs d'analyse anti-malware compris dans les solutions de sécurité de Bitdefender peuvent analyser tous types de fichiers pouvant contenir des menaces. La liste ci-dessous comprend les types de fichiers les plus communément analysés.

{*; 386; 3g2; 3gg; 7z; a6p; ac; accda; accdb; accdc; accde; accdr; accdt; accdu; acl; acm; acr; action; ade; adp; ain; air; app; ar; arc; arj; as; asd; asf; asp; au; avi; awk; ax; bas; bat; bin; bmp; boo; bz; bz2; bzip2; cab; cal; cgi; chm; cla; class; cmd; cnv; com; cpio; cpl; cru; crush; csc; csh; dat; dcx; deb (with gzip, bzip2, xz); dek; dld; dll; dmg (with HFS); doc; docm; docx; dot; dotm; dotx; drv; drw; ds; ds4; dtd; ebm; emf; eml; eps; esh; exe; ezs; fky; frs; fxp; gadget; gif; grv; gx2; gz; gzip; hap; hlp; hms; hta; htm; html; htt; iaf; icd; ico; img; inf; ini; inx; ipf; iso; isu; jar; jfif; jpe; jpeg; jpg; js; jse; jsx; kix; laccdb; lha; lzh; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mid; mmf; mov; mp3; mpd; mpeg; mpg; mpp; mpt; mpx; ms; msg; msi; mso; msp; mst; msu; nws; oab; obd; obi; obs; obt; ocx; odt; oft; ogg; ole; one; onepkg; osci; ost; ovl; pa; paf; pak; pat; pci; pcx; pdf; pex; pfd; pgm; php; pif; pip; png; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; ppz; prc; prf; prg; ps1; psd; psp; pst; pub; puz; pvd; pwc; pwz; py; pyc; pyo; qpx; qt; qxd; ra; ram; rar; rbx; rgb; rgs; rm; rox; rpj; rpm (with cpio, gzip, bzip2, xz); rtf; scar; scr; script; sct; sdr; sh3; shb; shs; shw; sit; sldm; sldx; smm; snp; snt; spr; src; svd; swf; sym; sys; tar; tar.z; tb2; tbz2; td0; tgz; thmx; tif; tiff; tlb; tms; tsp; tt6; u3p; udf; ufa; url; vb; vbe; vbs; vbscript; vwp; vxd; wav; wbk; wbt; wcm; wdm; wiz; wks; wll; wmf; wml; wpc; wpf; wpg; wpk; wpl; ws; ws2; wsc; wsf; wsh; xar; xl; xla; xlam; xlb; xlc; xll; xlm;

xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp; xz; z; zip; zl?; zoo

A.2. Objets de Sandbox Analyzer

A.2.1. Types et extensions de fichier pris en charge pour l'envoi manuel

Les extensions de fichier suivantes sont prises en charge et peuvent être détonées manuellement dans Sandbox Analyzer :

Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML (Unicode), JAR (archive), JS, LNK, MHTML (doc), MHTML (ppt), MHTML (xls), Microsoft Excel, Microsoft PowerPoint, Microsoft Word, MZ/PE files (exécutable), PDF, PEF (exécutable), PIF (exécutable), RTF, SCR, URL (binaire), VBE, VBS, WSF, WSH, WSH-VBS, XHTML.

Sandbox Analyzer est capable de détecter les types de fichiers mentionnés ci-dessus, mais aussi lorsqu'ils sont inclus dans les types de dossiers suivants : 7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, dossier compressé LZMA, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (multivolume), ZOO, XZ.

A.2.2. Types de fichier pris en charge par le préfiltrage de contenu lors de l'envoi automatique

Le préfiltrage de contenu déterminera le type d'un fichier en combinant le contenu et l'extension de l'objet. Ainsi, un exécutable avec l'extension `.tmp` sera reconnu comme une application et, si il est détecté comme étant suspect, il sera envoyé à Sandbox Analyzer.

- Applications - fichiers au format PE32, notamment, mais sans s'y limiter, les extensions suivantes : `exe`, `dll`, `com`.
- Documents - fichiers au format document, notamment, mais sans s'y limiter, les extensions suivantes : `xlsx`, `xls`, `ppt`, `doc`, `docx`, `dot`, `chm`, `xlm`, `docm`, `dotm`, `potm`, `potx`, `ppam`, `ppax`, `pps`, `ppsm`, `pptx`, `sldm`, `sldx`, `xlam`, `xlm`, `xltm`, `rtf`, `pdf`.

- Scripts : `ps, wsf, ws, php, py, js, vb, vbs, pyc, pyo, wsc, wsh, psc1, jse, vbe.`
- Archives : `zip, jar, 7z, bz, bz2, tgz , msi, rar, rev, z, arj, iso, lha, lhz, uu, uue, xxe, lzma, ace, r00.`
- E-mails (sauvegardés dans le système de fichiers) : `eml, tnef.`

A.2.3. Exclusions par défaut de l'envoi automatique

`asc, avi, bmp, gif, jpeg, jpg, mkv, mp4, pgp, png, txt.`

A.2.4. Applications recommandées pour les VM de détonation

Sandbox Analyzer On-Premises nécessite que certaines applications soient installées sur les machines virtuelles de détonation pour qu'elles puissent ouvrir les échantillons envoyés.

Applications	Types de fichiers
Suite Microsoft Office	xls, xltm, xltx, ppt, doc, dotx, docm, potm, potx, ppam, ppax, pps, ppsm, ppsx
Adobe Flash Player	swf
Adobe Acrobat Reader	pdf
Outils Windows par défaut	bat, cmd, ws, wsf, reg, exe, dll, lnk, com, chm, application, gadget, hta, cpl, msc, vbe, jse, wsc, wsh, psc1, scf, vb, vbs, pif
7zip WinZip WinRAR	7z, zip, z, arj, bz, bz2, tgz, jar, r00, ace, lzma, xxe, uue
Google Chrome Internet Explorer	html, url
Python	py, pyc, pyp
Mozilla Thunderbird Microsoft Outlook	eml