Bitdefender

GravityZone

GUÍA DE INSTALACIÓN

Bitdefender GravityZone
Guía de Instalación

fecha de publicación 2021.04.20

Advertencia legal

Advertencia legal

Todos los derechos reservados. Ninguna parte de este libro puede ser reproducida o transmitida de forma alguna, ni por ningún medio, electrónico o mecánico, incluyendo fotocopia, grabación o mediante un sistema de almacenamiento y recuperación, sin la autorización previa por escrito de un representante de Bitdefender. La

Tabla de contenidos

Prólogo

Esta guía va dirigida a los administradores de TI encargados de implementar la protección de GravityZone en las instalaciones de su organización. Los administradores de TI en busca de información sobre GravityZone pueden encontrar en esta guía los requisitos de GravityZone y los módulos de protección disponibles.

Este documento tiene por objetivo explicar la instalación y configuración de la solución GravityZone y sus agentes de seguridad en todo tipo de endpoints de su empresa.

1. Convenciones utilizadas en esta guía

Convenciones Tipográficas

Esta guía recurre a varios estilos de texto para mejorar su lectura. La siguiente tabla le informa sobre dichos estilos y su significado.

Apariencia	Descripción
`ejemplo`	Los nombres de comandos en línea y sintaxis, rutas y nombres de archivos, configuración, salidas de archivos y texto de entrada se muestran en caracteres de `espacio fijo`.
http://www.bitdefender.com	Los enlaces URL le dirigen a alguna localización externa, en servidores http o ftp.
gravityzone-docs@bitdefender.com	Las direcciones de e-mail se incluyen en el texto como información de contacto.
“Prólogo” (p. viii)	Este es un enlace interno, hacia alguna localización dentro del documento.
opción	Todas las opciones del producto se muestran utilizando caracteres en **negrita**.
palabra clave	Las opciones de interfaz, palabras clave o accesos directos se destacan mediante caracteres en **negrita**.

Admoniciones

Las advertencias son notas dentro del texto, marcadas gráficamente, que le facilitan información adicional relacionada con el párrafo que está leyendo.

Nota
La nota es una pequeña observación. Aunque puede omitirla, las notas pueden proporcionar información valiosa, como características específicas o enlaces hacia temas relacionados.

Importante
Esta requiere su atención y no es recommendable saltársela. Normalmente proporciona información importante aunque no extremadamente crítica.

Aviso
Se trata de información crítica que debería tartar con extremada cautela. Nada malo ocurrirá si sigue las indicaciones. Debería leer y entender estas notas, porque describen algo extremadamente peligroso.

1. ACERCA DE GRAVITYZONE

GravityZone es una solución de seguridad empresarial diseñada desde cero para la virtualización y la nube, con el fin de ofrecer servicios de seguridad a endpoints físicos, dispositivos móviles, máquinas virtuales en la nube privada y pública, y servidores de correo de Exchange.

GravityZone es un producto con una consola de administración unificada disponible en la nube, alojada por Bitdefender, o como appliance virtual que se aloja en las instalaciones de la organización, y proporciona un único punto para la implementación, aplicación y administración de las políticas de seguridad para cualquier número de endpoints de cualquier tipo y en cualquier ubicación.

GravityZone aporta múltiples capas de seguridad para endpoints y para los servidores de correo de Microsoft Exchange: antimalware con monitorización del comportamiento, protección contra amenazas de día cero, control de aplicaciones y entorno de pruebas, cortafuego, control de dispositivos, control de contenidos, antiphishing y antispam.

2. CAPAS DE PROTECCIÓN DE GRAVITYZONE

GravityZone proporciona las siguientes capas de protección:

- Antimalware
- Control avanzado de amenazas
- HyperDetect
- Antiexploit avanzado
- Cortafuego
- Control de Contenido
- Administración de parches
- Control de dispositivos
- Cifrado completo del disco duro
- Security for Exchange
- Control de aplicaciones
- Sandbox Analyzer
- Hypervisor Memory Introspection (HVI)
- Network Traffic Security Analytics (NTSA)
- Security for Storage
- Security for Mobile

2.1. Antimalware

La capa de protección antimalware se basa en el análisis de firmas y en el análisis heurístico (B-HAVE, ATC) contra virus, gusanos, troyanos, spyware, adware, keyloggers, rootkits y otros tipos de software malicioso.

La tecnología de análisis antimalware de Bitdefender se basa en las siguientes tecnologías:

- Primero, se utiliza un método de análisis tradicional donde el contenido analizado se compara con la base de datos de firmas. La base de datos de firmas contiene patrones de bytes específicos para conocer los peligros y se actualiza regularmente por Bitdefender. Este método de análisis es efectivo contra amenazas confirmadas que han sido descubiertas y documentadas. Sin embargo, no importa lo rápidamente que se actualice la base de datos de firmas, siempre hay una ventana de tiempo vulnerable entre que la amenaza es descubierta y una solución es lanzada.
- Contra las amenazas de nueva generación indocumentadas, una segunda capa de protección facilitada por **B-HAVE**, un motor heurístico de Bitdefender. Los

algoritmos heurísticos detectan el malware en función de las características de su comportamiento. B-HAVE ejecuta los archivos sospechosos en un entorno virtual para analizar su impacto en el sistema y asegurarse de que no supongan una amenaza. Si se detecta una amenaza, el programa está prevenido de ejecutarlo.

Motores de análisis

Bitdefender GravityZone puede configurar automáticamente los motores de análisis al crear los paquetes de agentes de seguridad según la configuración del endpoint.

El administrador también puede personalizar los motores de análisis, pudiendo elegir entre varias tecnologías de análisis:

1. **Análisis local**, cuando el análisis se realiza localmente en el endpoint. El modo de análisis local es adecuado para máquinas potentes, con los contenidos de seguridad almacenados localmente.
2. **Análisis híbrido con motores ligeros (nube pública)**, con una huella media, que utiliza el análisis en la nube y, parcialmente, los contenidos de seguridad locales. Este modo de análisis conlleva el beneficio de un menor consumo de recursos, aunque implica el análisis fuera de las instalaciones.
3. **Análisis centralizado en la nube pública o privada**, con una huella reducida que requiere un Security Server para el análisis. En este caso, el conjunto de contenidos de seguridad no se almacena localmente y el análisis se descarga en el Security Server.

   Nota
   Existe un reducido conjunto de motores almacenados localmente, necesarios para descomprimir los archivos comprimidos.

4. **Análisis centralizado (análisis en nube pública o privada con Security Server) con reserva* en análisis local (motores completos)**
5. **Análisis centralizado (análisis en nube pública o privada con Security Server) con reserva* en análisis híbrido (nube pública con motores ligeros)**

* Al utilizar análisis con motores duales, cuando el primer motor no esté disponible, se utilizará el motor de reserva. El consumo de recursos y la utilización de la red dependerán de los motores empleados.

2.2. Control avanzado de amenazas

Para las amenazas que logran eludir incluso el motor heurístico, existe otra capa de seguridad denominada Advanced Threat Control (ATC).

Advanced Threat Control monitoriza continuamente los procesos en ejecución y detecta las conductas sospechosas, como por ejemplo los intentos de ocultar el tipo de proceso, ejecutar código en el espacio de otro proceso (secuestro de memoria del proceso para escalado de privilegios), replicar, descartar archivos, ocultarse a las aplicaciones de listado de procesos, etc. Cada comportamiento sospechoso aumenta la calificación del proceso. Cuando se alcanza un límite, salta la alarma.

2.3. HyperDetect

Bitdefender HyperDetect es una capa adicional de seguridad específicamente diseñada para detectar ataques avanzados y actividades sospechosas en la fase previa a la ejecución. HyperDetect incorpora modelos de aprendizaje automático y una tecnología de detección de ataques sigilosos contra amenazas como las de día cero, amenazas persistentes avanzadas (APT), malware ofuscado, ataques sin archivos (uso ilegítimo de PowerShell, Windows Management Instrumentation, etc.), robo de credenciales, ataques selectivos, malware personalizado, ataques basados en scripts, exploits, herramientas de pirateo informático, tráfico de red sospechoso, aplicaciones potencialmente no deseadas (APND) y ransomware.

Nota
Este módulo es un complemento disponible con una clave de licencia independiente.

2.4. Antiexploit avanzado

El Antiexploit avanzado, basado en el aprendizaje automático, es una nueva tecnología proactiva que detiene los ataques de día cero canalizados a través de exploits evasivos. El Antiexploit avanzado ataja los últimos exploits en tiempo real y mitiga las vulnerabilidades de corrupción de memoria que pueden eludir otras soluciones de seguridad. Protege las aplicaciones más habituales, como por ejemplo navegadores, Microsoft Office o Adobe Reader, así como otras que pueda imaginar. Vigila los procesos del sistema y protege contra las violaciones de la seguridad y el secuestro de procesos existentes.

2.5. Cortafuego

El Cortafuego controla el acceso de las aplicaciones a la red y a Internet. Se permite automáticamente el acceso a una amplia base de datos de aplicaciones legítimas y conocidas. Más aun, el cortafuegos puede proteger el sistema contra escaneo de puertos, restringir ICS y avisar cuando se conecten a la red Wi-Fi nuevos nodos.

2.6. Control de Contenido

El módulo de Control de contenidos ayuda a hacer cumplir las políticas de la empresa para el tráfico permitido, el acceso Web, la protección de datos y el control de aplicaciones. Los administradores pueden definir las opciones de análisis de tráfico y las exclusiones, programar el acceso Web bloqueando o permitiendo ciertas categorías Web o URLs, configurar las reglas de protección de datos y definir permisos para el uso de aplicaciones concretas.

2.7. Network Attack Defense

El módulo Network Attack Defense se basa en una tecnología de Bitdefender que se centra en detectar ataques de red diseñados para obtener acceso a endpoints a través de técnicas específicas como ataques de fuerza bruta, exploits de red, ladrones de contraseñas, vectores de infección por descargas ocultas, bots y troyanos.

2.8. Administración de parches

La Administración de parches, que está completamente integrada en GravityZone, mantiene actualizados los sistemas operativos y las aplicaciones de software al tiempo que proporciona visibilidad completa del estado de los parches en los endpoints administrados de Windows.

El módulo de Administración de parches de GravityZone incluye varias características, como análisis de parches bajo demanda o programados, aplicación manual o automática de parches o informes de los parches que faltan.

Puede obtener más información sobre los proveedores y productos compatibles con la Administración de parches de GravityZone en este artículo de la base de conocimientos.

Nota
La Administración de parches es un complemento disponible con una clave de licencia independiente para todos los paquetes de GravityZone existentes.

2.9. Control de dispositivos

El módulo de control de dispositivos permite evitar la fuga de datos confidenciales y las infecciones de malware a través de dispositivos externos conectados a los endpoints. Para ello, aplica políticas con reglas de bloqueo y excepciones a una amplia gama de tipos de dispositivos (como por ejemplo unidades flash USB, dispositivos Bluetooth, reproductores de CD/DVD, dispositivos de almacenamiento, etc.).

2.10. Cifrado completo del disco duro

Esta capa de protección le permite proporcionar un cifrado de disco completo en los endpoints, mediante la administración de BitLocker en Windows y FileVault y diskutil en macOS. Puede cifrar y descifrar los volúmenes, ya sean de arranque o no, con unos pocos clics, mientras que GravityZone gestiona todo el proceso con una mínima intervención de los usuarios. Además, GravityZone almacena las claves de recuperación necesarias para desbloquear los volúmenes cuando los usuarios olvidan sus contraseñas.

Nota
El Cifrado de disco completo es un complemento disponible con una clave de licencia independiente para todos los paquetes de GravityZone existentes.

2.11. Security for Exchange

Bitdefender Security for Exchange ofrece antimalware, antispam, antiphishing y filtrado de contenidos y adjuntos con una magnífica integración en Microsoft Exchange Server, para garantizar un entorno seguro de mensajería y colaboración y aumentar la productividad. Mediante tecnologías antispam y antimalware galardonadas, protege a los usuarios de Exchange contra el malware más reciente y sofisticado y contra los intentos de robo de datos confidenciales y demás información valiosa de los usuarios.

Importante
Security for Exchange está diseñado para proteger toda la organización de Exchange a la que pertenece el Exchange Server protegido. Esto significa que protege todos los buzones activos, incluidos los de usuario/sala/equipo/compartidos.
Además de la protección de Microsoft Exchange, la licencia también cubre los módulos de protección de endpoints instalados en el servidor.

2.12. Control de aplicaciones

El módulo de Control de aplicaciones evita el malware y los ataques de día cero, y aumenta la seguridad sin afectar a la productividad. El Control de aplicaciones pone en práctica políticas flexibles de lista blanca de aplicaciones, lo que sirve para identificar y evitar la instalación y ejecución de aplicaciones no deseadas, poco fiables o maliciosas.

2.13. Sandbox Analyzer

Sandbox Analyzer de Bitdefender proporciona una potente capa de protección contra amenazas avanzadas que realiza un análisis automático y en profundidad de los archivos sospechosos que aún carecen de firma en los motores antimalware de Bitdefender. En el espacio aislado de Sandbox Analyzer se emplea un amplio conjunto de tecnologías de Bitdefender para ejecutar las posibles acciones destructivas en un entorno virtual contenido alojado por Bitdefender o implementado localmente, analizar su comportamiento e informar de cualquier cambio sutil en el sistema que pueda indicar malas intenciones.

Sandbox Analyzer utiliza una serie de sensores para detonar contenidos de los endpoints administrados, la cuarentena centralizada y los servidores ICAP.

Además, Sandbox Analyzer permite el envío de muestras manual y a través de API.

2.14. Hypervisor Memory Introspection (HVI)

Es de sobra conocido que los atacantes con ánimo de lucro altamente organizados buscan vulnerabilidades desconocidas (vulnerabilidades de día cero) o utilizan exploits únicos diseñados específicamente (exploits de día cero) y otras herramientas. Los atacantes también utilizan técnicas avanzadas para retrasar y fragmentar las acciones destructivas de los ataques y así enmascarar sus actividades maliciosas. Los nuevos ataques con ánimo de lucro se diseñan para que sean sigilosos y burlen a las herramientas de seguridad tradicionales.

Para los entornos virtualizados, el problema ya está resuelto: HVI protege centros de datos con una alta densidad de máquinas virtuales contra amenazas avanzadas y sofisticadas que los motores basados en firmas no pueden afrontar. Se impone un fuerte aislamiento, y se garantiza la detección en tiempo real de los ataques, su bloqueo en cuanto se producen y la eliminación inmediata de las amenazas.

Tanto si la máquina protegida es Windows o Linux, como si se trata de un servidor o de un equipo de escritorio, HVI proporciona una visión a un nivel que es imposible alcanzar desde dentro del sistema operativo del guest. Al igual que el hipervisor controla el acceso al hardware en nombre de cada máquina virtual guest, HVI tiene un profundo conocimiento tanto en modo usuario como en modo kernel de la memoria del guest. El resultado es que HVI tiene una visión total de la memoria del guest y, por tanto, un contexto completo. Al mismo tiempo, HVI se aísla de los guests protegidos, dado que el hipervisor en sí está aislado. Al operar a nivel de hipervisor y aprovechar las funcionalidades de este, HVI supera los desafíos técnicos de la seguridad tradicional para revelar la actividad maliciosa en los centros de datos.

HVI identifica las técnicas de ataque en lugar de los patrones de ataque. Así, esta tecnología es capaz de identificar, informar y prevenir técnicas de exploit comunes. El kernel está protegido contra las técnicas de ocultación de rootkits que se utilizan durante la cadena de terminaciones de ataques para que estos pasen desapercibidos. Los procesos en modo usuario también están protegidos contra la inyección de código, el desvío de funciones y la ejecución de código desde la pila o heap.

2.15. Network Traffic Security Analytics (NTSA)

Bitdefender Network Traffic Security Analytics (NTSA) es una solución de seguridad de red que analiza los flujos de tráfico de IPFIX para detectar la presencia de malware y comportamientos maliciosos.

Bitdefender NTSA está pensado para actuar conjuntamente con sus medidas de seguridad existentes, como una protección complementaria capaz de cubrir los puntos ciegos que las herramientas tradicionales no monitorizan.

Las herramientas de seguridad de red tradicionales generalmente intentan evitar infecciones de malware inspeccionando el tráfico entrante (mediante espacios aislados, cortafuegos, antivirus, etc.). Bitdefender NTSA se centra únicamente en monitorizar el tráfico de red saliente en busca de comportamientos maliciosos.

2.16. Security for Storage

GravityZone Security for Storage proporciona protección en tiempo real para los principales sistemas de almacenamiento de red y de uso compartido de archivos. Las actualizaciones del algoritmo de detección de amenazas y del sistema se realizan automáticamente, sin ningún esfuerzo por su parte y sin interrumpir a los usuarios finales.

Dos o más GravityZone Security Server multiplataforma desempeñan el rol de servidor ICAP y proporcionan servicios antimalware para dispositivos de almacenamiento conectados a la red (NAS) y sistemas de uso compartido de archivos que cumplan con el protocolo de adaptación de contenidos de Internet (ICAP, según se define en RFC 3507).

Cuando un usuario solicita abrir, leer, escribir o cerrar un archivo desde un portátil, estación de trabajo, un móvil u otro dispositivo, el cliente ICAP (un NAS o un sistema de uso compartido de archivos) envía una solicitud de análisis al Security Server y recibe un veredicto respecto al archivo. En función del resultado, Security Server permite el acceso, lo deniega o borra el archivo.

Nota
Este módulo es un complemento disponible con una clave de licencia independiente.

2.17. Security for Mobile

Unifica la seguridad en toda la empresa con la administración y control de cumplimiento de dispositivos iPhone, iPad y Android, proporcionando un software de confianza y distribución de actualizaciones a través de las tiendas online de Apple y Android. La solución se ha diseñado para permitir la adopción controlada de iniciativas bring-your-own-device (BYOD) haciendo cumplir las políticas de uso en todos los dispositivos portátiles. Las características de seguridad incluyen el bloqueo de pantalla, control de autenticación, localización del dispositivo, detección de dispositivos rooteados o con jailbreak y perfiles de seguridad. En dispositivos Android el nivel de seguridad se mejora con el análisis en tiempo real y el cifrado de medios extraíbles. Así, los dispositivos móviles se encuentran bajo control y se protege la información sensible que reside en ellos.

2.18. Disponibilidad de capas de protección de GravityZone

La disponibilidad de las capas de protección de GravityZone difiere según el sistema operativo del endpoint. Para obtener más información, consulte el artículo de la base de conocimientos Disponibilidad de capas de protección de GravityZone.

3. ARCHITECTURE GRAVITYZONE

La arquitectura única de GravityZone permite escalar la solución con facilidad y proteger cualquier número de sistemas. GravityZone se puede configurar para utilizar varios appliances virtuales y varias instancias de roles específicos (base de datos, servidor de comunicaciones, servidor de actualizaciones y consola Web) para garantizar la fiabilidad y la escalabilidad.

Cada instancia de rol se puede instalar en un appliance diferente. Los balanceadores de roles integrados aseguran que la implementación de GravityZone protege incluso las redes corporativas más grandes sin ocasionar demoras ni cuellos de botella. También se puede utilizar el hardware o software de equilibrio de carga existente en lugar de los balanceadores incorporados, si la red cuenta con él.

GravityZone, suministrado en un contenedor virtual, se puede importar para ejecutarse en cualquier plataforma de virtualización, incluyendo VMware, Citrix, Microsoft Hyper-V, Nutanix Prism y Microsoft Azure.

La integración con VMware vCenter, Citrix XenServer, Microsoft Active Directory, Nutanix Prism Element y Microsoft Azure reduce el trabajo de implementación de la protección en los endpoints físicos y virtuales.

La solución de GravityZone incluye los siguientes componentes:

- Appliance virtual GravityZone
- Security Server
- Paquete suplementario de HVI
- Agentes de seguridad

3.1. Appliance virtual de GravityZone

La solución GravityZone on-premise se proporciona como appliance virtual reforzado autoconfigurable para Linux Ubuntu, incorporado en una imagen de máquina virtual, fácil de instalar y configurar mediante una CLI (interfaz de línea de comandos). El dispositivo virtual está disponible en varios formatos y es compatible con las principales plataformas de virtualización (OVA, XVA, VHD, OVF, RAW).

3.1.1. Base de datos de GravityZone

La lógica central de la arquitectura de GravityZone. Bitdefender utiliza la base de datos no relacional MongoDB, fácil de escalar y replicar.

3.1.2. Servidor de actualizaciones de GravityZone

El Servidor de actualizaciones tiene la importante misión de actualizar la solución GravityZone y los agentes de endpoint mediante la replicación y la publicación de los paquetes o archivos de instalación necesarios.

3.1.3. Servidor de comunicaciones de GravityZone

El Servidor de comunicaciones es el vínculo entre los agentes de seguridad y la base de datos, y se ocupa de transmitir las políticas y las tareas a los endpoints protegidos, así como los eventos de los que informan los agentes de seguridad.

3.1.4. Consola web (GravityZone Control Center)

Las soluciones de seguridad de Bitdefender se gestionan desde un único punto de administración: la consola web Control Center. Esto proporciona una administración más fácil y acceso a la estrategia de seguridad general y a las amenazas globales contra la seguridad, así como control sobre todos los módulos de seguridad que protegen equipos de escritorio virtuales o físicos, servidores y dispositivos móviles. Equipado con la Arquitectura Gravity, Control Center es capaz de abordar las necesidades de incluso las organizaciones más grandes.

Control Center se integra con los sistemas de monitorización y administración existentes para aplicar fácilmente el sistema de protección a las estaciones de trabajo, servidores o dispositivos móviles no administrados que aparecen en Microsoft Active Directory, VMware vCenter, Nutanix Prism Element o Citrix XenServer, o que simplemente se detectan en la red.

3.1.5. Base de datos del generador de informes

El rol de Base de datos del Generador de informes proporciona los datos necesarios para crear informes basados en consultas.

3.1.6. Procesadores del generador de informes

El rol de Procesadores del Generador de informes es esencial para crear, administrar y almacenar los informes basados en consultas que utilizan la información de la Base de datos del Generador de informes.

3.2. Security Server

El Security Server es una máquina virtual dedicada que deduplica y centraliza la mayoría de las funciones antimalware de los agentes antimalware, actuando como servidor de análisis.

Hay tres versiones de Security Server, para cada tipo de entorno de virtualización:

- **Security Server for VMware NSX.** Esta versión se instala automáticamente en todos los hosts del cluster en los que se haya implementado Bitdefender.
- **Security Server for VMware vShield Endpoint.** Hay que instalar esta versión en cada host que vaya a protegerse.
- **Security Server Multi-Platform.** Esta versión es para otros entornos de virtualización diferentes y se debe instalar en uno o varios hosts con el fin de adaptarse al número de máquinas virtuales protegidas. Cuando utiliza HVI, debe haber instalado un Security Server en cada host que contenga las máquinas virtuales que se deseen proteger.

3.3. Paquete suplementario de HVI

El paquete HVI asegura el enlace entre el hipervisor y el Security Server en ese host. De esta manera, el Security Server es capaz de monitorizar la memoria en uso en el host en el que está instalado en función de las políticas de seguridad de GravityZone.

3.4. Agentes de seguridad

Para proteger su red con Bitdefender, debe instalar los agentes de seguridad de GravityZone apropiados en los endpoints de la red.

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

3.4.1. Bitdefender Endpoint Security Tools

GravityZone garantiza la protección de máquinas físicas y virtuales en Windows y Linux con Bitdefender Endpoint Security Tools, un agente de seguridad inteligente sensible al entorno que se adapta al tipo de endpoint. Bitdefender Endpoint Security Tools se puede implementar en cualquier máquina, ya sea virtual o física, y

proporciona un sistema de análisis flexible que constituye una solución ideal para entornos mixtos (físicos, virtuales y en la nube).

Además de la protección del sistema de archivos, Bitdefender Endpoint Security Tools también proporciona protección al servidor de correo para servidores de Microsoft Exchange.

Bitdefender Endpoint Security Tools utiliza una sola plantilla de política para las máquinas físicas y virtuales y una fuente de kit de instalación para cualquier entorno (físico o virtual) que ejecute Windows.

Capas de protección

Con Bitdefender Endpoint Security Tools hay disponibles las siguientes capas de protección:

- Antimalware
- Control avanzado de amenazas
- HyperDetect
- Cortafuego
- Control de Contenido
- Network Attack Defense
- Administración de parches
- Control de dispositivos
- Cifrado completo del disco duro
- Security for Exchange
- Sandbox Analyzer
- Control de aplicaciones

Roles de endpoint

- Usuario con Permisos
- Relay
- Servidor de almacenamiento en caché de parches
- Protección de Exchange

Usuario con Permisos

Los administradores del Control Center pueden conceder privilegios de Usuario avanzado a los usuarios de endpoints mediante los ajustes de políticas. El módulo de Usuario avanzado otorga privilegios de administración a nivel de usuario, lo que permite al usuario del endpoint acceder a los ajustes de seguridad y modificarlos

a través de una consola local. Control Center recibe una notificación cuando un endpoint está en modo de Usuario avanzado y el administrador de Control Center siempre puede sobrescribir los ajustes de seguridad locales.

Importante
Este módulo solo está disponible para sistemas operativos soportados de servidor y equipos de escritorio Windows. Para más información, diríjase a "Sistemas operativos soportados" (p. 30).

Relay

Los agentes de endpoint con rol de Bitdefender Endpoint Security Tools Relay actúan como servidores de comunicaciones, de actualizaciones y proxy para otros endpoints de la red. Los agentes de endpoint con rol de relay son especialmente necesarios en organizaciones con redes aisladas, donde todo el tráfico se canaliza a través de un único punto de acceso.

En las empresas con grandes redes distribuidas, los agentes de relay ayudan a reducir el uso de ancho de banda, al evitar que los endpoints protegidos y los servidores de seguridad se conecten directamente al appliance de GravityZone.

Una vez que se instala un agente Bitdefender Endpoint Security Tools Relay en la red, se pueden configurar otros endpoints mediante política para comunicarse con Control Center a través del agente de relay.

Los agentes Bitdefender Endpoint Security Tools Relay sirven para lo siguiente:

- Detección de todos los endpoints desprotegidos de la red.
- Implementación del agente de endpoint dentro de la red local.
- Actualización de los endpoints protegidos de la red.
- Garantía de la comunicación entre Control Center y los endpoints conectados.
- Funcionamiento como servidor proxy para endpoints protegidos.
- Optimización del tráfico de red durante las actualizaciones, implementaciones, análisis y otras tareas que consumen recursos.

Servidor de almacenamiento en caché de parches

Los endpoints con rol de relay también pueden actuar como servidor de almacenamiento en caché de parches. Con este rol habilitado, los relays sirven para almacenar parches de software descargados de los sitios web del proveedor y distribuirlos a los endpoints objetivo de su red. Cuando un endpoint conectado tiene software al que le falten parches, los obtiene del servidor y no del sitio web

del proveedor, lo que optimiza el tráfico generado y la carga del ancho de banda de la red.

Importante
Este rol adicional está disponible registrando un complemento de Administración de parches.

Protección de Exchange

Bitdefender Endpoint Security Tools con rol de Exchange se puede instalar en servidores Microsoft Exchange con el fin de proteger a los usuarios de Exchange contra las amenazas de correo.

Bitdefender Endpoint Security Tools con rol de Exchange protege tanto la máquina del servidor como la solución Microsoft Exchange.

3.4.2. Endpoint Security for Mac

Endpoint Security for Mac es un agente de seguridad diseñado para proteger estaciones de trabajo y portátiles Macintosh basados en Intel. La tecnología de análisis disponible es la de **Análisis local**, con contenidos de seguridad almacenados localmente.

Capas de protección

Con Endpoint Security for Mac hay disponibles las siguientes capas de protección:

- Antimalware
- Control avanzado de amenazas
- Control de Contenido
- Control de dispositivos
- Cifrado completo del disco duro

3.4.3. GravityZone Mobile Client

GravityZone Mobile Client extiende fácilmente las políticas de seguridad a cualquier número de dispositivos iOS y Android, protegiéndolos frente a usos no autorizados, riskware y pérdidas de datos confidenciales. Las características de seguridad incluyen el bloqueo de pantalla, control de autenticación, localización del dispositivo, detección de dispositivos rooteados o con jailbreak y perfiles de seguridad. En dispositivos Android el nivel de seguridad se mejora con el análisis en tiempo real y el cifrado de medios extraíbles.

GravityZone Mobile Client se distribuye exclusivamente en la App Store de Apple y en Google Play.

3.4.4. Bitdefender Tools (vShield)

Bitdefender Tools es un agente ligero para entornos virtualizados VMware integrados con vShield Endpoint. El agente de seguridad se instala en máquinas virtuales protegidas por Security Server, lo que le permite aprovechar la funcionalidad adicional que proporciona:

- Le permite ejecutar tareas de análisis de procesos y memoria en la máquina.
- Informa al usuario sobre las infecciones detectadas y las acciones aplicadas sobre ellas.
- Añade más opciones para las exclusiones de análisis antimalware.

3.5. Arquitectura de Sandbox Analyzer

Bitdefender Sandbox Analyzer proporciona una potente capa de protección contra amenazas avanzadas que realiza un análisis automático y en profundidad de los archivos sospechosos que aún carecen de firma en los motores antimalware de Bitdefender.

Sandbox Analyzer está disponible en dos variantes:

- Sandbox Analyzer en la nube, alojado por Bitdefender.
- Sandbox Analyzer On-Premises, disponible como appliance virtual que se puede implementar localmente.

Sandbox Analyzer en la nube

Sandbox Analyzer en la nube contiene los siguientes componentes:

- **Portal de Sandbox Analyzer**: Un servidor de comunicaciones alojado que se utiliza para gestionar las solicitudes entre los endpoints y el cluster de Sandbox Analyzer de Bitdefender.
- **Cluster de Sandbox Analyzer**: La infraestructura alojada del espacio aislado donde se realiza el análisis de comportamiento de la muestra. En este nivel, los archivos enviados se detonan en máquinas virtuales con Windows 7.

GravityZone Control Center actúa como consola de administración y generación de informes, donde se configuran las políticas de seguridad y se visualizan los informes de análisis y las notificaciones.

Bitdefender Endpoint Security Tools, el agente de seguridad instalado en los endpoints, actúa como sensor de alimentación de Sandbox Analyzer.

Sandbox Analyzer On-Premises

Sandbox Analyzer On-Premises se proporciona como appliance virtual Linux Ubuntu, incrustado en una imagen de máquina virtual, fácil de instalar y configurar mediante una interfaz de línea de comandos (CLI). Sandbox Analyzer On-Premises está disponible en formato OVA, implementable en VMware ESXi.

Una instancia de Sandbox Analyzer On-Premises contiene los siguientes componentes:

- **Administrador de espacio aislado**. Este componente es el orquestador del espacio aislado. Sandbox Manager se conecta al hipervisor ESXi mediante API y utiliza sus recursos de hardware para crear y hacer funcionar el entorno de análisis de malware.
- **Máquinas virtuales de detonación**. Este componente consta de máquinas virtuales que Sandbox Analyzer utiliza para ejecutar archivos y analizar su comportamiento. Las máquinas virtuales de detonación pueden ejecutar sistemas operativos Windows 7 y Windows 10 de 64 bits.

GravityZone Control Center actúa como consola de administración y generación de informes, donde se configuran las políticas de seguridad y se visualizan los informes de análisis y las notificaciones.

Sandbox Analyzer On-Premises controla los siguientes sensores de alimentación:

- **Sensor de endpoints**. Bitdefender Endpoint Security Tools para Windows actúa como sensor de alimentación instalado en los endpoints. El agente de Bitdefender utiliza algoritmos avanzados de aprendizaje automático y de redes neuronales para determinar los contenidos sospechosos y enviarlos a Sandbox Analyzer, incluyendo los objetos de la cuarentena centralizada.
- **Sensor de red**. Network Security Virtual Appliance (NSVA) es un appliance virtual implementable en el mismo entorno ESXi virtualizado que la instancia de Sandbox Analyzer. El sensor de red extrae contenidos de los flujos de red y lo envían a Sandbox Analyzer.
- **Sensor ICAP**. Bitdefender Security Server, implementado en dispositivos de almacenamiento conectado a la red (NAS) con el protocolo ICAP, admite el envío de contenidos a Sandbox Analyzer.

Además de estos sensores, Sandbox Analyzer On-Premises admite el envío manual y a través de API. Para más información, consulte el capítulo **Uso de Sandbox Analyzer** de la Guía del administrador de GravityZone.

4. REQUISITOS

Todas las soluciones GravityZone se instalan y administran a través del Control Center.

4.1. Appliance virtual GravityZone

4.1.1. Plataformas de virtualización y formatos compatibles

GravityZone se distribuye como appliance virtual. Está disponible en los siguientes formatos, compatibles con las plataformas de virtualización más habituales:

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

*Los paquetes OVF y RAW se comprimen en formato tar.bz2.

En cuanto a la compatibilidad con la plataforma Oracle VM VirtualBox, consulte este artículo de la base de conocimientos.

A petición puede proporcionarse soporte para otros formatos y plataformas de virtualización.

4.1.2. Hardware

Los requisitos de hardware del appliance virtual GravityZone varían en función del tamaño de su red y de la arquitectura de implementación que elija. Para redes de hasta 3000 endpoints, puede optar por instalar todos los roles de GravityZone en un solo appliance, mientras que para redes más grandes, debe plantearse distribuir los roles entre varios appliances. Los recursos requeridos por el appliance dependen de los roles que instale en él y de si usa o no el Conjunto de réplicas.

Nota
El Conjunto de réplicas es una característica de MongoDB que mantiene réplicas de las bases de datos y garantiza la redundancia y la alta disponibilidad de los datos almacenados. Para más información, consulte la documentación de MongoDB y "Administrar el appliance GravityZone" (p. 109).

Bitdefender HVI también solicita una cantidad notable de recursos. Si usa este servicio, consulte las tablas con los datos concretos. Para conocer todos los requisitos del sistema, consulte "HVI" (p. 50).

Importante
Las mediciones son el resultado de las pruebas internas de Bitdefender con una configuración básica de GravityZone y un uso normal. Los resultados pueden variar según la configuración de la red, el software instalado, la cantidad de eventos generados, etc. Para obtener métricas de escalabilidad personalizadas, póngase en contacto con Bitdefender.

vCPU

La siguiente tabla le informa de la cantidad de vCPU que solicita cada rol del appliance virtual.

Cada vCPU debe ser al menos de 2 GHz.

Módulo	Cantidad de endpoints (hasta)							
	250	500	1000	3000	5000	10000	25000	50000
Características básicas de GravityZone								
Servidor de actualizaciones*	8	12	14	16	4	4	6	8
Consola web**					6	10	12	12
Servidor de comunicaciones					6	10	12	18
Base de datos***					6	6	9	12
Total	**8**	**12**	**14**	**16**	**22**	**30**	**39**	**50**
GravityZone con Bitdefender HVI								
Servidor de actualizaciones*	8	4	4	4	4	4	6	8
Consola web**		6	8	8	10	10	12	12
Servidor de comunicaciones		6	8	8	10	10	16	20

Módulo	Cantidad de endpoints (hasta)							
	250	500	1000	3000	5000	10000	25000	50000
Base de datos***		6	6	6	6	6	9	12
Total	**8**	**22**	**26**	**26**	**30**	**30**	**43**	**52**

* Recomendado cuando no se implementan relays.
** Para cada integración activa, añada una vCPU al appliance virtual con el rol de Consola web.
*** En caso de instalaciones distribuidas de roles, junto con el Conjunto de réplicas: para cada instancia de base de datos adicional, añada el número especificado a la cantidad total.

RAM (GB)

Módulo	Cantidad de endpoints (hasta)							
	250	500	1000	3000	5000	10000	25000	50000
Características básicas de GravityZone								
Update Server	16	16	18	20	2	2	3	3
Consola web*					8	8	12	16
Servidor de comunicaciones					6	12	12	16
Base de datos**					8	10	12	12
Total	**16**	**16**	**18**	**20**	**24**	**32**	**39**	**47**
GravityZone con Bitdefender HVI								
Update Server	16	2	2	2	2	2	3	3
Consola web*		8	10	10	10	10	12	16
Servidor de comunicaciones		8	10	10	12	12	16	20
Base de datos**		8	8	8	8	12	12	12
Total	**16**	**26**	**30**	**30**	**32**	**36**	**43**	**51**

* Para cada integración activa, añada 1 GB de RAM al appliance virtual con el rol de Consola web.

** En caso de instalación distribuida de roles, junto con el Conjunto de réplicas: para cada instancia de base de datos adicional, añada el número especificado a la cantidad total.

Espacio libre en disco (GB)

Módulo	Cantidad de endpoints (hasta)								
	250	250*	500	1000	3000	5000	10000	25000	50000
Características básicas de GravityZone									
Update Server	120	**160**	160	200	200	80	80	80	80
Consola Web						80	80	80	80
Servidor de comunicaciones						80	80	80	80
Base de datos**						80	120	200	500
Total	**120**	**160**	**160**	**200**	**200**	**320**	**360**	**440**	**740**
GravityZone con Bitdefender HVI									
Update Server	120	160	80	80	80	80	80	80	80
Consola Web			80	80	80	80	80	80	80
Servidor de comunicaciones			80	80	80	80	80	80	80
Base de datos**			80	80	100	100	160	300	700
Total	**120**	**160**	**320**	**320**	**340**	**340**	**400**	**540**	**940**

Importante
Se recomienda encarecidamente utilizar unidades de estado sólido (SSD).

* Si se opta por la instalación automática, se necesita espacio SSD adicional, ya que también instala Security Server. Una vez finalizada la instalación, puede desinstalar Security Server para liberar espacio en disco.
** En caso de instalación distribuida de roles, junto con el Conjunto de réplicas: para cada instancia de base de datos adicional, añada el número especificado a la cantidad total.

4.1.3. Conexión de Internet

El appliance GravityZone necesita conexión a Internet.

4.2. Control Center

Para acceder a la consola web Control Center, es necesario lo siguiente:

- Internet Explorer 9 o superior, Mozilla Firefox 14 o superior, Google Chrome 15 o superior, Safari 5 o superior, Microsoft Edge 20 o superior, Opera 16 o superior
- Resolución de pantalla recomendada: 1280 x 800 o superior
- El equipo desde donde se conecte debe tener conexión de red con Control Center.

Aviso
Control Center no funcionará o se mostrará correctamente en Internet Explorer 9+ con la Vista de compatibilidad habilitada, que equivaldría a utilizar una versión de navegador no soportada.

4.3. Protección de endpoint

Para proteger su red con Bitdefender, debe instalar los agentes de seguridad de GravityZone en los endpoints de la red. Para una protección optimizada, también puede instalar Security Server. A tal fin, necesita un usuario de Control Center con privilegios de administración sobre los servicios que precise instalar y sobre los endpoints de la red bajo su administración.

Los requisitos para el agente de seguridad son diferentes en función de si tiene roles de servidor adicionales, como por ejemplo Relay, Protección de Exchange o Servidor de almacenamiento en caché de parches. Para obtener más información sobre los roles de los agentes, consulte “Agentes de seguridad” (p. 13).

4.3.1. Hardware

Agente de seguridad sin roles

Uso CPU

Sistemas objetivo	Tipo CPU	Sistemas operativos compatibles (SO)
Estaciones de trabajo	Procesador compatible Intel® Pentium a 2 GHz o más	Sistemas operativos de equipos de escritorio Microsoft Windows
	Intel® Core 2 Duo, 2 GHz o más	macOS
Dispositivos inteligentes	Procesador compatible Intel® Pentium a 800 MHz o más	SO integrados Microsoft Windows
Servidores	Mínimo: Procesador compatible Intel® Pentium a 2,4 GHz	SO Microsoft Windows Server y SO Linux
	Recomendado: CPU multinúcleo Intel® Xeon, 1,86 GHz o más	

Aviso
Los procesadores ARM no son compatibles actualmente.

Memoria RAM libre

En la instalación (MB)

SO	MOTOR ÚNICO					
	Análisis local		Análisis híbrido		Análisis central.	
	Solo AV	Opc. complet.	Solo AV	Opc. complet.	Solo AV	Opc. complet.
Windows	1024	1200	512	660	256	400
Linux	1024	1024	512	512	256	256
macOS	1024	1024	n/a	n/a	n/a	n/a

Para el uso diario (MB)*

SO	Antivirus (motor único)			Módulo de protección			
	Local	Híbrido	Centralizado	Análisis comportamiento	Cortafuego	Control contenidos	Usu avan
Windows	75	55	30	+13	+17	+41	+2
Linux	200	180	90	-	-	-	-
macOS	650	-	-	+100	-	+50	-

* Las cantidades cubren el uso diario de clientes de endpoint, sin tener en cuenta las tareas adicionales, como análisis bajo demanda o actualizaciones de productos.

Espacio Libre en Disco

En la instalación (MB)

SO	MOTOR ÚNICO						MOTOR DUAL			
	Análisis local		Análisis híbrido		Análisis central.		Análisis local + central.		Análisis híbrido + central.	
	Solo AV	Opc. complet.	Solo AV	Opc. complet.	Solo AV	Opc. complet.	Solo AV	Opc. complet.	Solo AV	Opc. complet.
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/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a

Para el uso diario (MB)*

SO	Antivirus (motor único)			Módulo de protección			
	Local	Híbrido	Centralizado	Análisis comportamiento	Cortafuego	Control contenidos	Usua avanz
Windows	410	190	140	+12	+5	+60	+8
Linux	500	200	110	-	-	-	-
macOS	1700	-	-	+20	-	+0	-

* Las cantidades cubren el uso diario de clientes de endpoint, sin tener en cuenta las tareas adicionales, como análisis bajo demanda o actualizaciones de productos.

Agente de seguridad con rol de Relay

El rol de Relay necesita recursos de hardware adicionales a la configuración básica del agente de seguridad. Estos requisitos se deben al Servidor de actualizaciones y a los paquetes de instalación alojados por el endpoint:

Número de endpoints conectados	CPU para el Servidor de actualizaciones	RAM	Espacio libre en disco para el Servidor de actualizaciones
1-300	Mínimo: Procesador Intel® Core™ i3 o equivalente, 2 vCPU por núcleo	1.0 GB	10 GB
300-1000	Mínimo: Procesador Intel® Core™ i5 o equivalente, 4 vCPU por núcleo	1.0 GB	10 GB

Aviso

- Los procesadores ARM no son compatibles actualmente.
- Los agentes de relay requieren discos SSD debido a la gran cantidad de operaciones de lectura y escritura.

Importante

- Si desea guardar los paquetes de instalación y las actualizaciones en otra partición distinta a donde está instalado el agente, asegúrese de que ambas particiones tengan suficiente espacio libre en el disco (10 GB) pues, de lo contrario, el agente abortará la instalación. Esto solo es necesario en la instalación.
- En los endpoints de Windows, deben habilitarse los vínculos simbólicos local a local.

Agente de seguridad con rol de Protección de Exchange

La cuarentena para servidores de Exchange requiere espacio de disco duro adicional en la partición donde esté instalado el agente de seguridad.

El tamaño de la cuarentena depende del número de elementos almacenados y de su tamaño.

Por defecto, el agente se instala en la partición del sistema.

Agente de seguridad con rol de Servidor de almacenamiento en caché de parches

El agente con el rol de Servidor de almacenamiento en caché de parches debe cumplir los siguientes requisitos acumulativos:

- Todos los requisitos de hardware del agente de seguridad simple (sin roles)
- Todos los requisitos de hardware del rol de Relay
- Además, 100 GB de espacio libre en el disco para almacenar los parches descargados

Importante
Si desea guardar los parches en otra partición distinta a donde está instalado el agente, asegúrese de que ambas particiones tengan suficiente espacio libre en el disco (100 GB) pues, de lo contrario, el agente abortará la instalación. Esto solo es necesario en la instalación.

Requisitos para entornos VMware vShield

Estos son los requisitos de Bitdefender Tools y huellas para sistemas integrados en entornos VMware con vShield Endpoint.

Plataforma	RAM	Espacio en disco
Windows	6-16* MB (~ 10 MB para GUI)	24 MB
Linux	9-10 MB	10-11 MB

*5 MB cuando está activa la opción Modo silencioso y 10 MB cuando está desactivada. Cuando se habilita el modo silencioso, la interfaz gráfica de usuario (GUI) de Bitdefender Tools no se carga automáticamente al inicio del sistema, con lo que se liberan los recursos correspondientes.

4.3.2. Sistemas operativos soportados

Equipo de escritorio de 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)
- Windows 10 October 2018 Update (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

Aviso

(1) La compatibilidad con Windows 8.1 (32 y 64 bits) para la plataforma VMware vShield (versión sin agente) está disponible con VMware vSphere 5.5 – ESXi compilación 1892794 y posteriores.
(2) En VMware NSX, la versión del sistema operativo es compatible a partir de vSphere 5.5 Patch 2.
(3) En VMware NSX, la versión del sistema operativo es compatible a partir de vSphere 5.5.

Aviso

Bitdefender no es compatible con las compilaciones del programa Windows Insider.

Windows incorporado y de tablet

- 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

Servidor Windows

- 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)]

Aviso

(1) La compatibilidad con Windows Server 2012 R2 (64 bits) para la plataforma VMware vShield (versión sin agente) está disponible con VMware vSphere 5.5 – ESXi compilación 1892794 y posteriores.
(2) En VMware NSX, la versión del sistema operativo es compatible a partir de vSphere 5.5 Patch 2.
(3) En VMware NSX, la versión del sistema operativo es compatible a partir de vSphere 5.5.
(4) VMware NSX no es compatible con las versiones de 32 bits de Windows 2012 y Windows Server 2008 R2.

Linux

Importante

Los endpoints de Linux utilizan puestos de licencia del grupo de licencias para sistemas operativos de servidor.

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

Aviso

(1) En Fedora 28 y superior, Bitdefender Endpoint Security Tools requiere la instalación manual del paquete `libnsl` mediante la ejecución del siguiente comando:

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

(2) Para instalaciones mínimas de CentOS, Bitdefender Endpoint Security Tools requiere la instalación manual del paquete `libnsl` mediante la ejecución del siguiente comando:

```
sudo yum install libnsl
```

Requisitos previos de Active Directory

Al integrar endpoints de Linux con un dominio de Active Directory a través del daemon de servicios de seguridad del sistema (SSSD), asegúrese de que estén instaladas las herramientas **ldbsearch, krb5-user,** y **krb5-config** y que kerberos esté correctamente configurado.

```
/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
        }
```

Nota
Todas las entradas distinguen mayúsculas de minúsculas.

Compatibilidad para análisis on-access

El análisis on-access está disponible para todos los sistemas operativos guest soportados. En sistemas Linux, se proporciona soporte de análisis on-access en las siguientes situaciones:

Versiones del kernel	Distribuciones Linux	Requisitos on-access
2.6.38 o superior*	Red Hat Enterprise Linux / CentOS 6.0 o superior Ubuntu 14.04 o superior SUSE Linux Enterprise Server 11 SP4 o superior OpenSUSE Leap 42.x Fedora 25 o superior Debian 9.0 o superior Oracle Linux 6.3 o superior Amazon Linux AMI 2016.09 o superior	**Fanotify** (opción del kernel) debe estar habilitado.
2.6.38 o superior	Debian 8	**Fanotify** debe estar habilitado y establecido en modo de aplicación obligatoria y, luego, hay que recompilar el paquete del kernel. Para más información, consulte este artículo de la base de conocimientos.
2.6.32 - 2.6.37	CentOS 6.x Red Hat Enterprise Linux 6.x	Bitdefender proporciona soporte mediante **DazukoFS** con módulos del kernel precompilados.
Todos los demás kernels	Todos los demás sistemas compatibles	El módulo **DazukoFS** debe compilarse manualmente. Para obtener más información, consulte "Compilación manual del módulo DazukoFS" (p. 157).

* Con ciertas limitaciones descritas más adelante.

Limitaciones de análisis on-access

Versiones del kernel	Distribuciones Linux	Detalles
2.6.38 o superior	Todos los sistemas compatibles	El análisis on-access solo monitoriza los recursos compartidos montados bajo las siguientes condiciones: • **Fanotify** está activado tanto en sistemas remotos como locales. • El recurso compartido se basa en los sistemas de archivos CIFS y NFS. **Nota** El análisis on-access no analiza los recursos compartidos montados utilizando SSH o FTP.
Todos los kernels	Todos los sistemas compatibles	No se admite el análisis on-access en sistemas con **DazukoFS** para recursos compartidos montados en rutas ya protegidas por el módulo on-access.

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)

El Control de contenido no es compatible con macOS Big Sur (11.0).

4.3.3. Sistemas de archivo compatibles

Bitdefender se instala y protege los siguientes sistemas de archivos:

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

Nota
El análisis on-access no es compatible con NFS ni CIFS/SMB.

4.3.4. Navegadores soportados

Se ha comprobado el funcionamiento de la seguridad del navegador del endpoint con los siguientes navegadores:

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

4.3.5. Plataformas de virtualización soportadas

Security for Virtualized Environments proporciona soporte instantáneo para las siguientes plataformas de virtualización:

- VMware vSphere y 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

  Nota
  La funcionalidad de administración de cargas de trabajo en vSphere 7.0 no es compatible.

- 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
- VMware Player 7.x, 6.x, 5.x
- Citrix XenServer 8.x, 7.x, 6.5, 6.2, 6.0, 5.6 o 5.5 (incluyendo Xen Hypervisor)
- Citrix Virtual Apps y Desktops 7 1808, 7 1811, 7 1903, 7 1906
- Citrix XenApp y 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 o Windows Server 2008 R2, 2012, 2012 R2 (incluyendo Hyper-V Hypervisor)
- Red Hat Enterprise Virtualization 3.0 (incluyendo 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

Nota
A petición puede proporcionarse soporte para otras plataformas de virtualización.

Requisitos de integración con VMware NSX-V

- ESXi 5.5 o posterior para cada servidor
- vCenter Server 5.5 o posterior
- NSX Manager 6.2.4 o posterior
- VMware Tools 9.1.0 o posterior, con agente ligero de Guest Introspection.
  - Para máquinas virtuales Windows, consulte el siguiente artículo de VMware Docs.
  - Para máquinas virtuales Linux, consulte el siguiente artículo de VMware Docs.

Nota
VMware recomienda utilizar las siguientes versiones de VMware Tools:
- 10.0.8 o posterior, para resolver máquinas virtuales lentas después de actualizar VMware Tools en NSX / vCloud Networking and Security (artículo 2144236 de la base de conocimientos de VMware).
- 10.0.9 y posterior para Windows 10.

Importante
Se recomienda mantener todos sus productos VMware actualizados con el último parche.

Requisitos de integración con VMware NSX-T Data Center

- VMware NSX-T Manager 2.4, 2.5 o 3.0
- ESXi compatible con la versión de NSX-T Manager
- vCenter Server y vSphere compatibles con la versión de NSX-T Manager
- VMware Tools con agente ligero de Guest Introspection, compatible con la versión de NSX-T Manager

Para obtener más información sobre la compatibilidad, consulte estas páginas web de VMware:

- Guía de compatibilidad de VMware: GravityZone vs. NSX-T Manager
- Matrices de interoperabilidad de productos de VMware: NSX-T Data Center vs. VMware vCenter y VMware Tools

Requisitos de integración con Nutanix Prism Element

- Credenciales de un Nutanix Prism Element con privilegios administrativos (administrador de cluster o administrador de usuarios).
- 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

Plataformas de nube admitidas

Además de con los entornos de virtualización on-premise, GravityZone también se puede integrar con las siguientes plataformas en la nube:

- **Amazon EC2**

  Como cliente de Amazon EC2, puede integrar el inventario de instancias de EC2 agrupadas por regiones y zonas de disponibilidad con el inventario de red de GravityZone.

- **Microsoft Azure**

Como cliente de Microsoft Azure, puede integrar las máquinas virtuales de Microsoft Azure agrupadas por regiones y zonas de disponibilidad con el inventario de red de GravityZone.

Compatibilidad con tecnologías de virtualización de aplicaciones y escritorios

GravityZone es compatible con las siguientes tecnologías de virtualización, a partir de Bitdefender Endpoint Security Tools versión 6.6.16.226:

- **VMware:**

  VMware V-App (la misma versión con vCenter Server)

  VMware ThinApp 5.2.6

  VMware AppVolumes 2.180

  Importante
  Se recomienda no instalar en pila de aplicaciones o volúmenes escribibles.

- **Microsoft:**

  Microsoft App-V 5.0, 5.1

  Microsoft FSLogix 2.9.7237

- **Citrix:**

  Citrix App Layering 19.10

  Citrix Appdisks 7.12

  Importante
  Asigne políticas basadas en reglas de usuario para que el Control de dispositivos no impida la creación de capas de plataforma y sistema operativo.
  Es posible que deba configurar las reglas del cortafuego de GravityZone para permitir el tráfico de red para cada una de estas aplicaciones. Para más información, consulte la documentación del producto Citrix App Layering.

Herramientas de administración de la virtualización soportadas

Control Center se integra actualmente con las siguientes herramientas de administración de la virtualización:

- VMware vCenter Server

- Citrix XenServer
- Nutanix Prism Element

Para configurar la integración debe proporcionar el nombre de usuario y contraseña de administrador.

4.3.6. Security Server

Security Server es una máquina virtual preconfigurada ejecutada en un Ubuntu Server con las siguientes versiones:

- 16.04 (VMware NSX y Multi-Platform)
- 12.04 LTS (VMware vShield)

Memoria y CPU

La asignación de recursos de memoria y CPU para el Security Server depende del número y tipo de máquinas virtuales ejecutadas en el host. La siguiente tabla indica los recursos recomendados que deben asignarse:

Número de MVs protegidas	RAM	CPUs
1-50 MVs	2 GB	2 CPUs
51-100 MVs	2 GB	4 CPUs
101-200 MVs	4 GB	6 CPUs

Security Server para NSX viene con una configuración predefinida de hardware (CPU y RAM), que puede ajustar en VMware vSphere Web Client apagando la máquina, modificando sus ajustes y, luego, volviendo a encenderla. Para información detallada, diríjase a "Instalación de Security Server para VMware NSX" (p. 127).

Espacio en disco duro

Entorno	Aprovisionamiento de espacio en disco duro
VMware NSX-V/NSX-T	40 GB
VMware con vShield Endpoint	40 GB
Otro	16 GB

Distribución del Security Server en los hosts

Entorno	Security Server frente a hosts
VMware NSX-V/NSX-T	Security Server se instala automáticamente en cada host ESXi del cluster que se ha de proteger en el momento de la implementación del servicio de Bitdefender.
VMware con vShield Endpoint	Security Server debe estar instalado en cada host ESXi a proteger.
Otro	Aunque no es obligatorio, Bitdefender recomienda instalar Security Server en cada host físico para mejorar el rendimiento.

Latencia de red

La latencia de comunicación entre el Security Server y los endpoints protegidos debe ser inferior a 50 ms.

Carga de Protección de almacenamiento

El impacto de la Protección de almacenamiento en Security Server al analizar 20 GB es el siguiente:

Estado de Protección de almacenamiento	Recursos de Security Server	Carga de Security Server	Tiempo de transferencia (mm:ss)
Desactivado (base de referencia)	N/A	N/A	10:10
Activado	4 vCPU 4 GB RAM	Normal	10:30
Activado	2 vCPU 2 GB RAM	Pesado	11:23

Nota
Estos resultados se obtienen con una muestra de varios tipos de archivos (.exe, .txt, .doc, .eml, .pdf, .zip, etc.), que van de 10 KB a 200 MB. La duración de la transferencia corresponde a 20 GB de datos contenidos en 46 500 archivos.

4.3.7. Uso de tráfico

- **Tráfico de actualizaciones de producto entre el cliente de endpoint y el servidor de actualizaciones**

  Las actualizaciones periódicas del producto Bitdefender Endpoint Security Tools generan el siguiente tráfico de descarga en cada cliente de endpoint:

  - En sistemas operativos Windows: ~20 MB
  - En sistemas operativos Linux: ~26 MB
  - En macOS: ~25 MB

- **Tráfico de actualizaciones de contenidos de seguridad descargados entre el cliente de endpoint y el Servidor de actualizaciones (MB/día)**

Tipo de Servidor de actualizaciones	Tipo de motor de análisis		
	Local	Híbrido	Central.
Relay	65	58	55
Servidor de actualizaciones público de Bitdefender	3	3.5	3

- **Tráfico de análisis centralizado entre el cliente de endpoint y Security Server**

Objetos analizados	Tipo tráfico		Bajada (MB)	Subida (MB)
Archivos*	Primer análisis		27	841
	Análisis en caché		13	382
Sitios Web**	Primer análisis	tráfico web	621	N/A
		Security Server	54	1050
	Análisis en caché	tráfico web	654	N/A
		Security Server	0.2	0.5

* Los datos proporcionados se han medido con 3,49 GB de archivos (6658 archivos), de los cuales 1,16 GB eran archivos portables ejecutables (PE).

** Los datos proporcionados se han medido para los 500 sitios Web mejor clasificados.

- **Tráfico de análisis híbrido entre el cliente de endpoint y Cloud Services de Bitdefender**

Objetos analizados	Tipo tráfico	Bajada (MB)	Subida (MB)
Archivos*	Primer análisis	1.7	0.6
	Análisis en caché	0.6	0.3
tráfico web**	tráfico web	650	N/A
	Cloud Services de Bitdefender	2.6	2.7

  * Los datos proporcionados se han medido con 3,49 GB de archivos (6658 archivos), de los cuales 1,16 GB eran archivos portables ejecutables (PE).

  ** Los datos proporcionados se han medido para los 500 sitios Web mejor clasificados.

- **Tráfico entre los clientes Bitdefender Endpoint Security Tools Relay y el Servidor de actualizaciones para descargar contenidos de seguridad**

  Los clientes con rol de Bitdefender Endpoint Security Tools Relay descargan ~16 MB / día* del servidor de actualizaciones.

  * Disponible con clientes Bitdefender Endpoint Security Tools a partir de la versión 6.2.3.569.

- **Tráfico entre clientes de endpoint y la consola web Control Center**

  Se genera un promedio de tráfico de 618 KB/día entre los clientes de endpoint y la consola Web Control Center.

4.4. Protección de Exchange

Security for Exchange se proporciona a través de Bitdefender Endpoint Security Tools, que puede proteger tanto el sistema de archivos como el servidor de correo de Microsoft Exchange.

4.4.1. Entornos de Microsoft Exchange compatibles

Security for Exchange es compatible con los siguientes roles y versiones de Microsoft Exchange:

- Exchange Server 2019 con rol de transporte perimetral o de buzón
- Exchange Server 2016 con rol de transporte perimetral o de buzón

- Exchange Server 2013 con rol de transporte perimetral o de buzón
- Exchange Server 2010 con rol de transporte perimetral, transporte de concentradores o de buzón
- Exchange Server 2007 con rol de transporte perimetral, transporte de concentradores o de buzón

Security for Exchange es compatible con Microsoft Exchange Database Availability Groups (DAGs).

4.4.2. Requisitos del Sistema

Security for Exchange es compatible con cualquier servidor de 64 bits físico o virtual (Intel o AMD) que ejecute un rol y versión compatible de Microsoft Exchange Server. Para más información sobre los requisitos del sistema de Bitdefender Endpoint Security Tools, consulte "Agente de seguridad sin roles" (p. 26).

Disponibilidad de recursos del servidor recomendada:

- Memoria RAM libre: 1 GB
- Espacio libre en disco: 1 GB

4.4.3. Otros requisitos de software

- Para Microsoft Exchange Server 2013 con Service Pack 1: KB2938053 de Microsoft.
- Para Microsoft Exchange Server 2007: .NET Framework 3.5 Service Pack 1 o superior

4.5. Sandbox Analyzer On-Premises

Sandbox Analyzer On-Premises tiene los siguientes requisitos específicos:

- ESXi Hypervisor (la plataforma de virtualización que ejecutará el entorno).
- Appliance virtual Sandbox Analyzer (el appliance de administración que controlará las máquinas virtuales de detonación).
- Appliance virtual de seguridad de red (una máquina virtual que encapsula un sensor de red capaz de extraer las cargas útiles del tráfico de red).
- Conectividad con un GravityZone Control Center existente utilizado para la administración de alto nivel del entorno de espacio aislado.

- Conexión a Internet para descargar el appliance virtual Sandbox Analyzer, con un ancho de banda de 5 MBps como mínimo.

  Importante
  Asegúrese de que no haya otras aplicaciones o procesos que puedan bloquear la conexión a Internet mientras descargue e instale Sandbox Analyzer.

4.5.1. Hypervisor ESXi

El appliance virtual Sandbox Analyzer está disponible en formato OVA, implementable en un único host físico que ejecute el hipervisor VMware ESXi (versión 6.5 o 6.7).

Requisitos de hardware para el host físico

- CPU: el número total de núcleos de CPU (considerando el hyperthreading) se puede extrapolar mediante el cálculo presentado en la sección "Requisitos de host físico y escalamiento del hardware" (p. 48).
- RAM: la cantidad total de RAM necesaria para el host físico se puede extrapolar mediante el cálculo presentado en la sección "Requisitos de host físico y escalamiento del hardware" (p. 48).
- Espacio en disco: al menos 1 TB de almacenamiento SSD (adecuado para un entorno de detonación de 8 máquinas virtuales, escalable con al menos 50 GB por cada máquina virtual de detonación adicional).
- Red: una tarjeta de interfaz de red (NIC) física dedicada.

  Esta NIC se puede dividir en dos NIC virtuales, con las siguientes asignaciones:

  - Una NIC para la interfaz de administración.
  - Una NIC para la red de detonación.

  Nota
  Se recomienda utilizar NIC físicas dedicadas con las mismas asignaciones que las vNIC mencionadas anteriormente si la configuración de hardware lo permite.

Requisitos de Software

Versiones compatibles del servidor ESXi: 6.5 o superior, VMFS versión 5.

Configuración adicional en el host ESXi:

- SSH habilitado al inicio.
- Servicio NTP configurado y activo.
- La opción de **inicio/parada con host** habilitada.

Nota
Sandbox Analyzer es compatible con la versión de evaluación de VMware ESXi. No obstante, para las implementaciones de producción, se recomienda la ejecución en una versión con licencia de ESXi.

4.5.2. Appliance virtual Sandbox Analyzer

El appliance virtual Sandbox Analyzer proporciona una escalabilidad prácticamente ilimitada, siempre que estén disponibles los recursos de hardware subyacentes.

De la cantidad total de recursos disponibles de ESXi, Sandbox Analyzer comparte la CPU y la RAM entre Sandbox Manager y las máquinas virtuales de detonación.

Requisitos mínimos del sistema de Sandbox Manager

- 6 vCPU
- 20 GB de RAM
- 600 GB de espacio en disco

Sandbox Manager tiene tres NIC virtuales internas asignadas de la siguiente manera:

- Una NIC para la comunicación con la consola de administración (GravityZone Control Center).
- Una NIC para la conectividad a Internet.
- Una NIC para la comunicación con las máquinas virtuales de detonación.

Nota
Para permitir la comunicación, tanto la vNIC de administración de ESXi como la de administración de Sandbox Manager deben estar en la misma red.

Máquinas virtuales de detonación

Requisitos del Sistema

- 4 vCPU (sobreaprovisionadas en una proporción de 4:1, consulte “Requisitos de host físico y escalamiento del hardware” (p. 48)).
- 3 GB de RAM
- 50 GB de espacio en disco

Sandbox Analyzer On-Premises proporciona imágenes de máquinas virtuales personalizadas. Esto permite la detonación de muestras en un entorno de tiempo de ejecución que imita a un entorno de producción realista.

Crear una imagen de máquina virtual requiere las siguientes condiciones:

- La imagen de la máquina virtual está en formato VMDK, versión 5.0.
- Sistemas operativos compatibles para crear máquinas virtuales de detonación:
  - Windows 7 64 bits (cualquier nivel de parche)
  - Windows 10 64 bits (cualquier nivel de parche)

Importante

- El sistema operativo debe instalarse en la segunda partición de la tabla de particiones y montarse en la unidad C: (configuración de instalación por defecto de Windows).
- La cuenta de "Administrador" local debe estar habilitada y tener una cadena de contraseña vacía (contraseña inhabilitada).
- Antes de exportar la imagen de la máquina virtual, debe poseer licencia válida del sistema operativo y de todo el software instalado en la imagen de la máquina virtual.

Software de imagen de la máquina virtual

Sandbox Analyzer admite la detonación de una amplia gama de formatos y tipos de archivos. Para obtener información, consulte “Objetos Sandbox Analyzer” (p. 236).

Para obtener informes concluyentes, asegúrese de haber instalado en la imagen personalizada el software que pueda abrir el tipo de archivo en particular que desee detonar. Para obtener información, consulte “Aplicaciones recomendadas para las máquinas virtuales de detonación” (p. 237).

4.5.3. Appliance virtual de seguridad de red

El Network Security Virtual Appliance controla el sensor de red, que extrae cargas útiles de los flujos de red y los envía a Sandbox Analyzer. Los requisitos mínimos de hardware son los siguientes:

- 4 vCPU
- 4 GB de RAM
- 1 TB de espacio en disco
- 2 vNICs

4.5.4. Requisitos de host físico y escalamiento del hardware

El algoritmo de escalamiento del entorno Sandbox Analyzer considera la siguiente fórmula, donde "K" es el número de slots de detonación (o máquina virtual de detonación):

- Sandbox Analyzer VA vCPU = 6 vCPUs + K x 1vCPU
- Sandbox Analyzer VA RAM = 20 GB RAM + K x 2GB

De manera similar, el algoritmo de escalamiento para el host es el siguiente:

- vCPU de host ESXi = 6 vCPU + K x 2 vCPU
- RAM del host ESXi = 20 GB de RAM + K x 5 GB

La principal diferencia entre los recursos de ESXi y el appliance virtual Sandbox Analyzer viene dada por los recursos asignados a cada máquina virtual de detonación.

Por lo tanto, un entorno de detonación típico (8 máquinas virtuales) tendría los siguientes requisitos:

- Sandbox Analyzer VA vCPU = 6 vCPUs + 8 x 1vCPU = 14 vCPUs
- Sandbox Analyzer VA RAM = 20 GB RAM + 8 x 2GB = 36GB RAM
- ESXi Host vCPU = 6 vCPUs + 8 x 2 vCPUs = 22 vCPUs

> **Nota**
> Cada máquina virtual de detonación necesita 1 vCPU asignada para el appliance virtual Sandbox Analyzer y 1 vCPU para la máquina virtual de detonación. La máquina virtual de detonación se aprovisionará con 4 vCPU, pero se

aprovisionarán en exceso en una proporción de 4:1, lo que hará que solo se necesite 1 vCPU para el host ESXi.

- RAM del host ESXi = 20 GB de RAM + 8 x 5 GB = 60 GB de RAM

> **Nota**
> La RAM se utiliza en una proporción de 1:1 entre el appliance virtual Sandbox Analyzer, las máquinas virtuales de detonación y el host ESXi. Por lo tanto, cada máquina virtual de detonación requerirá 5 GB de RAM del host ESXi, de los cuales 2 GB se asignarán al appliance virtual Sandbox Analyzer y 3 GB se asignarán a la máquina virtual de detonación.

El host físico resultante requiere, en el escenario mencionado anteriormente, al menos 22 núcleos de CPU (incluyendo hyperthreading) y al menos 60 GB de RAM, con un 10-20 % adicional de RAM reservada para el propio hipervisor.

Normalmente, la detonación de una muestra tarda nueve minutos en ejecutarse y generar el informe de detonación, y utiliza todos los recursos aprovisionados. Se recomienda que diseñe su entorno de espacio aislado comenzando por la capacidad de detonación (archivos/hora) y, luego, transformando esta métrica en los recursos necesarios a nivel de host y máquinas virtuales.

4.5.5. Requisitos de comunicación de Sandbox Analyzer

Los componentes de Sandbox Analyzer On-Premises utilizan ciertos puertos de comunicación vinculados a interfaces de red específicas para comunicarse entre sí o con los servidores públicos de Bitdefender.

El entorno de espacio aislado requiere tres interfaces de red:

- **eth0: interfaz de red de administración**. Se conecta a GravityZone y al host ESXi.

  Se recomienda conectar eth0 a la misma red que la interfaz de administración de ESXi. También se recomienda asignarlo a un adaptador físico dedicado.

  La siguiente tabla describe los requisitos de comunicación de red para eth0:

Dirección	Puertos de comunicación (TCP)	Fuente/Destino
Saliente	8443	Servidor de comunicaciones de GravityZone

Dirección	Puertos de comunicación (TCP)	Fuente/Destino
	443	Appliance virtual GravityZone
	80	Appliance virtual GravityZone
	22	Host ESXi.
	443	API de host ESXi.
Entrante	8443	Cualquiera

- **eth1: red de detonación**. No requiere ninguna configuración. El proceso de instalación crea los recursos virtuales necesarios.
- **eth2: red de acceso a Internet**. Se recomienda tener una conexión a Internet sin restricciones ni filtros.

  Se recomienda que la red de administración y la de acceso a Internet se asignen a diferentes subredes.

El appliance virtual GravityZone requiere acceso al appliance virtual Sandbox Analyzer en el puerto 443 (TCP) para ver y descargar informes de Sandbox Analyzer.

El appliance virtual GravityZone requiere conectividad con el appliance virtual Sandbox Analyzer en el puerto 443 (TCP) para solicitar el estado de las muestras detonadas.

4.6. HVI

HVI funciona con la ayuda de dos componentes: paquete suplementario de HVI y Security Server. Estos productos deben instalarse en los hosts de su entorno virtualizado donde tenga máquinas virtuales que desee proteger.

Antes de implementar HVI en los hosts, asegúrese de que se cumplen los siguientes requisitos:

Plataformas de virtualización soportadas

- Citrix XenServer 7.1 Enterprise Edition o superior, con los últimos parches

> **Importante**
> Para cualquier versión de XenServer a partir de la 7.1 que haya alcanzado su fin del ciclo de vida, Bitdefender brinda compatibilidad de HVI durante dos meses

más. Transcurrido este período, recomendamos actualizar a una versión de XenServer compatible con Citrix. Para obtener más información, consulte la tabla de productos antiguos de Citrix y la tabla de productos de Citrix.

- Citrix Hypervisor 8.0 Enterprise Edition o superior, con los últimos parches

  Aviso
  Para Citrix Hypervisor 8.0, debe instalar el parche XS80E004.

Máquinas virtuales guest compatibles

Las máquinas virtuales que desee proteger con HVI deben cumplir las siguientes condiciones:

1. Las máquinas están en modo de virtualización HVM, lo que significa que están totalmente virtualizadas.
2. Las máquinas ejecutan un sistema operativo compatible:
   - **Sistemas operativos de equipos de escritorio Windows (32 bits y 64 bits)**

     Actualización de Windows de 10 de mayo de 2020 (20H1)

     Actualización de Windows 10 de noviembre de 2019 (19H2)

     Actualización de Windows de 10 de mayo de 2019 (19H1)

     Windows 10 October 2018 Update (Redstone 5)

     Windows 10 April 2018 Update (Redstone 4)

     Windows 10 Fall Creators Update (Redstone 3)

     Windows 10 Creators Update (Restone 2)

     Windows 10 Anniversary Update (Redstone 1)

     Windows 10 November Update (Threshold 2)

     Windows 10

     Windows 8.1

     Windows 8

     Windows 7
   - **Sistemas operativos de servidores Windows (64 bits)**

Windows Server 2019

Windows Server 2016

Windows Server 2012/ Windows Server 2012 R2

Windows Server 2008 R2

- **Sistemas operativos Linux (64 bits)**

Distribución	Versión	Versión del kernel
Debian	10	4.19
Debian	9	4.9
Debian	8	3.16
Ubuntu	20.04 LTS	5.4
Ubuntu	18.04 LTS	4.15
Ubuntu	16.04 LTS	4.4
Ubuntu	14.04 LTS	3.13.139 y posterior
CentOS	8.2	4.18
CentOS	8	4.18
CentOS	7	3.10
Red Hat Enterprise Linux	8.2	4.18
Red Hat Enterprise Linux	8	4.18
Red Hat Enterprise Linux	7	3.10
Red Hat Enterprise Linux	6.8 / 6.9 / 6.10	2.36.32
SUSE Linux Enterprise Server	15 SP1	4.12
SUSE Linux Enterprise Server	12 SP4	4.12
SUSE Linux Enterprise Server	12 SP3	4.4
SUSE Linux Enterprise Server	12 SP2	4.4
SUSE Linux Enterprise Server	12 SP1	3.12
Oracle Linux	Anterior a la 7.5	4.1 (UEK/RHCK)
Oracle Linux	7.5 y posterior	4.14 (UEK/RHCK)

Requisitos de hardware para el appliance virtual GravityZone

- **Requerida vCPU**

  La siguiente tabla le informa de la cantidad de vCPU que solicita cada rol del appliance virtual.

  Cada vCPU debe ser al menos de 2 GHz.

Módulo	Cantidad de endpoints (hasta)							
	250	500	1000	3000	5000	10000	25000	50000
Servidor de actualizaciones*	8	4	4	4	4	4	6	8
Consola web**		6	8	8	10	10	12	12
Servidor de comunicaciones		6	8	8	10	10	16	20
Base de datos***		6	6	6	6	6	9	12
Total	**8**	**22**	**26**	**26**	**30**	**30**	**43**	**52**

  * Recomendado cuando no se implementan relays.
  ** Para cada integración activa, añada una vCPU al appliance virtual con el rol de Consola web.
  *** En caso de instalaciones distribuidas de roles, junto con el Conjunto de réplicas: para cada instancia de base de datos adicional, añada el número especificado a la cantidad total.

- **RAM requerida (GB)**

Módulo	Cantidad de endpoints (hasta)							
	250	500	1000	3000	5000	10000	25000	50000
Update Server	16	2	2	2	2	2	3	3
Consola web*		8	10	10	10	10	12	16
Servidor de comunicaciones		8	10	10	12	12	16	20
Base de datos**		8	8	8	8	12	12	12
Total	**16**	**26**	**30**	**30**	**32**	**36**	**43**	**51**

* Para cada integración activa, añada 1 GB de RAM al appliance virtual con el rol de Consola web.
** En caso de instalación distribuida de roles, junto con el Conjunto de réplicas: para cada instancia de base de datos adicional, añada el número especificado a la cantidad total.

- **Espacio en disco requerido (GB)**

Update Server	120	160	80	80	80	80	80	80	80
Consola Web			80	80	80	80	80	80	80
Servidor de comunicaciones			80	80	80	80	80	80	80
Base de datos**			80	80	100	100	160	300	700
Total	**120**	**160**	**320**	**320**	**340**	**340**	**400**	**540**	**940**

* Si se opta por la instalación automática, se necesita espacio SSD adicional, ya que también instala Security Server. Una vez finalizada la instalación, puede desinstalar Security Server para liberar espacio en disco.
** En caso de instalación distribuida de roles, junto con el Conjunto de réplicas: para cada instancia de base de datos adicional, añada el número especificado a la cantidad total.

Requisitos de hardware para hosts

- **Microarquitectura de CPU:**
  - Cualquier procesador Intel® Sandy Bridge o posterior, con soporte para la Intel® Virtualization Technology.
  - Las extensiones VT-x o VT-d deben estar habilitadas en la BIOS.
- **Espacio libre en disco:** Además del espacio requerido por Security Server, HVI requiere otros 9 MB para el paquete suplementario en cada host.

Requisitos de Security Server

La asignación de recursos de memoria y CPU para el Security Server depende del número y tipo de MVs ejecutadas en el host. La siguiente tabla indica los recursos recomendados que deben asignarse:

Número de MVs protegidas	RAM	CPUs
1-50 MVs	6 GB	4 CPUs
51-100 MVs	8 GB	6 CPUs
101-200 MVs	16 GB	8 CPU

Espacio libre en disco: Debe aprovisionar 8 GB de espacio en disco en cada host para Security Server.

Para obtener un rendimiento óptimo en un entorno XenAPP, escale los recursos de Security Server según su configuración, de la siguiente manera:

Número de VDA de XenApp	VDA		Security Server	
	CPUs	RAM (GB)	CPUs	RAM (GB)
1 VDA	4 / 8	12 / 24	2	4
2 VDA	4 / 8	12 / 24	2	8
4 VDA	8	24	2	16
8 VDA	4	12	4	16

Requisitos de las máquinas virtuales guest

En una configuración de entorno normal, para un ratio de consolidación de VM y rendimiento óptimos, se recomienda tener la siguiente configuración mínima de hardware para las máquinas virtuales guest:

- **vCPU:** 2 x vCPU
- **RAM:** 3 GB

4.7. Cifrado completo del disco duro

El Cifrado de disco completo de GravityZone le permite utilizar BitLocker en los endpoints de Windows y FileVault y la utilidad de línea de comandos diskutil en los endpoints de Mac a través de Control Center.

Para garantizar la protección de datos, este módulo proporciona el cifrado de disco completo en discos fijos, tanto en volúmenes que son de arranque como en los que no, y almacena las claves de recuperación en caso de que los usuarios olviden sus contraseñas.

El módulo de cifrado utiliza los recursos de hardware existentes en su entorno de GravityZone.

En cuanto al software, los requisitos son casi los mismos que para BitLocker, FileVault y la utilidad de línea de comandos diskutil, y la mayoría de las limitaciones dependen de estas herramientas.

Para Windows

El cifrado de GravityZone es compatible con BitLocker, a partir de la versión 1.2, en equipos con y sin chip de módulo de plataforma segura (TPM).

GravityZone admite BitLocker en endpoints con los siguientes sistemas operativos:

- 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 (con TPM)
- Windows 7 Enterprise (con TPM)
- Windows Server 2019*
- Windows Server 2016*
- Windows Server 2012 R2*
- Windows Server 2012*
- Windows Server 2008 R2* (con TPM)

* Estos sistemas operativos no incluyen BitLocker, por lo que debe instalarse por separado. Para obtener más información acerca de la implementación de BitLocker en Windows Server, consulte estos artículos de la base de conocimientos de 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

Importante
GravityZone no admite el cifrado en Windows 7 y Windows 2008 R2 sin TPM.

Para obtener información detallada sobre los requisitos de BitLocker, consulte este artículo de la base de conocimientos de Microsoft: https://technet.microsoft.com/en-us/library/cc766200(v=ws.10).aspx

Para Mac

GravityZone es compatible con FileVault y diskutil en endpoints de macOS con los siguientes sistemas operativos:

- 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)

4.8. Protección de almacenamiento

Soluciones compatibles de almacenamiento y uso compartido de archivos:

- Sistemas de red de área de almacenamiento (SAN) y de almacenamiento conectado en red (NAS) compatibles con ICAP de Dell®, EMC®, IBM®, Hitachi®, HPE®, Oracle® y otros
- Nutanix® Files 3.x hasta 3.6.2
- Citrix® ShareFile

4.9. Protección para móviles

4.9.1. Plataformas soportadas

Security for Mobile soporta los siguientes tipos de dispositivos móviles y sistemas operativos:

- iPhones y tablets iPad de Apple (iOS 8,1+).
- Smartphones y tablets Google Android (4.2+)

4.9.2. Requisitos de conexión

Los dispositivos móviles deben tener una conexión de datos o Wi-Fi activa, y conectividad con el Servidor de comunicaciones.

4.9.3. Notificaciones Push

Security for Mobile utiliza notificaciones push para alertar a los clientes cuando están disponibles actualizaciones de políticas y tareas. Las notificaciones Push se envían al Servidor de comunicaciones a través del servicio proporcionado por el fabricante del sistema operativo:

- Servicio de mensajería en la nube de Firebase (FCM) para dispositivos Android. Para que funcione FCM, se necesita lo siguiente:
  - Debe estar instalado Google Play Store.
  - Dispositivos con Android 4.2 o posterior.
  - Para enviar notificaciones push, debe abrirse determinado número de puertos.
- Servicio Apple Push Notifications (APNs) para dispositivos iOS. Para más información, consulte este artículo de la base de datos de conocimiento de Apple.

Puede comprobar si las notificaciones push móviles funcionan correctamente en la sección **Comprobación de notificaciones push para dispositivos móviles** de **Configuración > Varios**.

Para saber más sobre el flujo de trabajo de GravityZone Mobile Device Management, por favor consulte este artículo de la base de conocimientos.

4.9.4. Certificados de Administración de iOS

Para configurar la infraestructura para la administración de dispositivos móviles iOS, debe proporcionar varios certificados de seguridad.

Para más información, diríjase a “Certificados” (p. 102).

4.10. Generador de informes

Los roles del Generador de informes requieren ejecutarse en instancias independientes del appliance virtual GravityZone: el primer appliance virtual debe

tener instalado el rol de Base de datos del Generador de informes y el segundo ha de tener instalado el rol de Procesadores del Generador de informes.

4.10.1. Hardware

Los roles del Generador de informes requieren los siguientes recursos de hardware:

CPU requerida

Appliance virtual	Cantidad de endpoints (hasta)					
	250	1000	5000	10000	25000	50000
Base de Datos	4	4	4	4	6	8
Procesadores	6	6	6	6	6	6

RAM (GB)

Appliance virtual	Número de endpoints					
	250	1000	5000	10000	25000	50000
Base de Datos	8	8	8	8	16	16
Procesadores	8	8	8	8	8	8

Espacio libre en disco duro (GB)

Appliance virtual	Número de endpoints					
	250	1000	5000	10000	25000	50000
Base de datos*	15	20	50	90	210	400
Procesadores**	50	200	1000	1950	4800	9500

* Se proporciona el uso de disco del appliance virtual de la Base de datos del Generador de informes para eventos almacenados durante un año.
** Se proporciona el uso de disco del appliance virtual de Procesadores del Generador de informes para una media de diez informes al mes, con quince columnas cada uno. El appliance virtual de Procesadores del Generador de informes

necesita más espacio porque almacena todos los informes creados con datos de la Base de datos del Generador de informes.

4.10.2. Versiones del producto GravityZone

A partir de la versión 6.5.5-1 de GravityZone, los roles del Generador de informes se entregan con el appliance virtual GravityZone.

Antes de esta versión, los roles del Generador de informes se entregaban como un appliance virtual independiente compatible con Bitdefender GravityZone versión 6.1.27-537 o posterior.

4.11. Puertos de comunicación de GravityZone

GravityZone es una solución distribuida, lo que significa que sus componentes se comunican entre sí mediante la red local o Internet. Cada componente utiliza una serie de puertos para comunicarse con los demás. Debe asegurarse de que estos puertos estén abiertos para GravityZone.

Para obtener información detallada sobre los puertos de GravityZone, consulte este artículo de la base de conocimientos.

5. INSTALACIÓN DE LA PROTECCIÓN

GravityZone es una solución cliente-servidor. Para proteger su red con Bitdefender, debe implementar los roles de servidor de GravityZone, registrar su licencia, configurar los paquetes de instalación e implementarlos mediante agentes de seguridad en los endpoints. Algunas capas de protección requieren la instalación y configuración de componentes adicionales.

5.1. Instalación y configuración de GravityZone

Para asegurar que la instalación se realiza de forma correcta, siga estos pasos:

1. Prepararse para la instalación
2. Implementar y configurar GravityZone
3. Conéctese a Control Center y configure la primera cuenta de usuario
4. Configure los ajustes de Control Center

5.1.1. Preparándose para la instalación

Para la instalación necesita una imagen del appliance virtual GravityZone. Tras la implementación y configuración del appliance GravityZone, puede instalar el cliente de forma remota o descargar los paquetes de instalación necesarios para los otros componentes de los servicios de seguridad desde la interfaz Web de Control Center.

La imagen del appliance GravityZone está disponible en varios formatos, compatibles con las principales plataformas de virtualización. Puede obtener los enlaces de descarga registrándose para una versión de evaluación en el sitio web de Bitdefender.

Para la instalación y configuración inicial, debe tener a mano lo siguiente:

- Nombre DNS o direcciones IP fijas (bien sea por configuración estática o a través de la reserva DHCP) para los appliances GravityZone
- Nombre de usuario y contraseña de un administrador de dominio
- Información de vCenter Server, vShield Manager, XenServer (nombre del host o dirección IP, puerto de comunicaciones, nombre de usuario y contraseña de administrador)
- Claves de licencia (compruebe el registro para la versión de evaluación o el mensaje de correo electrónico de la compra)

- Configuración del servidor de correo saliente
- Configuración del servidor proxy, si es necesario
- Certificados de seguridad

5.1.2. Implementar GravityZone

Una implementación de GravityZone consiste en uno o varios appliances que ejecutan los roles de servidor. La cantidad de appliances depende de varios criterios, como el tamaño y el diseño de su infraestructura de red o las características de GravityZone que vaya a utilizar. Los roles de servidor son de tres tipos: básico, auxiliar y opcional.

Importante
Los roles auxiliar y opcional solo están disponibles para ciertas soluciones GravityZone.

Rol de GravityZone	Tipo de rol	Instalar
Servidor de base de datos Update Server Consola Web Servidor de comunicaciones	Básico (requerido)	Al menos una instancia de cada rol. Un appliance GravityZone puede desempeñar uno, varios o todos estos roles.
Base de datos del generador de informes Procesadores del generador de informes	Auxiliar	Un appliance para cada rol
Security Server	Opcional	Recomendado solo en redes pequeñas o con pocos recursos. De lo contrario, implemente un Security Server independiente desde Control Center una vez finalizada la implementación de GravityZone.

Dependiendo de cómo distribuya los roles de GravityZone, implementará uno o varios appliances GravityZone (al menos tres si usa el Generador de informes). El rol de Servidor de base de datos es el primero en instalarse.

En un escenario con múltiples appliances GravityZone, instalará el rol de Servidor de base de datos en el primer appliance y configurará los otros appliances para conectarse con la instancia de base de datos existente.

Puede implementar más instancias de los roles de Servidor de base de datos, Consola web y Servidor de comunicaciones. En este caso, utilizará el Conjunto de réplicas para el Servidor de base de datos y los equilibradores de carga para la Consola web y el Servidor de comunicaciones en los appliances GravityZone.

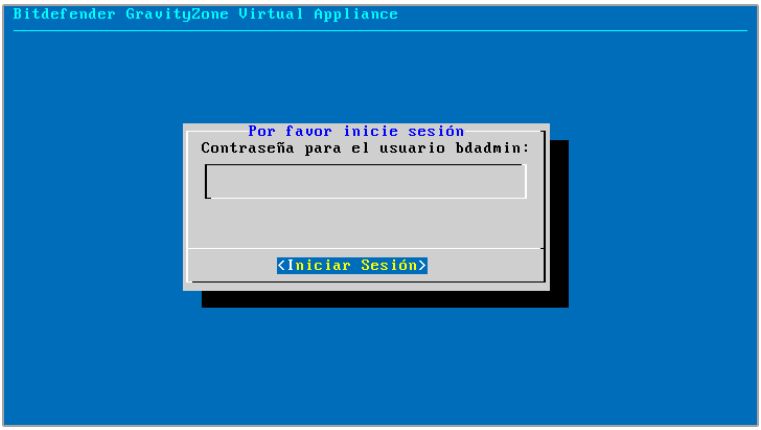
Se recomienda instalar los roles del Generador de informes después de configurar GravityZone, es decir: instalar los roles básicos de GravityZone, configurar Control Center, actualizar GravityZone e implementar la protección en los endpoints. Además, primero debe instalar la Base de datos del Generador de informes, seguida de los Procesadores del Generador de informes. Para obtener información, consulte "Instalación del Generador de informes" (p. 183).

Para implementar y configurar GravityZone:

1. Descargue la imagen del appliance virtual GravityZone desde el sitio web de Bitdefender (se proporciona el enlace durante el registro o en el mensaje de correo electrónico de la compra).
2. Importar la imagen del appliance virtual GravityZone en su entorno virtualizado.
3. Encender el appliance.
4. Desde su herramienta de administración de la virtualización, acceda a la interfaz de la consola del appliance GravityZone.
5. Configure la contraseña para `bdadmin`, el administrador del sistema incorporado.

Interfaz de consola del appliance: introduzca una nueva contraseña

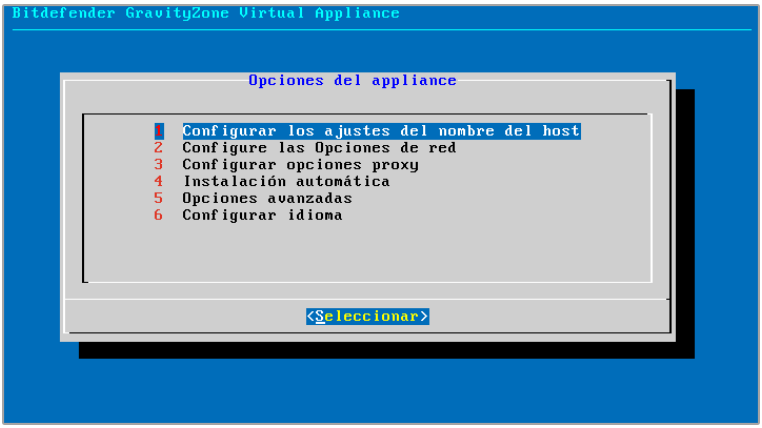
6. Inicie sesión con la contraseña que ha establecido.



Interfaz de consola del appliance: inicio de sesión

Accederá a la interfaz de configuración del appliance.

Utilice las teclas de flecha y la tecla `Tabulador` para navegar por los menús y opciones. Pulse `Intro` para seleccionar una opción específica.



Interfaz de consola del appliance: menú principal

7. Si necesita cambiar el idioma de la interfaz, seleccione la opción **Configurar idioma**. Para obtener más información sobre la configuración, consulte "Configurar idioma" (p. 71).
8. Configure el nombre de host del appliance.
9. Configure los ajustes de la red.
10. Configure los ajustes del proxy. (en caso necesario)
11. Instale los roles de servidor de GravityZone. Hay dos opciones:
    - Instalación automática. Seleccione esta opción si necesita implementar solo un appliance GravityZone en su red.
    - Ajustes avanzados. Seleccione esta opción si necesita implementar GravityZone manualmente o en una arquitectura distribuida.

Tras implementar y configurar el appliance GravityZone, puede modificar en cualquier momento los ajustes del appliance mediante la interfaz de configuración. Para obtener más información acerca de la configuración del appliance GravityZone, consulte "Administrar el appliance GravityZone" (p. 109).

Configurar los ajustes del nombre del host

La comunicación con los roles de GravityZone se realizan usando la dirección IP o nombre DNS del appliance en el que están instalados. Los componentes de GravityZone se comunican de forma predeterminada usando direcciones IP. Si desea activar la comunicación a través de nombres DNS, debe configurar los appliances GravityZone con un nombre DNS y asegurar que resuelve correctamente con las direcciones IP configuradas del appliance.

Requisitos:

- Configure el registro DNS en el servidor DNS
- El nombre DNS debe resolver correctamente la dirección IP configurada en el appliance. Por ello, debe asegurarse de que el appliance está configurado con la dirección IP correcta.

Para configurar los ajustes del nombre del host:

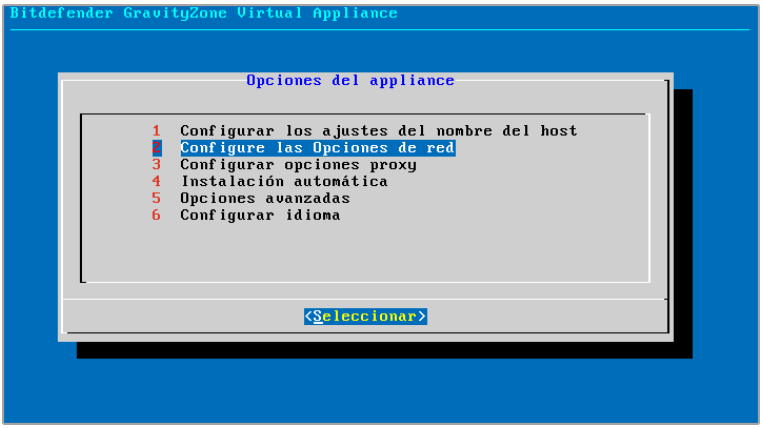
1. En el menú principal, seleccione **Configurar los ajustes del nombre del host**.
2. Escriba el nombre del host del appliance y el nombre de dominio de Active Directory (si fuera necesario).

3. Seleccione **Aceptar** para guardar los cambios.

Configure las Opciones de red

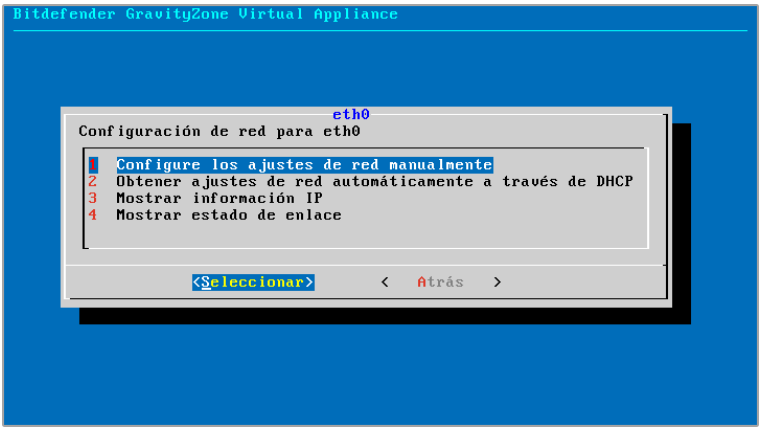
Puede configurar el appliance para que obtenga los ajustes de red automáticamente desde el servidor DHCP o puede configurar los ajustes de red manualmente. Si elige utilizar DHCP, debe configurar el Servidor DHCP para reservar direcciones IP específicas para el appliance.

1. Desde el menú principal, seleccione **Configurar ajustes de red**.



Interfaz de consola del appliance: opción de ajustes de red

2. Seleccione la interfaz de red.
3. Seleccione el método de configuración:
   - **Configure los ajustes de red manualmente.** Debe especificar la dirección IP, máscara de red, dirección de puerta de enlace y direcciones de servidores DNS.
   - **Obtener ajustes de red automáticamente a través de DHCP.** Utilice esta opción si ha configurado el servidor DHCP para reservar direcciones IP específicas para el appliance.



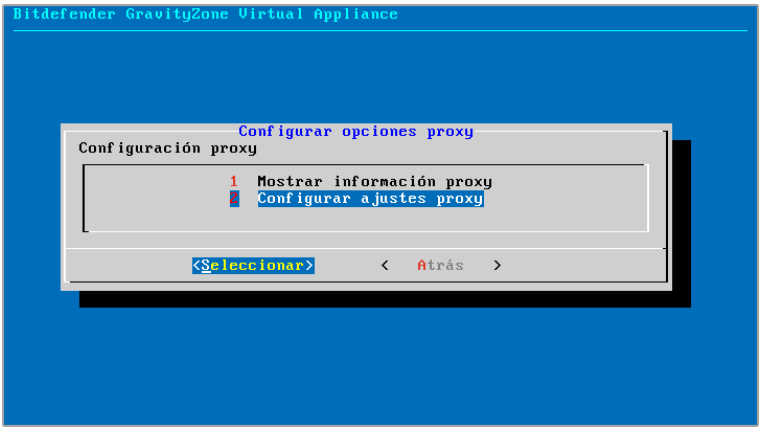
Interfaz de consola del appliance: configuración de red

4. Puede comprobar los detalles de la configuración IP actual o estado de enlace seleccionando las opciones correspondientes.

Configurar opciones proxy

Si desea que el appliance se conecte a Internet a través de un servidor proxy, debe configurar los ajustes del proxy.

1. Desde el menú principal, seleccione **Configurar ajustes del proxy**.
2. Seleccione **Mostrar información proxy** para comprobar si este se encuentra habilitado.
3. Seleccione **Aceptar** para volver a la pantalla anterior.
4. Seleccione nuevamente **Configurar ajustes proxy**.



Interfaz de consola del appliance: configure los ajustes del proxy

5. Escriba la dirección del servidor proxy. Utilice la siguiente sintaxis:
   - Si el servidor proxy no requiere autenticación:

     `http(s)://<IP/nombredelhost>:<puerto>`
   - Si el servidor proxy requiere autenticación:

     `http(s)://<nombredeusuario>:<contraseña>@<IP/nombredelhost>:<puerto>`
6. Seleccione **Aceptar** para guardar los cambios.

Instalación automática

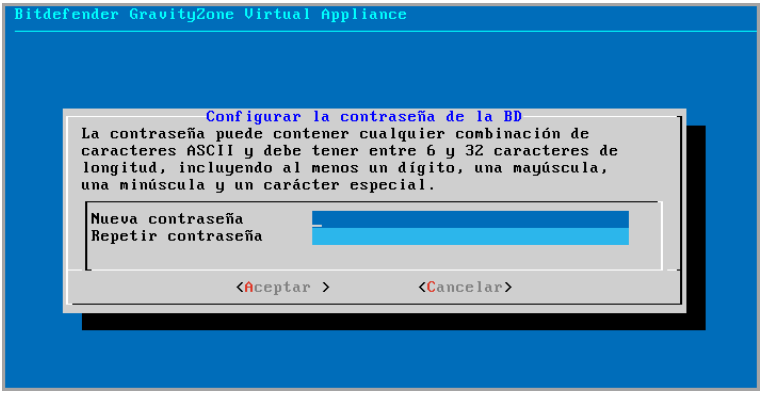
Durante la instalación automática, todos los roles básicos se instalan en el mismo appliance. Para una implementación distribuida de GravityZone, consulte "Opciones avanzadas" (p. 69).

Importante
La implementación automática también instalará el Security Server, integrado en el appliance GravityZone. Para obtener información sobre Security Server, consulte "Architecture GravityZone" (p. 11).
La opción de instalación automática de roles solo está disponible durante la configuración inicial de GravityZone.

Para instalar los roles automáticamente:

1. En el menú principal, seleccione **Instalación automática**.
2. Para continuar, lea y acepte el Acuerdo de licencia de usuario final (EULA, por sus siglas en inglés).
3. Confirme los roles que se han de instalar.
4. Establezca la contraseña para el Servidor de base de datos.

   La contraseña puede contener cualquier combinación de caracteres ASCII y debe tener entre 6 y 32 caracteres de longitud, incluyendo al menos un dígito, una mayúscula, una minúscula y un carácter especial.



Interfaz de consola del appliance: configure una contraseña para la base de datos

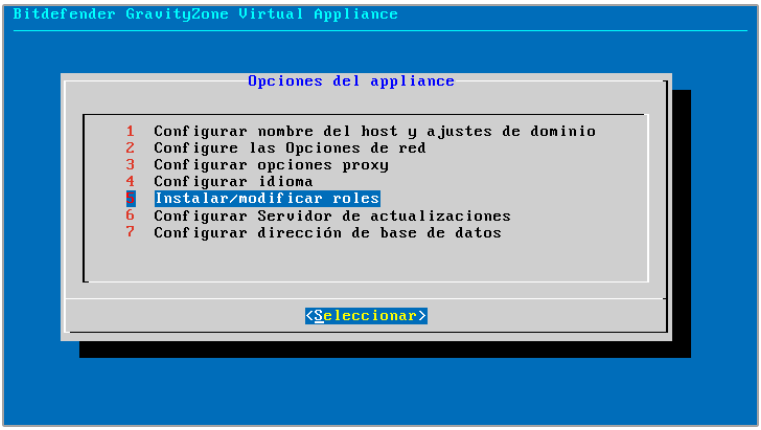
5. Espere a que finalice el proceso de instalación.

Opciones avanzadas

Use esta opción para instalar solo una parte o todos los roles de GravityZone, individualmente, o para ampliar su infraestructura de GravityZone. Puede instalar los roles en uno o varios appliances. Este método de instalación es necesario cuando se realizan ensayos de actualizaciones o en arquitecturas distribuidas de GravityZone para escalar GravityZone en redes grandes y para garantizar una alta disponibilidad de los servicios de GravityZone.

Para instalar los roles individualmente:

1. En el menú principal, seleccione **Configuración avanzada**.



Interfaz de consola del appliance: instale roles

2. Seleccione **Instalar/desinstalar roles** para instalar el appliance en un entorno GravityZone con un solo servidor de base de datos.

   Nota
   Las otras opciones son para extender la implementación de GravityZone a una arquitectura distribuida. Para obtener más información, consulte "Conectarse a la base de datos existente" (p. 120) o "Conectarse a la base de datos existente (Cluster VPN seguro)" (p. 121).

3. Seleccione **Añadir o eliminar roles**. Aparecerá un mensaje de confirmación.
4. Pulse `Intro` para continuar.
5. Pulse la `barra espaciadora` y luego la tecla `Intro` para instalar el rol de Servidor de base de datos. Debe confirmar su elección pulsando `Intro` nuevamente.
6. Establezca la contraseña de base de datos.

   La contraseña puede contener cualquier combinación de caracteres ASCII y debe tener entre 6 y 32 caracteres de longitud, incluyendo al menos un dígito, una mayúscula, una minúscula y un carácter especial.
7. Haga clic en `Intro` y espere a que finalice la instalación.

8. Instale los otros roles seleccionando **Añadir o eliminar roles** en el menú **Instalar/desinstalar roles** y luego los roles que desee instalar.
   a. Elija **Añadir o eliminar roles** en el menú **Instalar/Desinstalar roles**.
   b. Lea el Acuerdo de licencia de usuario final. Pulse `Intro` para aceptarlo y continuar.

      Nota
      Esto es necesario solo una vez después de instalar el Servidor de base de datos.

   c. Seleccione los roles que desea instalar. Pulse la `barra espaciadora` para seleccionar un rol e `Intro` para continuar.
   d. Pulse `Intro` para confirmar y luego espere a que finalice la instalación.

Nota
Cada rol se instala normalmente en unos minutos. Durante la instalación, se descargan los archivos necesarios de Internet. Por consiguiente, la instalación lleva más tiempo si la conexión a Internet es lenta. Si la instalación se bloquea, reinstale el appliance.

Configurar idioma

Inicialmente, la interfaz de configuración del appliance está en inglés.

Para cambiar el idioma de la interfaz:

1. Seleccione **Configurar idioma** en el menú principal.
2. Seleccione el idioma deseado entre las opciones disponibles. Aparecerá un mensaje de confirmación.

   Nota
   Es posible que tenga que desplazarse hacia abajo para ver su idioma.

3. Seleccione **Aceptar** para guardar los cambios.

5.1.3. Configuración inicial de Control Center

Tras implementar y configurar el appliance GravityZone, debe acceder a la interfaz web de Control Center y configurar su cuenta de administrador de empresa.

1. En la barra de dirección de su navegador Web, escriba la dirección IP o el nombre del host DNS del appliance Control Center (usando el prefijo `https://`). Se mostrará un asistente de configuración.
2. Proporcione las claves de licencia necesarias para validar los servicios de seguridad de GravityZone adquiridos. También puede proporcionar cualquier clave de complementos de GravityZone que tenga.

   Consulte el registro de la versión de evaluación o email de compra para encontrar sus claves de licencia.

   a. Haga clic en el botón ⊕ **Añadir** en la parte superior de la tabla. Aparecerá una nueva ventana de configuración.

   b. Seleccione el tipo de registro de la licencia (online u offline).

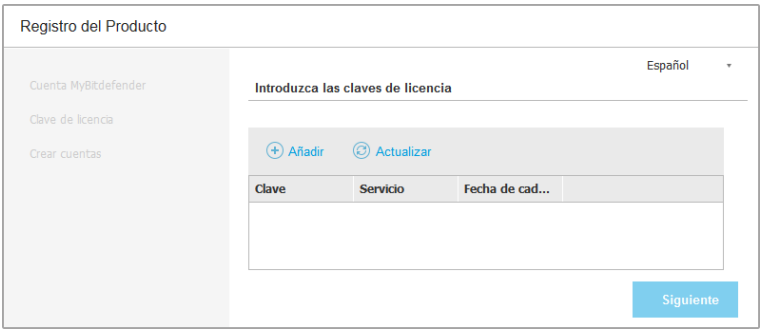
   c. Introduzca la clave de licencia en el campo **Clave de licencia**. Para el registro sin conexión ha de proporcionar también el código de registro.

   d. Espere a que se valide la clave de licencia. Haga clic en **Añadir** para terminar.

   La clave de licencia se mostrará en la tabla de licencias. También puede ver el servicio de seguridad, su estado, la fecha de caducidad y el uso actual para cada clave de licencia en las columnas correspondientes.

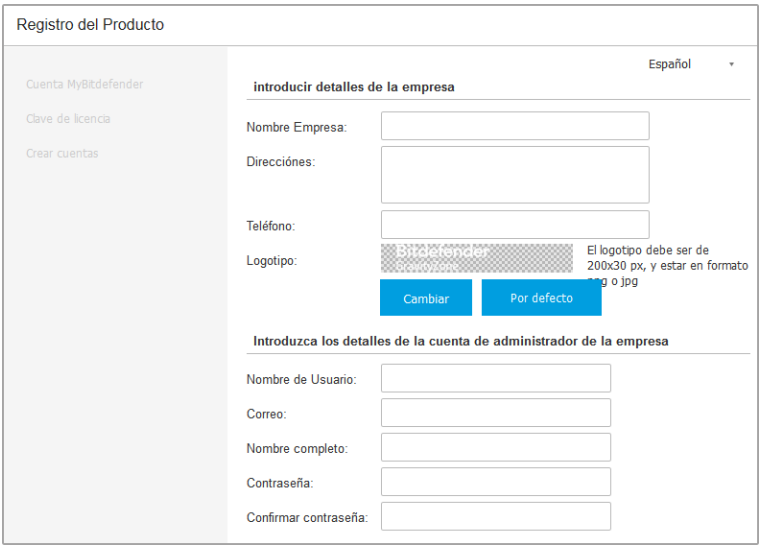
   Nota

   - Durante la instalación inicial, al menos debe proporcionarse una clave de licencia válida para empezar a usar GravityZone. Más adelante puede añadir más claves de licencia o de complementos y modificar las existentes.
   - Puede usar los complementos siempre que proporcione una licencia básica válida. De lo contrario, verá las características pero no podrá utilizarlas.



Configuración inicial - Proporcione las claves de licencia

3. Haga clic en **Siguiente** para continuar.
4. Introduzca la información de su empresa, como por ejemplo el nombre de la empresa, la dirección y el teléfono.
5. Puede cambiar el logotipo que aparece en Control Center y también en los informes de su empresa y en las notificaciones de correo electrónico como se indica a continuación:
   - Haga clic en **Cambiar** para buscar el logotipo en su equipo. El formato de archivo de imagen debe ser .png o .jpg y el tamaño de la imagen ha de ser 200x30 píxeles.
   - Haga clic en **Predeterminada** para borrar la imagen y restaurar la proporcionada por Bitdefender.
6. Indique los detalles requeridos correspondientes a la cuenta de administrador de su empresa: nombre de usuario, dirección de e-mail y contraseña. La contraseña debe contener al menos un carácter en mayúsculas, uno en minúsculas, y un número o un carácter especial.



Configuración inicial - Configure su cuenta

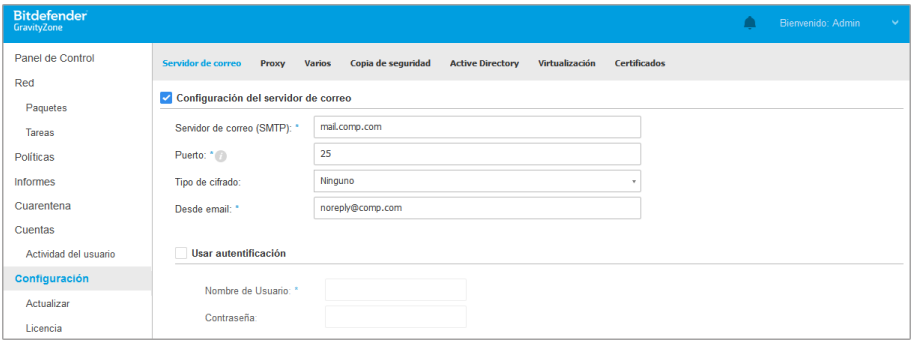
7. Haga clic en **Crear cuenta**.

Se creará la cuenta de administrador de su empresa e iniciará sesión automáticamente con ella en la Control Center de Bitdefender.

5.1.4. Configure los ajustes de Control Center

Tras la configuración inicial, ha de configurar los ajustes de Control Center. Como administrador de empresa, puede hacer lo siguiente:

- Configurar el correo, proxy y otros ajustes generales.
- Ejecutar o programar una copia de seguridad de la base de datos de Control Center.
- Configurar la integración con Active Directory y con las herramientas de administración de la virtualización (vCenter Server, XenServer).
- Instalar certificados de seguridad.



Configuración del servidor de correo

Servidor de correo

Control Center requiere un servidor de correo externo para enviar comunicaciones por email.

Nota
Se recomienda crear una cuenta de correo dedicada para utilizarla en Control Center.

Para activar el envío de emails en Control Center:

1. Acceda a la página **Configuración**.
2. Seleccione la pestaña **Servidor de correo**.
3. Seleccione **Ajustes del servidor de correo** y configure los ajustes requeridos:
   - **Servidor de correo (SMTP).** Introduzca la dirección IP o el nombre del host del servidor de correo que va a enviar los e-mails.
   - **Puerto.** Introduzca el puerto utilizado para conectarse con el servidor de correo.
   - **Tipo de cifrado.** Si el servidor de correo necesita una conexión cifrada, seleccione el tipo adecuado desde el menú (SSL, TLS o STARTTLS).
   - **Desde email.** Introduzca la dirección de e-mail que quiere que aparezca en el campo De del e-mail (dirección de e-mail del remitente).
   - **Usar autentificación.** Marque esta casilla de verificación si el servidor de correo requiere autenticación. Debe especificar un nombre de usuario / dirección de correo y contraseña válidos.

4. Haga clic en **Guardar**.

Control Center valida automáticamente los ajustes de correo cuando los guarda. Si los ajustes definidos no pueden validarse, un mensaje de error le informará de los ajustes incorrectos. Corrija el ajuste e inténtelo de nuevo.

Proxy

Si su empresa se conecta a Internet a través de un servidor proxy, puede especificar los ajustes del proxy:

1. Acceda a la página **Configuración**.
2. Seleccione la pestaña **Proxy**.
3. Seleccione **Usar ajustes del proxy** y configure los ajustes requeridos:
   - **Dirección** - introduzca la dirección IP del servidor proxy.
   - **Puerto** - introduzca el puerto utilizado para conectar con el servidor proxy.
   - **Nombre** - escriba un nombre de usuario que el proxy reconozca.
   - **Contraseña** - escriba una contraseña válida para el usuario indicado anteriormente.
4. Haga clic en **Guardar**.

Varios

En la página **Configuración**, pestaña **Varios**, puede configurar las siguientes preferencias generales:

- **Cuando se necesita una imagen del Security Server no disponible.** El appliance GravityZone no incluye de forma predeterminada las imágenes de máquinas virtuales Security Server. Si un administrador intenta descargar una imagen de Security Server o ejecutar una tarea de instalación Security Server, la acción va a producir un error. Puede configurar una acción automatizada para esta situación seleccionando una de las siguientes opciones:
  - **Límite de licencia alcanzado**
  - **Notificar al administrador y no descargar**

  Nota

  Para evitar interferir con el trabajo del administrador, puede descargar manualmente los paquetes del Security Server necesarios desde la página

Actualizar, en la pestaña **Actualización de producto**. Para más información, diríjase a "Descarga de actualizaciones de productos" (p. 194).

- **Cuando se necesita un kit no disponible.** Puede configurar una acción automatizada para esta situación seleccionando una de las siguientes opciones:
  - **Descargar el paquete automáticamente**
  - **Notificar al administrador y no descargar**
- **Implementaciones simultáneas.** Los administradores pueden implementar componentes de seguridad de forma remota ejecutando tareas de instalación. Utilice esta opción para especificar el número máximo de implementaciones simultáneas que pueden ejecutarse a un mismo tiempo.

  Por ejemplo, si el número máximo de implementaciones simultáneas está definido en 10 y una tarea de instalación cliente remota se asigna a 100 equipos, Control Center inicialmente enviará 10 paquetes de instalación a través de la red. En este caso, la instalación cliente se ejecuta simultáneamente en un número máximo de 10 equipos, quedando el resto de subtareas en estado pendiente. Tan pronto como se realiza la subtarea, se envía otro paquete de instalación, y así sucesivamente.
- **Hacer cumplir la autenticación en dos fases para todas las cuentas.** La autenticación en dos fases aporta una capa adicional de seguridad a las cuentas de GravityZone, ya que requiere un código de autenticación además de las credenciales de Control Center. Esta característica requiere descargar e instalar Google Authenticator, Microsoft Authenticator o cualquier otra app de autenticación TOTP (Time-Based One-Time Password Algorithm) en dos fases compatible con el estándar RFC 6238 en el dispositivo móvil del usuario, vincular la app a la cuenta de GravityZone y utilizarla siempre para iniciar sesión en Control Center. La app de autenticación genera un código de seis dígitos cada treinta segundos. Para finalizar el inicio de sesión en Control Center, después de introducir la contraseña, el usuario deberá proporcionar también el código de autenticación de seis dígitos.

  Al crear una empresa se habilita por defecto la autenticación en dos fases. Después de eso, al iniciar sesión, una ventana de configuración solicitará a los usuarios que habiliten esta característica. Los usuarios tendrán la opción de omitir la activación de la autenticación en dos fases solo tres veces. En el cuarto intento de inicio de sesión, no será posible omitir la configuración de la autenticación en dos fases y el usuario no podrá iniciar sesión.

Si, una vez activada, desea desactivar la obligación de la autenticación en dos fases en su empresa para todas las cuentas de usuario, basta con que desmarque la opción. Aparecerá un mensaje de confirmación antes de que los cambios surtan efecto. A partir de este momento, los usuarios seguirán teniendo activada la autenticación en dos fases, pero podrán desactivarla desde los ajustes de su cuenta.

Nota

- Puede ver el estado de la autenticación en dos fases de una cuentas de usuario en la página **Cuentas**.
- Si un usuario con la autenticación en dos fases activada no pudiese iniciar sesión en GravityZone (debido a que tenga un nuevo dispositivo o a que haya perdido la clave secreta), podrá restablecer la activación de su autenticación en dos fases desde la página de la cuenta de usuario, en la sección **Autenticación en dos fases**. Para obtener más información, consulte el capítulo **Cuentas de usuario > Administrar autenticación en dos fases** de la Guía del administrador.

- **Configuración del servidor NTP**. El servidor NTP se utiliza para la sincronización horaria entre todos appliances GravityZone. De forma predeterminada, se proporciona una dirección de servidor NTP, que puede cambiar en el campo **Dirección del servidor NTP**.

  Nota
  Para que los appliances GravityZone se comuniquen con el servidor NTP, tiene que estar abierto el puerto 123 (UDP).

- **Habilitar Syslog**. Al habilitar esta función, permite que GravityZone envíe notificaciones a un servidor de registro que utiliza el protocolo Syslog. Así tiene la posibilidad de controlar mejor los eventos de GravityZone.

  Para ver o configurar la lista de notificaciones enviadas al servidor Syslog, consulte el capítulo **Notificaciones** de la Guía del administrador de GravityZone.

  Para habilitar el registro en un servidor Syslog remoto:

  1. Marque la casilla de verificación **Habilitar Syslog**.
  2. Introduzca el nombre del servidor o la IP, el protocolo preferido y el puerto de escucha de Syslog..
  3. Seleccione el formato en que desea enviar los datos al servidor Syslog:

– **Formato JSON**. JSON es un formato liviano de intercambio de datos completamente independiente de cualquier lenguaje de programación. JSON representa los datos en un formato de texto legible por humanos. En el formato JSON, los detalles de cada evento se estructuran en objetos, cada uno de los cuales consiste en un par nombre/valor.

  Por ejemplo:

```
{
    "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"
}
```

  Para obtener más información, consulte www.json.org.

  Este es el formato por defecto en GravityZone.

– **Formato de evento común (CEF)**. CEF es un estándar abierto, desarrollado por ArcSight, que simplifica la administración de registros.

  Por ejemplo:

```
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
```

  Para obtener más información, consulte el Estándar de implementación del formato de evento común (CEF) de ArcSight.

En el capítulo **Notificaciones** de la Guía del administrador, puede ver los tipos de notificación disponibles en cada formato.

4. Haga clic en el botón ⊕ **Añadir** de la columna **Acción**.

Haga clic en **Guardar** para aplicar los cambios.

Copia de seguridad

Para asegurarse de que todos los datos de su Control Center están a salvo, puede que desee hacer una copia de seguridad de la base de datos de GravityZone. Puede realizar tantas copias de seguridad de la base de datos como desee, o puede programar copias de seguridad periódicas para que se ejecuten automáticamente en un intervalo de tiempo especificado.

Cada comando de copia de seguridad de la base de datos crea un archivo `tgz` (archivo comprimido Tar GZIP) en la ubicación especificada en los ajustes de la copia de seguridad.

Cuando haya varios administradores con privilegios de administración sobre los ajustes de Control Center, también puede configurar las **Opciones de notificación** para que se le avise cada vez que se haya completado una copia de seguridad de la base de datos. Para más información, consulte el capítulo **Notificaciones** de la Guía del administrador de GravityZone.

Creación de copias de seguridad de bases de datos

Para realizar una copia de seguridad de la base de datos:

1. Acceda a la página **Configuración** en Control Center y haga clic en la pestaña **Copia de seguridad**.
2. Haga clic en el botón **Copiar ahora** en la zona superior de la tabla. Aparecerá una nueva ventana de configuración.
3. Seleccione el tipo de ubicación donde se guardará el archivo de copia de seguridad:
   - **Local**, para guardar el archivo de copia de seguridad en el appliance GravityZone. En tal caso, tiene que especificar la ruta de acceso al directorio concreto del appliance GravityZone donde se guardará el archivo.

     El appliance GravityZone posee una estructura de directorios Linux. Por ejemplo, puede optar por crear la copia de seguridad en el directorio `tmp`. De ser así, introduzca `/tmp` en el campo **Ruta**.
   - **FTP**, para guardar el archivo de copia de seguridad en un servidor FTP. En este caso, escriba los detalles del FTP en los campos correspondientes.

- **Red**, para guardar el archivo de copia de seguridad en un recurso compartido de red. De ser este el caso, introduzca la ruta de acceso a la ubicación de red que desee (por ejemplo, `\\equipo\carpeta`), el nombre de dominio y las credenciales de usuario del dominio.

4. Pulse el botón **Probar ajustes**. Un aviso de texto le informará de si los ajustes especificados son válidos o no.

   Para crear una copia de seguridad, todos los ajustes tienen que ser válidos.

5. Haga clic en **Generar**. Se mostrará la página **Copia de seguridad**. Se añadirá a la lista una nueva copia de seguridad. Compruebe el **Estado** de la nueva copia de seguridad. Cuando se complete la copia de seguridad, hallará el archivo `tgz` en la ubicación especificada.

> **Nota**
> La lista disponible en la página **Copia de seguridad de** contiene los registros de todas las copias de seguridad creadas. Estos registros no proporcionan acceso a los archivos de copia de seguridad; solo muestran la información de las copias de seguridad creadas.

Para programar una copia de seguridad de la base de datos:

1. Acceda a la página **Configuración** en Control Center y haga clic en la pestaña **Copia de seguridad**.
2. Haga clic en el botón **Ajustes de copia de seguridad** en la zona superior de la tabla. Aparecerá una nueva ventana de configuración.
3. Seleccione **Copia de seguridad programada**.
4. Configure el intervalo de la copia de seguridad (diaria, semanal o mensual) y la hora de inicio.

   Por ejemplo, puede programar copias de seguridad para que se realicen semanalmente, todos los viernes, a partir de las 22:00.

5. Configure la ubicación de la copia de seguridad programada.
6. Seleccione el tipo de ubicación donde se guardará el archivo de copia de seguridad:

   - **Local**, para guardar el archivo de copia de seguridad en el appliance GravityZone. En tal caso, tiene que especificar la ruta de acceso al directorio concreto del appliance GravityZone donde se guardará el archivo.

El appliance GravityZone posee una estructura de directorios Linux. Por ejemplo, puede optar por crear la copia de seguridad en el directorio `tmp`. De ser así, introduzca `/tmp` en el campo **Ruta**.

- **FTP**, para guardar el archivo de copia de seguridad en un servidor FTP. En este caso, escriba los detalles del FTP en los campos correspondientes.
- **Red**, para guardar el archivo de copia de seguridad en un recurso compartido de red. De ser este el caso, introduzca la ruta de acceso a la ubicación de red que desee (por ejemplo, `\\equipo\carpeta`), el nombre de dominio y las credenciales de usuario del dominio.

7. Pulse el botón **Probar ajustes**. Un aviso de texto le informará de si los ajustes especificados son válidos o no.

   Para crear una copia de seguridad, todos los ajustes tienen que ser válidos.

8. Haga clic en **Guardar** para crear la copia de seguridad programada.

Restauración de la copia de seguridad de una base de datos

Cuando por algún motivo su instancia de GravityZone no funcione adecuadamente (actualizaciones fallidas, problemas operativos de la interfaz, archivos dañados, errores, etc.), puede restaurar la base de datos de GravityZone a partir de una copia de seguridad mediante:

- El mismo appliance
- Una imagen nueva de GravityZone
- La característica del Conjunto de réplicas

Elija la opción que mejor se adapte a su situación y no proceda a la restauración hasta haber leído detenidamente los requisitos descritos a continuación.

Restauración de la base de datos al mismo appliance virtual GravityZone

Requisitos

- Una conexión SSH con el appliance GravityZone, con privilegios de **root**.

  Puede usar **putty** y las credenciales de **bdadmin** para conectarse al appliance mediante SSH y, a continuación, ejecutar el comando `sudo su` para cambiar a la cuenta **root**.

- La infraestructura de GravityZone no ha cambiado desde la copia de seguridad.

- La copia de seguridad es anterior al 30 de abril de 2017 y la versión de GravityZone es superior a la 6.2.1-30. En caso contrario, póngase en contacto con el equipo de soporte técnico.
- En arquitecturas distribuidas, GravityZone no se ha configurado para usar la replicación de bases de datos (Conjunto de réplicas).

  Para comprobar la configuración, siga estos pasos:

  1. Abra el archivo `/etc/mongodb.conf`.
  2. Compruebe que `replSet` no está configurado, como en el siguiente ejemplo:

     ```
     # replSet = setname
     ```

  Nota
  Para restaurar la base de datos cuando esté habilitado el Conjunto de réplicas, consulte "Restauración de la base de datos en un entorno de Conjunto de réplicas" (p. 87).

- No hay procesos de la CLI en ejecución.

  Para asegurarse de que todos los procesos de la CLI están detenidos, ejecute el siguiente comando:

  ```
  # killall -9 perl
  ```

- El paquete **mongoconsole** está instalado en el appliance.

  Para comprobar que se cumple esta condición, ejecute este comando:

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

  El comando no debería devolver ningún error; de lo contrario, ejecute:

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

Restauración de la base de datos

1. Acceda a la ubicación que contiene el archivo de base de datos:

   ```
   # cd /directorio-con-backup
   ```

   , donde `directorio-con-backup` es la ruta hasta la ubicación de los archivos de copia de seguridad.

   Por ejemplo:

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

2. Restaure la base de datos.

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

   Importante
   Asegúrese de sustituir `GZ_db_password` por la contraseña real del Servidor de base de datos de GravityZone y las variables de marca de tiempo en el nombre del archivo por la fecha real.
   Por ejemplo, la fecha real debería parecerse a esta:

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

3. Reinicie los appliances.

   Ha finalizado la restauración de la base de datos.

Restauración de la base de datos a partir de un appliance virtual GravityZone fuera de servicio

Requisitos

- Una instalación de un nuevo appliance virtual GravityZone:
  - Con la misma IP que el appliance antiguo.

– SOLO con el rol de Servidor de bases de datos instalado.

Puede descargar la imagen del appliance virtual GravityZone desde aquí.

- Una conexión SSH con el appliance virtual GravityZone, con privilegios de **root**.
- La infraestructura de GravityZone no ha cambiado desde que se efectuó la copia de seguridad.
- La copia de seguridad es anterior al 30 de abril de 2017.
- En arquitecturas distribuidas, GravityZone no se ha configurado para usar la replicación de bases de datos (Conjunto de réplicas).

  Si utiliza el Conjunto de réplicas en su entorno GravityZone, también tiene el rol de Servidor de bases de datos instalado en otras instancias del appliance.

  Para restaurar la base de datos cuando esté habilitado el Conjunto de réplicas, consulte "Restauración de la base de datos en un entorno de Conjunto de réplicas" (p. 87).

Restauración de la base de datos

1. Conéctese al appliance GravityZone a través de SSH y pase a **raíz**.
2. Detenga VASync:

   ```
   # stop vasync
   ```

3. Detenga el CLI:

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

4. Acceda a la ubicación donde se encuentra la copia de seguridad:

   ```
   # cd /directorio-con-backup
   ```

   , donde `directorio-con-backup` es la ruta hasta la ubicación de los archivos de copia de seguridad.

   Por ejemplo:

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

5. Restaure la base de datos.

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

Importante
Asegúrese de sustituir `GZ_db_password` por la contraseña real del Servidor de base de datos de GravityZone y las variables de marca de tiempo en el nombre del archivo por la fecha real.
Por ejemplo, la fecha real debería parecerse a esta:

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

6. Restaure el ID del appliance antiguo:

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

Importante
Recuerde reemplazar `GZ_db_password` por la contraseña real del Servidor de base de datos de GravityZone.

7. Elimine la referencia a los roles antiguos.

```
# /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
```

Importante
Recuerde reemplazar `GZ_db_password` por la contraseña real del Servidor de base de datos de GravityZone.

8. Inicie VASync:

```
# start vasync
```

9. Inicie el CLI:

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

10. Instale los otros roles.

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

Tenga en cuenta que el esquema de la base de datos se ha actualizado correctamente a la versión más reciente:

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

11. Reinicie el dispositivo.

Ha finalizado la restauración de la base de datos.

Restauración de la base de datos en un entorno de Conjunto de réplicas

Si ha implementado la base de datos en un entorno de Conjunto de réplicas, puede encontrar el procedimiento oficial de restauración en el manual online de mongoDB (solo en inglés).

Nota
Este procedimiento requiere conocimientos técnicos avanzados y solo debe llevarlo a cabo un técnico capacitado. Si tiene dificultades, póngase en contacto con nuestro Soporte técnico para que le ayude en la restauración de la base de datos.

Active Directory

Mediante la integración de Active Directory, puede importar en Control Center el inventario existente desde Active Directory local y desde Active Directory alojado en Microsoft Azure, lo que simplifica la implementación, administración, monitorización e informes de la seguridad. Además, pueden asignarse distintos roles a los usuarios de Active Directory en Control Center.

Para integrar y sincronizar GravityZone con un dominio de Active Directory:

1. Acceda a **Configuración > Active Directory > Dominios** y haga clic en ⊕ **Añadir**.
2. Configure los ajustes precisos:
   - Intervalo de sincronización (en horas)
   - Nombre del dominio de Active Directory (incluyendo la extensión del dominio)
   - Nombre de usuario y contraseña de un administrador de dominio
   - Ubicación en el inventario de red donde mostrar los endpoints de AD:
     - Mantener la estructura de AD e ignorar las unidades organizativas vacías
     - Ignorar la estructura de AD e importar a grupos personalizados
     - Mantener la estructura de AD solo con las unidades organizativas seleccionadas
   - Los controladores de dominio con los que se sincroniza Control Center. Expanda la sección **Solicitar controlador de dominio** y elija los controladores en la tabla.
3. Haga clic en **Guardar**.

Importante
Siempre que cambie la contraseña de usuario, recuerde también actualizarla en Control Center.

Permisos de acceso

Con los permisos de acceso puede otorgar acceso a GravityZone Control Center a los usuarios de Active Directory (AD) en función de las reglas de acceso. Para integrar y sincronizar dominios de AD, consulte Active Directory. Para obtener más

información sobre la administración de cuentas de usuario mediante reglas de acceso, consulte el capítulo **Cuentas de usuario** de la Guía de instalación de GravityZone.

Proveedores de virtualización

GravityZone puede integrarse actualmente con VMware vCenter Server, Citrix XenServer, Nutanix Prism Element, Amazon EC2 y Microsoft Azure.

- "Integrar con vCenter Server" (p. 89)
- "Integrar con XenServer" (p. 92)
- "Integración con Nutanix Prism Element" (p. 93)
- "Integración con Amazon EC2" (p. 95)
- "Integrar con Microsoft Azure" (p. 96)
- "Administración de plataformas integradas" (p. 97)

Importante
Siempre que establezca una nueva integración con otro vCenter Server, XenServer, Nutanix Prism Element o Microsoft Azure, recuerde también revisar y actualizar los privilegios de acceso para los usuarios existentes.

Integrar con vCenter Server

Puede integrar GravityZone con uno o con varios sistemas vCenter Server. Los sistemas vCenter Server en modo Linked deben añadirse a Control Center de forma independiente.

Para configurar la integración con un vCenter Server:

1. Acceda a la página **Configuración** en Control Center y acceda a la pestaña **Proveedores de virtualización > Plataformas de administración**.
2. Haga clic en el botón ⊕ **Añadir** de la parte superior de la tabla y seleccione **vCenter Server** desde el menú. Aparecerá una nueva ventana de configuración.
3. Especifique los detalles de vCenter Server.
   - Nombre del sistema vCenter Server en Control Center
   - Nombre del host o dirección IP del sistema vCenter Server
   - Puerto vCenter Server (predeterminado `443`)
4. Especifique las credenciales a utilizar para autenticarse con el vCenter Server. Puede elegir usar las credenciales proporcionadas para la integración con Active

Directory o un conjunto de credenciales diferente. El usuario cuyas credenciales proporcione deberá tener permisos de administrador o root en el vCenter Server.

5. Elija la plataforma de VMware instalada en su entorno y configure los ajustes en consecuencia:

   - **Ninguna**. Seleccione esta opción para NSX-T si no hay instalada ninguna plataforma de VMware concreta y haga clic en **Guardar**. Se requiere aceptar el certificado de seguridad autofirmado para la integración.

     Para configurar la integración de NSX-T Manager y aplicar la protección de endpoints a sus máquinas virtuales mediante la política de Guest Introspection de GravityZone, consulte el siguiente artículo de la base de conocimientos.

   - **vShield**. Especifique los detalles del sistema vShield Manager integrado con vCenter Server.
     - Nombre del host o dirección IP del sistema vShield Manager
     - Puerto vShield Manager (predeterminado `443`)

   - **NSX-V**. Especifique los detalles del NSX Manager integrado con vCenter Server.

     Nota
     Para actualizar de VMware vShield a NSX, consulte este artículo de la base de conocimientos.

     - Nombre de host o dirección IP del NSX Manager
     - Puerto del NSX Manager (`443` por defecto)
     - Nombre de usuario y contraseña utilizada para autenticarse en el NSX Manager.

       Estas credenciales se guardarán en la entidad protegida, no en el Gestor de credenciales.
     - Marque la casilla de verificación **Etiquetar si se encuentra un virus** para utilizar las etiquetas de seguridad de NSX por defecto cuando se encuentra malware en la máquina virtual.

       Se puede etiquetar una máquina con tres etiquetas de seguridad diferentes en función del nivel de riesgo de la amenaza.

- `ANTI_VIRUS.VirusFound.threat=low`, se aplica a la máquina cuando Bitdefender encuentra malware de bajo riesgo, que puede eliminar.
- `ANTI_VIRUS.VirusFound.threat=medium`, se aplica a la máquina si Bitdefender no puede eliminar los archivos infectados, pero sí desinfectarlos.
- `ANTI_VIRUS.VirusFound.threat=high`, se aplica a la máquina si Bitdefender no puede ni eliminar ni desinfectar los archivos infectados, pero sí bloquear el acceso a ellos.

Cuando se detecten amenazas de diferentes niveles de riesgo en la misma máquina, se aplicarán todas las etiquetas correspondientes. Por ejemplo, una máquina en la que se haya encontrado malware de alto y de bajo riesgo, tendrá ambas etiquetas de seguridad.

Nota
Puede encontrar las etiquetas de seguridad de VMware vSphere, en la pestaña **Red y seguridad > NSX Managers >** `NSX Manager` **> Administrar > Etiquetas de seguridad**.
Aunque puede crear tantas etiquetas como desee, Bitdefender solo funciona con las tres mencionadas.

6. **Restringir la asignación de políticas desde la vista de red**. Utilice esta opción para controlar los permisos de los administradores de red para cambiar las políticas de las máquinas virtuales desde la vista **Equipos y máquinas virtuales** de la página **Red**. Cuando se selecciona esta opción, los administradores pueden cambiar las políticas de las máquinas virtuales solo desde la vista **Máquinas virtuales** del inventario de red.
7. Haga clic en **Guardar**. Se le pedirá que acepte los certificados de seguridad para vCenter Server y NSX Manager. Estos certificados garantizan una comunicación segura entre los componentes de VMware y GravityZone, lo que evita el riesgo de ataques man-in-the-middle.

   Puede verificar si se instalaron los certificados correctos cotejando la información sobre el sitio del navegador para cada componente de VMware con la información del certificado que aparece en Control Center.
8. Marque las casillas de verificación para aceptar el uso de los certificados.

9. Haga clic en **Guardar**. Podrá ver el vCenter Server en la lista de integraciones activas.
10. Si utiliza la plataforma NSX-V:
    a. Acceda a la pestaña **Actualizar > Componentes**.
    b. Descargue y luego publique el paquete **Security Server (VMware con NSX)**. Para obtener más información sobre cómo actualizar los componentes de GravityZone, consulte "Actualización de GravityZone" (p. 190).
    c. Acceda a la pestaña **Configuración > Proveedores de virtualización**.
    d. En la columna **Acción**, haga clic en el botón **Registrar** correspondiente al vCenter integrado con NSX para registrar el servicio de Bitdefender con NSX Manager de VMware.

    Aviso
    Cuando el certificado de seguridad haya caducado y vCenter intente sincronizar, una ventana emergente le preguntará si desea actualizarlo. Entre en la ventana de configuración de la integración de vCenter Server, haga clic en **Guardar**, acepte los nuevos certificados y haga clic nuevamente en **Guardar**.

    Después del registro, Bitdefender añade a la consola de VMware vSphere:
    - Servicio de Bitdefender
    - Administrador de servicio de Bitdefender
    - Tres nuevos perfiles de servicio por defecto para los modos de análisis tolerante, normal y agresivo.

    Nota
    También puede ver estos perfiles de servicio en la página **Políticas** de Control Center. Haga clic en el botón **Columnas** de la parte superior derecha del panel derecho para ver información adicional.

Al final, puede ver que el vCenter Server se está sincronizando. Espere un par de minutos hasta que finalice la sincronización.

Integrar con XenServer

Puede integrar GravityZone con uno o con varios sistemas XenServer.

Para configurar la integración con un XenServer:

1. Acceda a la página **Configuración** en Control Center y haga clic en la pestaña **Proveedores de virtualización**.
2. Haga clic en el botón ⊕ **Añadir** de la parte superior de la tabla y seleccione **XenServer** desde el menú. Aparecerá una nueva ventana de configuración.
3. Especifique los detalles de XenServer.
   - Nombre del sistema XenServer en Control Center
   - Nombre del host o dirección IP del sistema XenServer
   - Puerto XenServer (predeterminado `443`)
4. Especifique las credenciales a utilizar para autenticarse con el XenServer. Puede elegir usar las credenciales proporcionadas para la integración con Active Directory o un conjunto de credenciales diferente.
5. **Restringir la asignación de políticas desde la vista de red**. Utilice esta opción para controlar los permisos de los administradores de red para cambiar las políticas de las máquinas virtuales desde la vista **Equipos y máquinas virtuales** de la página **Red**. Cuando se selecciona esta opción, los administradores pueden cambiar las políticas de las máquinas virtuales solo desde la vista **Máquinas virtuales** del inventario de red.
6. Haga clic en **Guardar**. Podrá ver el vCenter Server en la lista de integraciones activas y que se está sincronizando. Espere un par de minutos hasta que finalice la sincronización.

Integración con Nutanix Prism Element

Puede integrar GravityZone con uno o varios clusters de Nutanix Prism Element, ya estén registrados o no en Nutanix Prism Central.

Para configurar la integración con Nutanix Prism Element:

1. Acceda a la página **Configuración** en Control Center y haga clic en la pestaña **Proveedores de virtualización**.
2. Haga clic en el botón ⊕ **Añadir** de la parte superior de la tabla y seleccione **Nutanix Prism Element** en el menú. Aparecerá una nueva ventana de configuración.
3. Especifique los detalles del Nutanix Prism Element:
   - Nombre del Nutanix Prism Element en Control Center.
   - La dirección IP de una Controller Virtual Machine (CVM) del cluster Nutanix Prism Element o la dirección IP de la IP virtual del cluster.

- Puerto de Nutanix Prism Element (`9440` por defecto).

4. Especifique las credenciales que se han de utilizar para autenticarse con Nutanix Prism Element.

   Importante
   El usuario cuyas credenciales proporcione debe tener privilegios de administrador de clusters o de administrador de usuarios en Nutanix Prism Element.

5. **Restringir la asignación de políticas desde la vista de red**. Utilice esta opción para controlar los permisos de los administradores de red para cambiar las políticas de las máquinas virtuales desde la vista **Equipos y máquinas virtuales** de la página **Red**. Cuando se selecciona esta opción, los administradores pueden cambiar las políticas de las máquinas virtuales solo desde la vista de máquinas virtuales del inventario de red.
6. Haga clic en **Guardar**. Se le pedirá que acepte los certificados de seguridad para Nutanix Prism. Estos certificados garantizan una comunicación segura entre los componentes de Nutanix Prism Element y GravityZone, lo que evita el riesgo de ataques man-in-the-middle.

   Puede comprobar si se instalaron los certificados correctos cotejando la información sobre el sitio del navegador para cada cluster de Nutanix Prism Element o CVM con la información del certificado que aparece en Control Center.
7. Marque las casillas de verificación para aceptar el uso de los certificados.
8. Haga clic en **Guardar**.

   Si introdujo una IP de la CVM para configurar la integración, se le preguntará en una nueva ventana si desea usar la IP virtual del cluster en lugar de la IP de la CVM:

   a. Haga clic en **Sí** para usar la IP virtual del cluster para la integración. La IP virtual del cluster reemplazará a la IP de la CVM en los detalles de Nutanix Prism Element.

   b. Haga clic en **No** para seguir usando la IP de la CVM.

      Nota
      Se recomienda utilizar la IP virtual del cluster en lugar de la IP de la CVM. De esta manera, la integración permanece activa incluso cuando un host concreto deja de estar disponible.

c. En la ventana **Añadir Nutanix Prism Element**, haga clic en **Guardar**.

Podrá ver el Nutanix Prism Element en la lista de integraciones activas. Espere un par de minutos hasta que finalice la sincronización.

Integración con Amazon EC2

Puede integrar GravityZone con su inventario de Amazon EC2 y proteger sus instancias de EC2 alojadas en la nube de Amazon.

Requisitos:

- El acceso y las claves secretas de una cuenta de AWS válida
- La cuenta de AWS debe tener los siguientes permisos:
  - `IAMReadOnlyAccess`
  - `AmazonEC2ReadOnly` para todas las regiones de AWS

Puede crear varias integraciones de Amazon EC2. Para cada integración, debe proporcionar una cuenta de usuario de AWS válida.

Nota
No es posible añadir varias integraciones usando las credenciales de los roles de IAM creados para la misma cuenta de AWS.

Para configurar la integración con Amazon EC2:

1. Acceda a la página **Configuración** en Control Center y haga clic en la pestaña **Proveedores de virtualización**.
2. Haga clic en el botón ⊕ **Añadir** de la parte superior de la tabla y seleccione **Integración de Amazon EC2** en el menú. Aparecerá una nueva ventana de configuración.
3. Especifique los detalles de la integración de Amazon EC2:
   - El nombre de la integración. Si añade varias integraciones de Amazon EC2, puede identificarlas por su nombre.
   - El acceso y las claves secretas de la cuenta de usuario de AWS.
4. **Restringir la asignación de políticas desde la vista de red**. Utilice esta opción para controlar los permisos de los administradores de red para cambiar las políticas de las máquinas virtuales desde la vista **Equipos y máquinas virtuales** de la página **Red**. Cuando se selecciona esta opción, los administradores pueden

cambiar las políticas de las máquinas virtuales solo desde la vista **Máquinas virtuales** del inventario de red.

5. Haga clic en **Guardar**. Si las credenciales proporcionadas son válidas, la integración se creará y se añadirá.

Espere unos momentos mientras GravityZone se sincroniza con el inventario de Amazon EC2.

Integrar con Microsoft Azure

Puede integrar GravityZone con Microsoft Azure y proteger sus máquinas virtuales alojadas en la nube de Microsoft.

Requisitos:

- Aplicación de Azure con permisos de lectura
- ID de Active Directory
- ID de aplicación
- Secreto de la aplicación

Para informarse de cómo obtener las credenciales necesarias y cómo configurar la aplicación de Azure, consulte este artículo de la base de conocimientos.

Puede crear varias integraciones de Microsoft Azure. Para cada integración, debe tener un ID válido de Active Directory.

Para configurar la integración con Microsoft Azure:

1. Acceda a la página **Configuración** en Control Center y haga clic en la pestaña **Proveedores de virtualización**.
2. Haga clic en el botón ⊕ **Añadir** de la parte superior de la tabla y seleccione **Integración de Azure** en el menú. Aparecerá una nueva ventana de configuración.
3. Especifique los detalles de la integración de Azure:
   - **El nombre de la integración**. Si añade varias integraciones de Azure, puede identificarlas por su nombre.
   - **ID de Active Directory**. Cada instancia de Azure Active Directory tiene un identificador único disponible en la información de la cuenta de Microsoft Azure.
   - **ID de aplicación**. Cada aplicación de Azure tiene un identificador único disponible en la información de la aplicación.

- **Secreto de la aplicación**. El secreto de la aplicación es el valor que se muestra al guardar una clave en los ajustes de la aplicación de Azure.

4. Seleccione la opción **Restringir la asignación de políticas desde la vista de red** para cambiar la política solo desde la vista de **Máquinas virtuales**. Si no está marcada, puede cambiar la política desde la vista de **Equipos y máquinas virtuales**.
5. Haga clic en **Guardar**. Si las credenciales proporcionadas son válidas, la integración se creará y se añadirá.

Espere unos momentos mientras GravityZone se sincroniza con el inventario de Microsoft Azure.

Administración de plataformas integradas

Para modificar o actualizar la integración de una plataforma:

1. En Control Center, acceda a la pestaña **Configuración > Proveedores de virtualización**.
2. Haga clic en el botón **Editar** de la columna **Acción**.
3. Configure los ajustes de la regla según sea necesario. Para obtener más información, consulte una de las secciones siguientes según el caso:
   - “Integrar con vCenter Server” (p. 89)
   - “Integrar con XenServer” (p. 92)
   - “Integración con Nutanix Prism Element” (p. 93)
   - “Integración con Amazon EC2” (p. 95)
   - “Integrar con Microsoft Azure” (p. 96)
4. Haga clic en **Guardar**. Espere un par de minutos hasta que el servidor se resincronice.

Las integraciones de Nutanix Prism Element, Amazon EC2 y Microsoft Azure se sincronizan automáticamente cada quince minutos. Puede sincronizar manualmente una integración en cualquier momento de la siguiente manera:

1. En Control Center, acceda a la pestaña **Configuración > Proveedores de virtualización**.
2. Haga clic en el botón **Resincronizar** de la columna **Acción**.
3. Haga clic en **Sí** para confirmar la acción.

El botón **Resincronizar inventario** es especialmente útil cuando cambia el estado de integración y requiere sincronización, como en las siguientes situaciones:

- Para la integración de Nutanix Prism Element:
  - El usuario ya no tiene privilegios administrativos en el inventario.
  - El usuario deja de ser válido (contraseña modificada o eliminada).
  - El certificado de seguridad deja de ser válido.
  - Hay un error de conexión.
  - Se añade o elimina un host en el cluster de Nutanix Prism Element.
- Para la integración de Microsoft Azure:
  - Se añade o elimina una suscripción en Microsoft Azure.
  - Las máquinas virtuales se añaden o eliminan en el inventario de Microsoft Azure.

También puede sincronizar la integración haciendo clic en el botón **Editar** y, a continuación, haciendo clic en **Guardar**.

Para eliminar una integración de vShield, XenServer, Nutanix Prism Element, Amazon EC2 o Microsoft Azure:

1. En Control Center, acceda a la pestaña **Configuración > Proveedores de virtualización**.
2. Haga clic en el botón **Eliminar** de la columna **Acción** correspondiente a la integración que desee eliminar.
3. Haga clic en **Sí** para confirmar la acción.

Para eliminar una integración de NSX:

1. Inicie sesión en la consola de VMware vSphere y elimine todos los Security Server y políticas de Bitdefender.
2. En Control Center, acceda a la pestaña **Configuración > Proveedores de virtualización**.
3. En la columna **Acción** correspondiente a la integración que desea eliminar, haga clic en **Anular registro** y, luego, en **Eliminar**.
4. Haga clic en **Sí** para confirmar la acción.

Para asegurarse de que se está mostrando la información más reciente, haga clic en el botón **Actualizar** de la zona superior de la tabla.

Proveedores de seguridad

GravityZone Security for Virtualized Environments se integra con VMware NSX-T Data Center a través de NSX-T Manager.

Integración con el administrador de NSX-T

NSX-T Manager es el plan de administración de sus servidores vCenter integrados con un NSX-T Data Center. Para que la integración funcione, deberá configurar la integración de los servidores vCenter asociados con el NSX-T Manager. Para más información, consulte Integrar con vCenter Server.

Para establecer la integración con NSX-T Manager:

1. En Control Center, acceda a **Configuración > Proveedores de virtualización > Proveedores de seguridad**.
2. Haga clic en el botón ⊕ **Añadir** en la parte superior de la tabla. Aparecerá una nueva ventana de configuración.
3. Especifique los detalles de la integración NSX-T:
   - Nombre de la integración NSX-T.
   - Nombre del host o dirección IP del sistema vCenter Server asociado.
   - Puerto NSX-T (por defecto 433).
4. Especifique las credenciales para autenticarse con el vCenter Server. Puede elegir usar las credenciales proporcionadas para la integración con Active Directory o un conjunto de credenciales diferente. El usuario cuyas credenciales proporcione deberá tener permisos de administrador o root en el vCenter Server.
5. Haga clic en **Guardar**.

   Control Center está ahora integrado con NSX-T. Para aplicar la protección de endpoints a sus máquinas virtuales mediante la política de introspección de guest de GravityZone, consulte el artículo de la base de conocimientos Configurar y aplicar la protección de endpoints a las máquinas virtuales guest VMware NSX-T mediante la política de introspección de guest de GravityZone.

Nota
GravityZone solo se puede usar para proteger el servidor vCenter asociado.

NTSA

En esta sección, puede configurar la integración con Bitdefender Network Traffic Security Analytics, una solución de seguridad empresarial que detecta con precisión las vulneraciones y proporciona información sobre los ataques avanzados mediante el análisis del tráfico de red. Para obtener más información sobre esta solución, consulte la documentación de Bitdefender NTSA.

Importante
La sección de integración de NTSA está disponible solo después de proporcionar una clave de licencia válida de NTSA en la página **Configuración > Licencia**.

Para configurar la integración de NTSA, debe tener la solución NTSA instalada en su entorno y credenciales para acceder a la consola web de NTSA.

Durante la integración, se le pedirá que proporcione la dirección de la consola web de NTSA (IP o nombre de host) y un token (clave de vinculación) generado en la consola web de NTSA, como se explica más adelante.

Configurar la integración de NTSA

1. Inicie sesión en GravityZone Control Center.
2. Acceda a la página **Configuración** y haga clic en la pestaña NTSA.
3. Active la opción **Integrar con Network Traffic Security Analytics (NTSA)**.
4. Introduzca los siguientes datos:
   - La dirección de la consola web de NTSA (IP/nombre de host).
   - El puerto utilizado por GravityZone para comunicarse con NTSA (443 por defecto).
   - La clave de vinculación (token) generada por la consola web de NTSA de la siguiente manera:
     a. Acceda a su consola web de NTSA y vaya a la página de **Licencias**.
     b. Seleccione la opción **Integración con GravityZone**.
     c. Haga clic en **Generar clave de vinculación**. La clave aparecerá automáticamente.
     d. Utilice el botón **Copiar al portapapeles** para obtener la clave de vinculación.

e. Haga clic en **Aceptar** para confirmar.

5. Compruebe que la huella digital del host que se muestra coincida con el hash del certificado SSL del appliance NTSA y, a continuación, habilite la opción **Acepto el certificado**.
6. Haga clic en **Guardar**.

Cuando la configuración haya finalizado correctamente, la integración se mostrará como **Sincronizada**. La integración de NTSA puede presentar los siguientes estados:

- **N/D**: la integración no se ha configurado aún.
- **Sincronizada**: la integración está configurada y habilitada.
- **Token no válido**: la clave de vinculación de la consola web de NTSA no es válida.
- **Error de conexión**: no se pudo conectar con la dirección de la consola web de NTSA especificada (IP/nombre de host no válido).
- **Error de certificado**: la huella digital actual del certificado SSL del appliance NTSA no coincide con la aceptada inicialmente.
- **Error desconocido**: se ha producido un error de comunicación desconocido.

El campo **Último cambio de estado** muestra la fecha y la hora del último cambio correcto de los ajustes de integración o del último cambio de estado de la integración.

Una vez configurada la integración con NTSA, puede inhabilitar o habilitar la integración mediante la casilla de verificación disponible en la parte superior de la página **NTSA**.

Vincular sus cuentas de GravityZone y NTSA

Tras configurar la integración, se vincularán sus cuentas de GravityZone y NTSA y podrá navegar fácilmente a la consola web de NTSA de la siguiente manera:

1. En GravityZone Control Center, haga clic en el botón **NTSA** situado en la esquina inferior izquierda de la ventana.
2. Se le redirigirá a la página de inicio de sesión de la consola web de NTSA. Después de introducir sus credenciales de inicio de sesión de NTSA, puede empezar a navegar por la consola web de NTSA.

   Solo necesita introducir sus credenciales de NTSA la primera vez. Después, se le otorgará acceso a la consola web de NTSA automáticamente haciendo clic en el botón **NTSA**, sin que se le pida iniciar sesión.

Eliminar la integración de NTSA

Al eliminar la clave de licencia de NTSA de la página **Configuración > Licencia** se eliminará también la integración de NTSA.

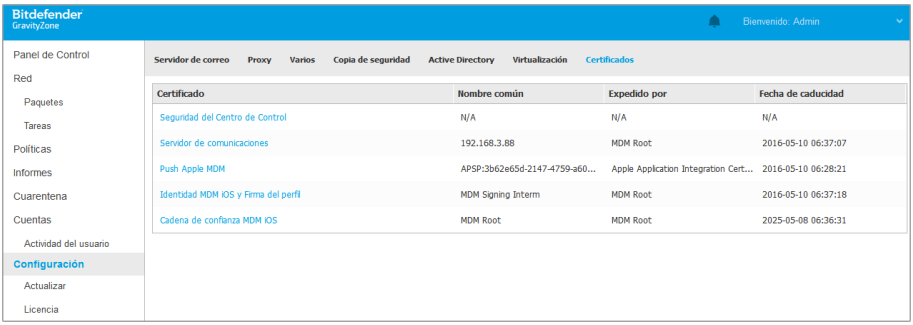
Nota

Su cuenta de NTSA y GravityZone se desvincularán en las siguientes situaciones:

- La clave de licencia de NTSA se ha eliminado.
- Su contraseña de NTSA ha cambiado.
- Su contraseña de GravityZone ha cambiado.
- Se han modificado los ajustes de integración de NTSA.

Certificados

Para que su implementación de GravityZone funcione correctamente y con seguridad, debe crear y añadir una serie de certificados de seguridad en Control Center.



La página de Certificados

Control Center es compatible con los siguientes formatos de certificado:

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

Nota
Los siguientes certificados son necesarios exclusivamente para la gestión de la seguridad en los dispositivos iOS de Apple:

- Certificado del Servidor de comunicaciones
- Certificado Push MDM de Apple
- Certificado de firma de perfil e identidad MDM iOS
- Certificado de cadena de confianza MDM iOS

Si no tiene pensado llevar a cabo la administración de dispositivos móviles iOS, no necesita proporcionar estos certificados.

Certificado de Seguridad de Control Center

El certificado de Seguridad de Control Center es necesario para identificar la consola Web de Control Center como un sitio Web de confianza en el navegador Web. Control Center utiliza por omisión el certificado SSL firmado por Bitdefender. Este certificado integrado no es reconocido por los navegadores Web y dispara alertas de seguridad. Para evitar las alertas de seguridad del navegador, añada un certificado SSL firmado por su empresa o por una Certificate Authority (CA) externa.

Para añadir o reemplazar el certificado de Control Center:

1. Acceda a la página **Configuración** y haga clic en la pestaña **Certificados**.
2. Haga clic en el nombre del certificado.
3. Seleccione el tipo de certificado (con clave privada independiente o incrustada).
4. Haga clic en el botón **Añadir** junto al campo **Certificado** y cargue el certificado.
5. Para los certificados con claves privadas independientes, haga clic en el botón **Añadir** junto al campo **Clave privada** y cargue la clave privada.
6. Si el certificado está protegido por contraseña, escriba la contraseña en el campo correspondiente.
7. Haga clic en **Guardar**.

Endpoint - Certificado de seguridad de comunicaciones de Security Server

Este certificado garantiza una comunicación segura entre los agentes de seguridad y el Security Server (multiplataforma) asignado.

Durante su implementación, el Security Server genera un certificado autofirmado predeterminado. Puede reemplazar este certificado incorporado añadiendo en Control Center uno de su elección.

Para añadir o reemplazar un endpoint - Certificado de comunicaciones de Security Server:

1. Acceda a la página **Configuración** y haga clic en la pestaña **Certificados**.
2. Haga clic en el nombre del certificado.
3. Seleccione el tipo de certificado (con clave privada independiente o incrustada).
4. Haga clic en el botón **Añadir** junto al campo **Certificado** y cargue el certificado.
5. Para los certificados con claves privadas independientes, haga clic en el botón **Añadir** junto al campo **Clave privada** y cargue la clave privada.
6. Si el certificado está protegido por contraseña, escriba la contraseña en el campo correspondiente.
7. Haga clic en **Guardar**. Si el certificado está autofirmado o ha caducado podría aparecer un mensaje de advertencia. Si ha caducado, renueve su certificado.
8. Haga clic en **Sí** para seguir cargando el certificado. En cuanto finalice la carga, Control Center enviará el certificado de seguridad a los Security Server.

Si es necesario, puede volver al certificado original incorporado de cada Security Server de la siguiente manera:

1. Haga clic en el nombre del certificado en la página **Certificados**.
2. Elija **Sin certificado (utilizar predeterminado)** como tipo de certificado.
3. Haga clic en **Guardar**.

Certificado del Servidor de comunicaciones

El certificado del Servidor de comunicaciones se utiliza para asegurar la comunicación entre el Servidor de comunicaciones y los dispositivos móviles iOS.

Requisitos:

- Este certificado SSL puede firmarlo o bien su empresa, o bien una Autoridad de Certificación (Certificate Authority) externa.

Aviso
El certificado puede ser invalidado si no lo emite una autoridad de certificación pública o de confianza (por ejemplo, certificados autofirmados).

- El nombre común del certificado debe coincidir exactamente con el nombre de dominio o dirección IP utilizada por los clientes móviles para conectarse al Servidor de comunicaciones. Esto se configura como una dirección MDM externa en la interfaz de configuración de la consola del appliance GravityZone.
- Los clientes móviles deben confiar en este certificado. Para esto, debe añadir también el certificado de Cadena de confianza iOS MDM.

Para añadir o reemplazar el certificado del Servidor de comunicaciones:

1. Acceda a la página **Configuración** y haga clic en la pestaña **Certificados**.
2. Haga clic en el nombre del certificado.
3. Seleccione el tipo de certificado (con clave privada independiente o incrustada).
4. Haga clic en el botón **Añadir** junto al campo **Certificado** y cargue el certificado.
5. Para los certificados con claves privadas independientes, haga clic en el botón **Añadir** junto al campo **Clave privada** y cargue la clave privada.
6. Si el certificado está protegido por contraseña, escriba la contraseña en el campo correspondiente.
7. Haga clic en **Guardar**.

Certificado Push MDM de Apple

Apple requiere un Certificado Push MDM para garantizar la comunicación segura entre el Servidor de comunicaciones y el servicio Apple Push Notifications (APNs) cuando se envían notificaciones push. Las notificaciones push se utilizan para solicitar a los dispositivos que se conecten al Servidor de comunicación cuando hay disponibles nuevas tareas o se producen cambios en las políticas.

Apple emite este certificado directamente a su empresa, pero requiere que la Solicitud de firma de certificado (CSR) esté firmada por Bitdefender. El Control Center proporciona un asistente para ayudarle a obtener fácilmente su certificado Push MDM de Apple.

Importante

- Necesita un ID de Apple para obtener y administrar el certificado. Si no dispone de un ID de Apple puede crear uno en la página Web Mi ID de Apple. Utilice una dirección de correo electrónico genérica y no la de un empleado para registrarse en el ID de Apple, dado que la necesitará más adelante para renovar el certificado.
- El sitio Web de Apple no funciona correctamente en Internet Explorer. Recomendamos el uso de las últimas versiones de Safari o Chrome.
- El certificado Push MDM de Apple es válido solo por un año. Cuando el certificado esté a punto de caducar, debe renovarlo e importar el certificado renovado en Control Center. Si deja que el certificado caduque, deberá crear uno nuevo y volver a activar todos sus dispositivos.

Añadir un certificado Push MDM de Apple

Para obtener el certificado Push MDM de Apple e importarlo en Control Center:

1. Acceda a la página **Configuración** y haga clic en la pestaña **Certificados**.
2. Haga clic en el nombre del certificado y siga el asistente como se indica a continuación:

   Paso 1 - Obtener una solicitud de firma de certificado firmada por Bitdefender

   Seleccione la opción adecuada:

   - **Necesito generar una solicitud de firma de certificado firmada por Bitdefender** (Recomendado)
     a. Introduzca el nombre de su empresa, su nombre completo y su dirección de correo electrónico en los campos correspondientes.
     b. Haga clic en **Generar** para descargar el archivo CSR firmado por Bitdefender.
   - **Ya poseo una solicitud de firma de certificado y necesito que lo firme Bitdefender**
     a. Cargue el archivo CSR y la clave privada asociada haciendo clic en el botón **Añadir** situado junto a los campos correspondientes.

        El Servidor de comunicaciones necesita la clave privada para la autenticación con los servidores APNs.
     b. Especifique la contraseña que protege la clave privada, de existir.
     c. Haga clic en el botón **Firmar** para descargar el archivo CSR firmado por Bitdefender.

Paso 2 - Solicitar un certificado push de Apple

a. Haga clic en el enlace **Portal de certificados push de Apple** e inicie sesión con su ID de Apple y su contraseña.
b. Haga clic en el botón **Crear un certificado** y acepte los Términos de uso.
c. Haga clic en **Seleccionar archivo**, seleccione el archivo CSR y, a continuación, haga clic en **Cargar**.

> **Nota**
> Puede que el botón **Seleccionar archivo** se llame de una forma diferente, como por ejemplo **Elegir** o **Examinar**, dependiendo del navegador que utilice.

d. En la página de confirmación, haga clic en el botón **Descargar** para recibir su certificado Push MDM.
e. Regrese al asistente de Control Center.

Paso 3 - Importar el certificado push de Apple

Haga clic en el botón **Añadir certificado** para cargar el archivo del certificado desde su equipo.

Puede comprobar la información del certificado en el campo de abajo.

3. Haga clic en **Guardar**.

Renovación del certificado Push MDM Apple

Para renovar el certificado Push MDM de Apple y actualizarlo en Control Center:

1. Acceda a la página **Configuración** y haga clic en la pestaña **Certificados**.
2. Haga clic en el nombre del certificado para abrir el asistente de importación.
3. Obtenga una Solicitud de firma de certificado firmada por Bitdefender. El procedimiento es el mismo que para la obtención de un certificado nuevo.
4. Haga clic en el enlace **Portal de certificados push de Apple** e inicie sesión con el mismo ID de Apple que utilizó para crear el certificado.
5. Busque el certificado Push MDM de Bitdefender y haga clic en el botón **Renovar** correspondiente.
6. Haga clic en **Seleccionar archivo**, seleccione el archivo CSR y, a continuación, haga clic en **Cargar**.
7. Haga clic en **Descargar** para guardar el certificado en su equipo.
8. Vuelva a Control Center e importe el nuevo certificado push de Apple.
9. Haga clic en **Guardar**.

Certificado de firma de perfil e identidad MDM iOS

El Servidor de comunicaciones utiliza el certificado de firma de perfil e identidad iOS MDM para firmar los certificados de identidad y perfiles de configuración enviados a los dispositivos móviles.

Requisitos:

- Debe ser un certificado de Entidad final o Intermedia, firmado o bien por su empresa o bien por una Autoridad de Certificación (Certificate Authority) externa.
- Los clientes móviles deben confiar en este certificado. Para esto, debe añadir también el certificado de Cadena de confianza iOS MDM.

Para añadir o reemplazar el certificado de firma de perfil y el de identidad MDM iOS:

1. Acceda a la página **Configuración** y haga clic en la pestaña **Certificados**.
2. Haga clic en el nombre del certificado.
3. Seleccione el tipo de certificado (con clave privada independiente o incrustada).
4. Haga clic en el botón **Añadir** junto al campo **Certificado** y cargue el certificado.
5. Para los certificados con claves privadas independientes, haga clic en el botón **Añadir** junto al campo **Clave privada** y cargue la clave privada.
6. Si el certificado está protegido por contraseña, escriba la contraseña en el campo correspondiente.
7. Haga clic en **Guardar**.

Certificado de cadena de confianza MDM iOS

Los certificados de Cadena de confianza MDM iOS son necesarios para garantizar que confían en el Certificado del Servidor de comunicación y en el Certificado de firma de perfil e identidad MDM iOS. El Servidor de comunicación envía este certificado a los dispositivos móviles durante la activación.

El certificado de Cadena de confianza iOS MDM debe incluir todos los certificados intermedios hasta el certificado raíz de su empresa o hasta el certificado intermedio emitido por la Autoridad de certificación externa.

Para añadir o reemplazar los certificados de Cadena de confianza MDM iOS:

1. Acceda a la página **Configuración** y haga clic en la pestaña **Certificados**.
2. Haga clic en el nombre del certificado.

3. Haga clic en el botón **Añadir** junto al campo **Certificado** y cargue el certificado.
4. Haga clic en **Guardar**.

Repositorio

Esta pestaña muestra información acerca de las actualizaciones del agente de seguridad, incluyendo las versiones del producto almacenadas en el Servidor de actualizaciones, así como las disponibles en el repositorio oficial de Bitdefender, anillos de actualización, la fecha y hora de la actualización y la última búsqueda de nuevas versiones.

Nota
Las versiones del producto no están disponibles para Servidores de seguridad.

5.1.5. Administrar el appliance GravityZone

El appliance GravityZone se entrega con una interfaz de configuración básica, disponible desde la herramienta de administración utilizada para gestionar el entorno virtualizado donde ha implementado el appliance.

Estas son las principales opciones disponibles después de implementar el primer appliance GravityZone:

- Configurar los ajustes del nombre del host
- Configure las Opciones de red
- Configurar opciones proxy
- Servidor de comunicaciones MDM
- Opciones avanzadas
- Configurar idioma

Utilice las teclas de flecha y la tecla `Tabulador` para navegar por los menús y opciones. Pulse `Intro` para seleccionar una opción específica.

Configurar el nombre del host y los ajustes

La comunicación con los roles de GravityZone se realizan usando la dirección IP o nombre DNS del appliance en el que están instalados. Los componentes de GravityZone se comunican de forma predeterminada usando direcciones IP. Si desea activar la comunicación a través de nombres DNS, debe configurar los

appliances GravityZone con un nombre DNS y asegurar que resuelve correctamente con las direcciones IP configuradas del appliance.

Requisitos:

- Configure el registro DNS en el servidor DNS
- El nombre DNS debe resolver correctamente la dirección IP configurada en el appliance. Por ello, debe asegurarse de que el appliance está configurado con la dirección IP correcta.

Para configurar los ajustes del nombre del host:

1. Acceda a la consola del appliance desde su herramienta de administración de la virtualización (por ejemplo, vSphere Client).
2. En el menú principal, seleccione **Configurar los ajustes del nombre del host**.
3. Escriba el nombre del host del appliance y el nombre de dominio de Active Directory (si fuera necesario).
4. Seleccione **Aceptar** para guardar los cambios.

Configure las Opciones de red

Puede configurar el appliance para que obtenga los ajustes de red automáticamente desde el servidor DHCP o puede configurar los ajustes de red manualmente. Si elige utilizar DHCP, debe configurar el Servidor DHCP para reservar direcciones IP específicas para el appliance.

Para configurar los ajustes de red:

1. Acceda a la consola del appliance desde su herramienta de administración de la virtualización (por ejemplo, vSphere Client).
2. Desde el menú principal, seleccione **Configurar ajustes de red**.
3. Seleccione la interfaz de red (predeterminada `eth0`).
4. Seleccione el método de configuración:
   - **Configure los ajustes de red manualmente.** Debe especificar la dirección IP, máscara de red, dirección de puerta de enlace y direcciones de servidores DNS.
   - **Obtener ajustes de red automáticamente a través de DHCP.** Utilice esta opción si ha configurado el servidor DHCP para reservar direcciones IP específicas para el appliance.

5. Puede comprobar los detalles de la configuración IP actual o estado de enlace seleccionando las opciones correspondientes.

Configurar opciones proxy

Si su appliance está conectado a Internet a través de un servidor proxy, debe configurar las opciones del proxy.

Nota
Los ajustes del proxy pueden configurarse también desde Control Center, página **Configuración > Proxy**. Cambiar los ajustes del proxy en una ubicación los actualiza automáticamente también en otras ubicaciones.

Para configurar las opciones del proxy:

1. Acceda a la consola del appliance desde su herramienta de administración de la virtualización (por ejemplo, vSphere Client).
2. Desde el menú principal, seleccione **Configurar ajustes del proxy**.
3. Seleccione **Configurar las opciones de proxy**.
4. Escriba la dirección del servidor proxy. Utilice la siguiente sintaxis:
   - Si el servidor proxy no requiere autenticación:

     `http(s)://<IP/nombredelhost>:<puerto>`
   - Si el servidor proxy requiere autenticación:

     `http(s)://<nombredeusuario>:<contraseña>@<IP/nombredelhost>:<puerto>`
5. Seleccione **Aceptar** para guardar los cambios.

Seleccione **Mostrar información proxy** para comprobar los ajustes del proxy.

Servidor de comunicaciones MDM

Nota
Esta configuración solo se requiere para la administración de dispositivos móviles, si su clave de licencia cubre el servicio Security for Mobile. La opción aparece en el menú después de instalar el rol de Servidor de comunicaciones.

En la configuración predeterminada de GravityZone, los dispositivos móviles pueden gestionarse solamente cuando están conectados directamente a la red corporativa (vía Wi-Fi o VPN). Esto ocurre porque al inscribir los dispositivos móviles están

configurados para conectarse a la dirección local del appliance Servidor de comunicaciones.

Para poder gestionar dispositivos móviles a través de Internet, con independencia de dónde estén localizados, debe configurar el Servidor de comunicaciones con una dirección accesible públicamente.

Para poder administrar dispositivos móviles cuando no están conectados a la red de la empresa, están disponibles las siguientes opciones:

- Configurar un puerto de envío en la puerta de enlace corporativa para el appliance que ejecuta el rol de Servidor de comunicaciones.
- Añadir un adaptador de red adicional al appliance que desempeña el rol de Servidor de comunicaciones y asignarle una dirección IP pública.

En ambos casos debe configurar el Servidor de comunicaciones con la dirección externa para utilizar la gestión de dispositivos móviles:

1. Acceda a la consola del appliance desde su herramienta de administración de la virtualización (por ejemplo, vSphere Client).
2. En el menú principal, seleccione **Servidor de comunicaciones MDM**.
3. Seleccione **Configurar dirección externa del Servidor MDM**.
4. Escriba la dirección externa.

   Utilice la siguiente sintaxis: `https://<IP/Dominio>:<Puerto>`.

   - Si utiliza reenvío de puertos, debe escribir la dirección IP pública o el nombre de dominio y el puerto abierto en la puerta de enlace.
   - Si utiliza una dirección pública para el Servidor de comunicaciones, debe escribir la dirección IP pública o nombre de dominio y el puerto del Servidor de comunicaciones. El puerto predeterminado es `8443`.
5. Seleccione **Aceptar** para guardar los cambios.
6. Seleccione **Mostrar dirección externa de Servidor MDM** para comprobar los ajustes.

Opciones avanzadas

Los ajustes avanzados cubren varias opciones para la implementación manual, la extensión del entorno y las mejoras de la seguridad:

- Instalar/desinstalar roles

- Instalar Security Server
- Establecer la nueva contraseña de la base de datos
- Update Server
- Configurar balanceadores de rol
- Conjunto de réplicas
- Habilitar Cluster VPN seguro
- Conectarse a la base de datos existente
- Conectarse a la base de datos existente (Cluster VPN seguro)
- Comprobar Cluster VPN seguro

La disponibilidad de opciones varía según los roles instalados y los servicios habilitados. Por ejemplo, si el rol de Servidor de base de datos no está instalado en el appliance, solo puede instalar roles o conectarse a una base de datos GravityZone implementada en su red. Una vez que el rol de Servidor de base de datos se ha instalado en el appliance, dejan de estar disponibles las opciones para conectarse a otra base de datos.

Instalar/desinstalar roles

El appliance GravityZone puede desempeñar uno, varios o todos los roles siguientes:

- **Servidor de base de datos**
- **Update Server**
- **Consola Web**
- **Servidor de comunicaciones**
- **Servidor de incidentes**

Una implementación de GravityZone requiere ejecutar una instancia de cada rol. Consecuentemente, implementará entre uno y cuatro appliances GravityZone, dependiendo de cómo prefiera distribuir los roles de GravityZone. El rol de Servidor de base de datos es el primero en instalarse. En un escenario con múltiples appliances GravityZone, instalará el rol de Servidor de base de datos en el primer appliance y configurará los otros appliances para conectarse con la instancia de base de datos existente.

Nota

Puede instalar instancias adicionales de roles específicos usando los balanceadores de roles. Para más información, diríjase a "Configurar balanceadores de rol" (p. 117).

Para instalar los roles GravityZone:

1. Acceda a la consola del appliance desde su herramienta de administración de la virtualización (por ejemplo, vSphere Client).
2. En el menú principal, seleccione **Configuración avanzada**.
3. Seleccione **Instalar/desinstalar roles**.
4. Seleccione **Añadir o eliminar roles**.
5. Proceda de acuerdo con su situación actual:
   - Si esta es la implementación inicial del appliance GravityZone, pulse la `barra espaciadora` y luego `Intro` para instalar el rol de Servidor de base de datos. Debe confirmar su elección pulsando `Intro` nuevamente. Configure la contraseña de la base de datos y espere a que finalice la instalación.
   - Si ya ha instalado otro appliance con el rol de Servidor de base de datos, elija **Cancelar** y vuelva al menú **Añadir o eliminar roles**. Luego debe seleccionar **Configurar dirección de la base de datos** e introducir la dirección del servidor de base de datos. Asegúrese de establecer una contraseña para la base de datos antes de acceder a esta opción. Si desconoce la contraseña de la base de datos, configure una nueva seleccionando **Ajustes avanzados > Establecer nueva contraseña de base de datos** en el menú principal.

     Utilice la siguiente sintaxis: `http://<IP/Nombredelhost>:<Puerto>`. El puerto predeterminado de la base de datos es `27017`. Introduzca la contraseña de base de datos principal.
6. Instale los otros roles seleccionando **Añadir o eliminar roles** en el menú **Instalar/desinstalar roles** y luego los roles que desee instalar. Para cada función que desee instalar o desinstalar, pulse la `barra espaciadora` para seleccionar o anular la selección del rol y luego pulse `Intro` para continuar. Debe confirmar su elección pulsando `Intro` nuevamente y esperar a que se complete la instalación.

Nota

Cada rol se instala normalmente en unos minutos. Durante la instalación, se descargan los archivos necesarios de Internet. Por consiguiente, la instalación lleva más tiempo si la conexión a Internet es lenta. Si la instalación se bloquea, reinstale el appliance.

Puede ver los roles instalados y sus direcciones IP seleccionando una de las siguientes opciones del menú **Instalar/desinstalar roles**:

- Puede **mostrar roles instalados localmente** para ver solo los roles instalados en ese appliance.
- También puede **mostrar todos los roles instalados** para ver todos los roles instalados en su entorno GravityZone.

Instalar Security Server

Nota
Solo podrá utilizar el Security Server si su clave de licencia lo permite.

Puede instalar el Security Server desde la interfaz de configuración del appliance GravityZone, directamente en el appliance GravityZone o desde Control Center como un appliance independiente. Las ventajas de la instalación del Security Server desde el appliance son:

- Adecuado para implementaciones de GravityZone con un solo appliance que tenga todos los roles.
- Puede ver y utilizar el Security Server sin tener que integrar GravityZone con una plataforma de virtualización.
- Menos operaciones de implementación que realizar.

Requisitos:

El appliance GravityZone debe tener instalado el rol de servidor de base de datos, o debe estar configurado para conectarse a una base de datos existente.

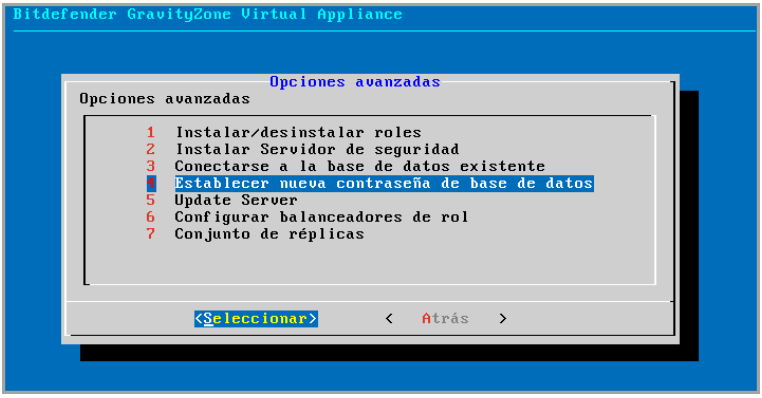
Para instalar el Security Server desde la interfaz del appliance:

1. Acceda a la consola del appliance desde su herramienta de administración de la virtualización (por ejemplo, vSphere Client).
2. En el menú principal, seleccione **Configuración avanzada**.
3. Seleccione **Instalar Security Server**. Aparecerá un mensaje de confirmación.
4. Pulse `Intro` para continuar y espere hasta que finalice la instalación.

Nota
Puede desinstalar este Security Server solo desde el menú **Configuración avanzada** de la interfaz del appliance.

Establecer la nueva contraseña de la base de datos

Al instalar el rol de Servidor de base de datos, debe establecer una contraseña para proteger la base de datos. Si desea cambiarla, establezca una nueva accediendo a **Ajustes avanzados > Establecer nueva contraseña de base de datos** en el menú principal.



Interfaz de consola del appliance: opción de Establecer nueva contraseña de base de datos

Siga las directrices para establecer una contraseña segura.

Configurar Servidor de actualizaciones

El appliance GravityZone está configurado de forma predeterminada para actualizarse desde Internet. Si lo prefiere, puede ajustar sus appliances para actualizarse desde el servidor de actualización local de Bitdefender (el appliance GravityZone con el rol Servidor de actualización instalado).

Para establecer la dirección del servidor de actualización:

1. Acceda a la consola del appliance desde su herramienta de administración de la virtualización (por ejemplo, vSphere Client).
2. En el menú principal, seleccione **Configuración avanzada**.
3. Seleccione **Servidor de actualizaciones**.
4. Seleccione **Configurar dirección de actualización**.

5. Introduzca la dirección IP o nombre del host del appliance que ejecuta el rol de Servidor de actualización. El puerto predeterminado del Servidor de actualización es el `7074`.

Configurar balanceadores de rol

Para garantizar la fiabilidad y escalabilidad, puede instalar múltiples instancias de roles específicos (Servidor de comunicación, Consola Web).

Para garantizar la fiabilidad y escalabilidad, puede instalar múltiples instancias de roles específicos (Servidor de incidentes, Servidor de comunicaciones, Consola Web).

Cada instancia de rol se instala en un appliance diferente.

Todas las instancias de un rol específico deben estar conectadas a los otros roles a través de un balanceador de roles.

El appliance GravityZone incluye balanceadores incorporados que puede instalar y utilizar. Si ya posee software o hardware de balanceo dentro de su red, puede elegir utilizarlo en lugar de usar los balanceadores integrados.

Los balanceadores de roles integrados no pueden instalarse junto con roles en un appliance GravityZone.

1. Acceda a la consola del appliance desde su herramienta de administración de la virtualización (por ejemplo, vSphere Client).
2. En el menú principal, seleccione **Configuración avanzada**.
3. Seleccione **Configurar equilibradores de roles**.
4. Seleccione la opción deseada:
   - **Utilizar balanceadores externos.** Seleccione esta opción si su infraestructura de red ya incluye software o hardware de balanceo que pueda utilizar. Debe introducir la dirección del balanceador para cada rol que quiera balancear. Utilice la siguiente sintaxis:

     `http(s)://<IP/nombredelhost>:<puerto>`.
   - **Utilizar balanceadores incorporados.** Seleccione esta opción para instalar y utilizar el software de balanceo integrado.

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

5. Seleccione **Aceptar** para guardar los cambios.

Conjunto de réplicas

Con esta opción puede habilitar el uso de un conjunto de réplicas de base de datos en lugar de una única instancia de servidor de bases de datos. Este mecanismo permite la creación de varias instancias de base de datos en un entorno GravityZone distribuido, garantizando la alta disponibilidad de la base de datos en caso de fallo.

Importante
La replicación de bases de datos solo está disponible para las instalaciones nuevas del appliance GravityZone desde la versión 5.1.17-441.

Configuración del conjunto de réplicas

En primer lugar, ha de habilitar el Conjunto de réplicas en el primer appliance GravityZone instalado. Luego, podrá añadir miembros al conjunto de réplicas mediante la instalación del rol de base de datos en las demás instancias de GravityZone del mismo entorno.

Importante

- El conjunto de réplicas requiere al menos tres miembros para funcionar.
- Puede añadir hasta siete instancias de rol de base de datos como miembros del conjunto de réplicas (limitación de MongoDB).
- Se recomienda utilizar un número impar de instancias de base de datos. Un número par de miembros solo consumirá más recursos pero con los mismos resultados.

Para habilitar la replicación de bases de datos en su entorno GravityZone:

1. Instale el rol de Servidor de base de datos en el primer appliance GravityZone. Para más información, diríjase a “Instalar/desinstalar roles” (p. 113).
2. Configure los demás appliances para que se conecten a la primera instancia de base de datos. Para más información, diríjase a “Conectarse a la base de datos existente” (p. 120).
3. Acceda al menú principal del primer appliance, seleccione **Configuración avanzada** y luego seleccione **Conjunto de réplicas** para habilitarlo. Aparecerá un mensaje de confirmación.
4. Seleccione **Sí** para confirmar.

5. Instale el rol de Servidor de base de datos en los demás appliances GravityZone.

En cuanto se hayan completado los pasos anteriores, todas las instancias de base de datos comenzarán a funcionar como un conjunto de réplicas:

- Se elige una instancia principal, que será la única que acepte las operaciones de escritura.
- La instancia principal escribe en un registro todos los cambios realizados en su conjunto de datos.
- Las instancias secundarias replican este registro y aplican los mismos cambios en sus conjuntos de datos.
- Cuando la instancia principal no esté disponible, el conjunto de réplicas elegirá una de las instancias secundarias como principal.
- Cuando una instancia principal no se comunique con los otros miembros del conjunto durante más de 10 segundos, el conjunto de réplicas intentará seleccionar otro miembro para que se convierta en la nueva instancia principal.

Eliminación de miembros del conjunto de réplicas

Para eliminar miembros del conjunto de réplicas, basta con escoger en la interfaz de consola del appliance (interfaz de menú) **Instalar/desinstalar roles > Añadir o eliminar roles** y desmarcar **Servidor de base de datos**.

Nota
Puede eliminar un miembro del conjunto de réplicas solo si se han instalado en la red al menos cuatro instancias de base de datos.

Habilitar Cluster VPN seguro

Los roles de GravityZone tienen varios servicios internos que se comunican exclusivamente entre sí. Para disponer de un entorno más seguro, puede aislar estos servicios creando un cluster VPN para ellos. Ya estén estos servicios en el mismo appliance o en varios, se comunicarán a través de un canal seguro.

Importante

- Esta característica requiere una implementación estándar de GravityZone, sin ninguna herramienta personalizada instalada.
- Una vez habilitado el cluster, no puede inhabilitarlo.

Para proteger los servicios internos en los appliances:

1. Acceda a la consola del appliance desde su herramienta de administración de la virtualización (por ejemplo, vSphere Client).
2. En el menú principal, seleccione **Configuración avanzada**.
3. Seleccione Habilitar **Cluster VPN seguro**.

   Un mensaje le informa de los cambios que se realizarán.
4. Seleccione **Sí** para confirmar y continuar con la instalación de VPN.

   Al finalizar, se muestra un mensaje de confirmación.

A partir de ahora, todos los roles del appliance se instalan en modo seguro y los servicios se comunicarán a través de la interfaz VPN. Cualquier nuevo appliance que añada al entorno debe unirse al cluster VPN. Para más información, diríjase a "Conectarse a la base de datos existente (Cluster VPN seguro)" (p. 121).

Conectarse a la base de datos existente

En una arquitectura distribuida de GravityZone, deberá instalar el rol de Servidor de base de datos en el primer appliance y luego configurar los otros appliances para que se conecten con la instancia de base de datos existente. De esta manera, todos los appliances compartirán la misma base de datos.

Importante
Se recomienda habilitar el Cluster VPN seguro y conectarse a una base de datos de dicho cluster. Para obtener más información, consulte:

- "Habilitar Cluster VPN seguro" (p. 119)
- "Conectarse a la base de datos existente (Cluster VPN seguro)" (p. 121)

Para conectar el appliance a una base de datos de GravityZone fuera de un Cluster VPN seguro:

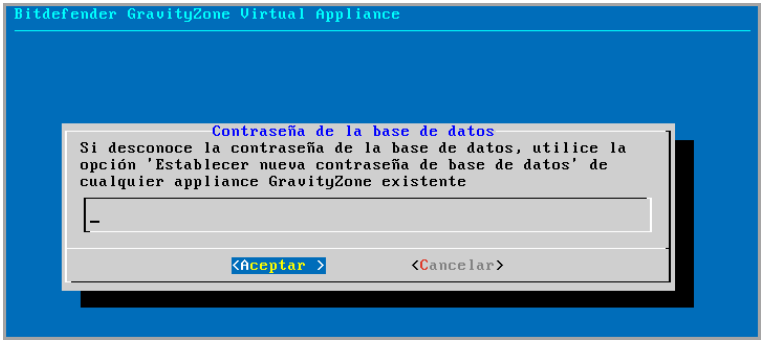
1. Acceda a la consola del appliance desde su herramienta de administración de la virtualización (por ejemplo, vSphere Client).
2. En el menú principal, seleccione **Configuración avanzada**.
3. Seleccione **Conectarse a la base de datos existente**.

Nota
Asegúrese de establecer una contraseña para la base de datos antes de acceder a esta opción. Si desconoce la contraseña de la base de datos, establezca una nueva accediendo a **Ajustes avanzados > Establecer nueva contraseña de base de datos** en el menú principal.

4. Seleccione **Configurar dirección del servidor de base de datos**.
5. Introduzca la dirección de la base de datos con la siguiente sintaxis:

   `<IP/Nombredelhost>:<Puerto>`

   Especificar el puerto es opcional. El puerto predeterminado es el `27017`.
6. Introduzca la contraseña de base de datos principal.



Interfaz de consola del appliance: introduzca la contraseña de la base de datos

7. Seleccione **Aceptar** para guardar los cambios.
8. Seleccione **Mostrar dirección del servidor de base de datos** para asegurar que la dirección se ha configurado correctamente.

Conectarse a la base de datos existente (Cluster VPN seguro)

Use esta opción cuando necesite ampliar su implementación de GravityZone con más appliances y el Cluster VPN seguro esté habilitado. De esta manera, el nuevo appliance compartirá la misma base de datos con la implementación existente en modo seguro.

Para obtener más información sobre el Cluster VPN seguro, consulte "Habilitar Cluster VPN seguro" (p. 119).

Requisitos

Antes de continuar, asegúrese de tener a mano lo siguiente:

- Dirección IP del Servidor de base de datos
- Contraseña del usuario **bdadmin** en el appliance con el rol de Servidor de base de datos

Conectarse a la base de datos

Para conectar el appliance a una base de datos de GravityZone dentro de un Cluster VPN seguro:

1. Acceda a la consola del appliance desde su herramienta de administración de la virtualización (por ejemplo, vSphere Client).
2. En el menú principal, seleccione **Configuración avanzada**.
3. Seleccione **Conectarse a la base de datos existente (Cluster VPN seguro)**.

   Se le informará de los requisitos y alternativas en caso de que no se cumplan.
4. Seleccione **Aceptar** para confirmar y continuar.
5. Introduzca la dirección IP del Servidor de base de datos dentro del Cluster VPN seguro.
6. Introduzca la contraseña del usuario **bdadmin** en el appliance del Servidor de base de datos.
7. Seleccione **Aceptar** para guardar los cambios y continuar.

Cuando finalice el proceso, recibirá un mensaje de confirmación. El nuevo appliance se convertirá en miembro del cluster y se comunicará con los otros appliances de forma segura. Todos los appliances compartirán la misma base de datos.

Comprobar el estado del Cluster VPN seguro

Esta opción está disponible solo después de haber habilitado previamente el Cluster VPN seguro. Seleccione esta opción para comprobar qué appliances de su implementación de GravityZone no han protegido aún sus servicios. Es posible que deba investigar más a fondo y ver si los appliances están online y accesibles.

Configurar idioma

Para cambiar el idioma de la interfaz de la configuración del appliance:

1. Seleccione **Configurar idioma** en el menú principal.
2. Seleccione el idioma deseado entre las opciones disponibles. Aparecerá un mensaje de confirmación.

   Nota
   Es posible que tenga que desplazarse hacia abajo para ver su idioma.

3. Seleccione **Aceptar** para guardar los cambios.

5.2. Administración de Licencias

Los servicios de seguridad GravityZone se licencian y venden de forma independiente. Cada servicio de seguridad GravityZone requiere una clave de licencia básica válida. Debe proporcionarse al menos una clave de licencia válida para utilizar GravityZone.

Además de los servicios básicos de seguridad, GravityZone también proporciona características de protección importantes como complementos. La licencia de cada complemento se concede mediante una clave independiente que puede usarse sola o junto con una licencia básica válida. Si la licencia principal no es válida, verá los ajustes de las características pero no podrá utilizarlas.

Puede elegir probar GravityZone y decidir si es la solución adecuada para su organización. Para activar su periodo de evaluación, debe escribir las claves de licencia del mensaje de correo de registro en Control Center.

Nota
Control Center se suministra gratuitamente con cualquier servicio de seguridad GravityZone.

Para seguir utilizando el servicio de seguridad una vez finalizado el periodo de evaluación, debe adquirir una clave de licencia y utilizarla para registrar el servicio.

Para comprar una licencia, contacte con un reseller de Bitdefender o contáctenos a través del e-mail enterprisesales@bitdefender.com.

Las claves de licencia de GravityZone pueden administrarse desde la página **Configuración > Licencia** en Control Center. Cuando su clave de licencia actual

esté a punto de caducar, aparecerá un mensaje en la consola informándole de que necesita ser renovada. Para introducir una nueva clave de licencia o ver los detalles de la licencia actual, diríjase a la página **Configuración > Licencia**.

5.2.1. Encontrar un reseller

Nuestros resellers le proporcionarán toda la información que necesite y le ayudarán a elegir la mejor opción de licencia para usted.

Para encontrar un reseller de Bitdefender en su país:

1. Acceda a la página del Buscador de partners en el sitio Web de Bitdefender.
2. Seleccione el país en el que reside para ver la información de contacto de los partners de Bitdefender disponibles.
3. Si no encuentra un reseller Bitdefender en su país, no dude en contactar con nosotros por correo en comercial@bitdefender.es.

5.2.2. Introducción de sus claves de licencia

El registro de la licencia de GravityZone se puede hacer online u offline (cuando no haya conexión a Internet). En ambos casos, ha de proporcionar una clave de licencia válida para cada servicio de seguridad que desee utilizar.

Para el registro offline necesitará también el código de registro offline asociado a la clave de licencia.

Puede introducir varias claves de licencia para el mismo servicio, pero sólo permanecerá activa la última clave introducida.

Para aplicar la licencia de sus servicios de seguridad de GravityZone, cambiar la clave de licencia actual o introducir una clave independiente para un complemento:

1. Inicie sesión en Control Center usando una cuenta de administrador de empresa.
2. Diríjase a la página **Configuración > Licencia**.
3. Haga clic en el botón ⊕ **Añadir** en la parte superior de la tabla.
4. Seleccione el tipo de registro:
   - **online**. En este caso, introduzca una clave de licencia válida en el campo **Clave de licencia**. La clave de licencia se verificará y se validará online.
   - **Offline**, cuando no haya conexión a Internet. En este caso, tendrá que proporcionar la clave de licencia y también su código de registro.

   Si la clave de licencia no es válida, se mostrará un error de validación en forma de información rápida sobre el campo **Clave de licencia**.

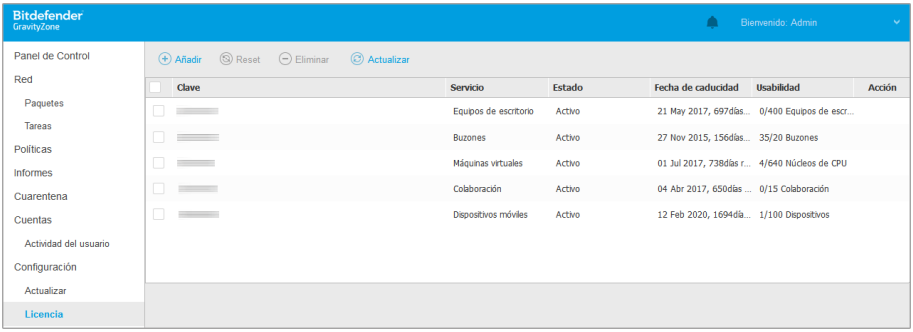
5. Haga clic en **Añadir**. Se añadirá la clave de licencia a la página de **Licencia**, donde podrá comprobar su información.
6. Haga clic en **Guardar** para aplicar los cambios. Control Center se reinicia y es necesario volver a iniciar sesión para ver los cambios.

Nota
Puede usar los complementos siempre que haya una licencia básica compatible válida. De lo contrario, verá las características pero no podrá utilizarlas.

5.2.3. Comprobar los detalles de licencia actuales

Para ver los detalles de su licencia:

1. Inicie sesión en Control Center usando una cuenta de administrador de empresa.
2. Diríjase a la página **Configuración > Licencia**.



La página Licencia

3. En la tabla, puede ver los detalles sobre las claves de licencia existentes.
   - Clave de licencia
   - Servicio de seguridad al que se aplica la clave de licencia
   - Estado de la clave de licencia

     Importante
     Sólo se puede activar una clave de licencia a la vez para un servicio específico.

   - Fecha de caducidad y periodo de licencia restante

Importante
Cuando caduca la licencia, se desactivan los módulos de protección de los agentes instalados. Como resultado de ello, los endpoints dejan de estar protegidos y no es posible realizar ninguna tarea de análisis. Cualquier nuevo agente instalado comenzará en periodo de evaluación.

- Cómputo de utilización de la licencia

5.2.4. Restablecer el contador de uso de licencia

Puede hallar información respecto al recuento de uso de sus claves de licencia en la página **Licencia**, bajo la columna **Uso**.

Si precisa actualizar la información de uso, seleccione la clave de licencia que desee y haga clic en el botón **Restablecer** en la parte superior de la tabla.

5.2.5. Borrado de claves de licencia

Puede elegir borrar claves de licencia no válidas o caducadas en la página **Licencia**.

Aviso
Al borrar una clave de licencia se eliminará el servicio de seguridad correspondiente de Control Center. No podrá instalar ni administrar la protección que ofrece ese servicio en los endpoints de su red. Sin embargo, los endpoints permanecerán protegidos siempre y cuando la clave de licencia sea válida.
Si introduce una nueva clave de licencia válida que incluya el servicio previamente eliminado, volverán a habilitarse en Control Center todas las características de ese servicio.

Para eliminar una clave de licencia:

1. Inicie sesión en Control Center usando una cuenta de administrador de empresa.
2. Diríjase a la página **Configuración > Licencia**.
3. Seleccione la clave de licencia que desee eliminar y haga clic en el botón **Borrar** de la parte superior de la tabla.

5.3. Instalación de la protección de endpoints

Dependiendo de la configuración de las máquinas y del entorno de red, puede elegir instalar solo los agentes de seguridad o usar también un Security Server. En este último caso, tiene que instalar primero el Security Server y, luego, los agentes de seguridad.

Se recomienda utilizar el Security Server en entornos virtualizados como Nutanix, VMware o Citrix Xen, o si las máquinas cuentan con recursos de hardware escasos.

Importante
Solo Bitdefender Tools y Bitdefender Endpoint Security Tools admiten la conexión a un Security Server. Para más información, diríjase a "Architecture GravityZone" (p. 11).

5.3.1. Instalación de Security Server

Security Server es una máquina virtual dedicada que deduplica y centraliza la mayoría de las funciones antimalware de los clientes antimalware, actuando como servidor de análisis.

La implementación de Security Server es específica del entorno en el que está instalado. A continuación se describen los procedimientos de instalación:

- Security Server para VMware NSX
- Security Server multiplataforma o para VMware vShield
- Security Server para Amazon EC2
- Security Server para Microsoft Azure

Instalación de Security Server para VMware NSX

En entornos VMware NSX, debe implementar el servicio de Bitdefender en cada cluster que vaya a protegerse. El appliance especialmente diseñado se implementará automáticamente en todos los hosts del cluster. Todas las máquinas virtuales de un host se conectan automáticamente a la instancia de Security Server instalada en ese host, a través de Guest Introspection.

La implementación de Security Server se realizará exclusivamente desde vSphere Web Client.

Para instalar el servicio de Bitdefender:

1. Inicie sesión en vSphere Web Client.
2. Acceda a **Red y seguridad > Instalación** y haga clic en la pestaña **Implementaciones de servicios**.
3. Haga clic en el botón **Implementación de nuevo servicio** (el icono del signo más). Se abre la ventana de configuración.
4. Seleccione **Guest Introspection** y haga clic en **Siguiente**.

5. Seleccione el centro de datos y los clusters en los que se implementará el servicio y, a continuación, haga clic en **Siguiente**.
6. Seleccione la red de administración y almacenamiento, haga clic en **Siguiente** y luego en **Finalizar**.
7. Repita los pasos del 3 al 6, esta vez escogiendo el servicio de **Bitdefender**.

   Antes de proceder a la instalación, asegúrese de disponer de conexión de red entre la red seleccionada y GravityZone Control Center.

   Una vez instalado el servicio de Bitdefender, implementará automáticamente Security Server en todos los hosts ESXi de los clusters seleccionados.

Aviso
Para que los servicios funcionen correctamente, es muy importante que los instale por este orden: primero Guest Introspection y luego Bitdefender, y no ambos al mismo tiempo.

Nota
Para obtener más información sobre la adición de servicios de partner a NSX, consulte el Centro de documentación de VMware NSX.
Si elige **Especificado en el host** para la red de administración y almacenamiento, compruebe que el Agente VM está configurado en los hosts, tanto para los servicios de Bitdefender como para Guest Introspection.

Security Server posee requisitos específicos que dependen del número de máquinas virtuales que haya que proteger. Para ajustar la configuración de hardware predeterminada de Security Server:

1. Inicie sesión en VMware vSphere Web Client.
2. Acceda a **Hosts y clusters**.
3. Seleccione el cluster donde se implementa Security Server y, a continuación, seleccione la pestaña **Objetos relacionados > Máquinas virtuales**.
4. Apague el appliance de **Bitdefender**.
5. Haga clic con el botón derecho en el nombre del appliance y, a continuación, elija **Editar configuración...** en el menú contextual.
6. En la pestaña **Hardware virtual**, ajuste los valores de CPU y RAM para que satisfagan sus necesidades y, a continuación, haga clic en **Aceptar** para guardar los cambios.

7. Vuelva a encender el appliance.

Nota
Para actualizar de VMware vShield a NSX, consulte este artículo de la base de conocimientos.

Instalación de Security Server multiplataforma o para VMware vShield

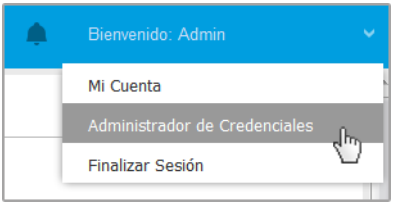
1. Conéctese a la plataforma de virtualización
2. Instale Security Server en los hosts

Conexión a la plataforma de virtualización

Para acceder a la infraestructura virtualizada integrada con Control Center, debe proporcionar sus credenciales de usuario para cada sistema servidor de virtualización disponible. Control Center usa sus credenciales para conectar con la infraestructura virtualizada, mostrando solamente los recursos a los que tiene acceso (según se define en el vCenter Server).

Para especificar las credenciales para conectarse a los sistemas servidores de virtualización:

1. Haga clic en su nombre de usuario en la esquina superior derecha de la página y seleccione **Gestor de credenciales**.



El menú Red > Paquetes

2. Vaya a la pestaña **Entorno virtual**.
3. Especifique las credenciales de autenticación necesarias.
   a. Seleccione un servidor desde el menú correspondiente.

Nota
Si el menú no está disponible, o bien no se ha configurado todavía la integración, o todas las credenciales necesarias ya han sido configuradas.

b. Escriba su nombre de usuario y contraseña, y una descripción adecuada.

c. Haga clic en el botón ⊕ **Añadir**. El nuevo conjunto de credenciales se muestra en la tabla.

Nota
Sí no ha especificado sus credenciales de autenticación, necesitará introducirlas cuando intente examinar el inventario de cualquier sistema vCenter Server. Una vez introducidas las credenciales, se guardan automáticamente en su Gestor de credenciales para que no tenga que volver a introducirlas la próxima vez.

Instalación de Security Server en los hosts

Debe instalar Security Server en los hosts de la forma siguiente:

- En entornos VMware con vShield Endpoint, debe instalar al appliance diseñado para ello en cada host que vaya a protegerse. Todas las máquinas virtuales de un host se conectan automáticamente a la instancia Security Server instalada en ese host, a través de vShield Endpoint.
- En entornos Citrix, debe instalar Security Server en cada host que desee proteger con HVI a través de la tarea de instalación remota.
- En entornos Nutanix Prism Element, debe instalar el Servidor de seguridad en cada host mediante una tarea de instalación a distancia.
- En el resto de entornos, debe instalar Security Server en uno o más hosts para asignar el número de máquinas virtuales a proteger. Debe considerar el número de máquinas virtuales protegidas, recursos disponibles para Security Server en los hosts, además de la conectividad de red entre Security Server y las máquinas virtuales protegidas. El agente de seguridad instalado en las máquinas virtuales se conecta a Security Server sobre TCP/IP, utilizando la información configurada en la instalación o través de una política.

Si Control Center se integra con vCenter Server, XenServer y Nutanix Prism Element, puede implementar automáticamente Security Server en los hosts desde Control Center. También puede descargar los paquetes de Security Server para la instalación independiente desde Control Center.

Nota
Para entornos VMware con vShield Endpoint, puede desplegar Security Server en los hosts exclusivamente a través de tareas de instalación.

Instalación local

En todos los entornos virtualizados que no están integrados con Control Center, debe instalar Security Server en los hosts manualmente, usando un paquete de instalación. El paquete Security Server está disponible para su descarga desde Control Center en diferentes formatos, compatibles con las principales plataformas de virtualización.

Descarga de los paquetes de instalación de Security Server

Para descargar los paquetes de instalación de Security Server:

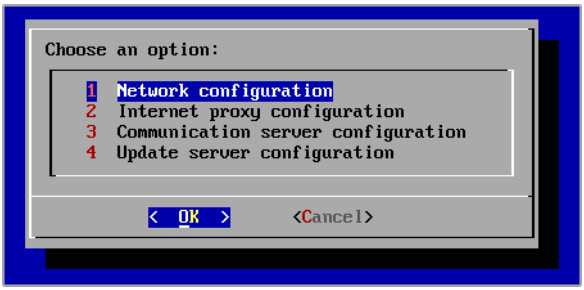
1. Vaya a la página **Red > Paquetes**.
2. Seleccione el paquete Security Server por defecto.
3. Haga clic en el botón **Descargar** en la zona superior de la tabla y seleccione el tipo de paquete desde el menú.
4. Guarde el paquete seleccionado en la ubicación deseada.

Implementación de los paquetes de instalación de Security Server

Una vez que tiene el paquete de instalación, impleméntelo en el host utilizando su herramienta de implementación de máquinas virtuales preferida.

Tras la implementación, configure el Security Server como se indica a continuación:

1. Acceda a la consola del appliance desde su herramienta de administración de la virtualización (por ejemplo, vSphere Client). Como alternativa, puede conectarse al appliance vía SSH.
2. Inicie sesión utilizando las credenciales por omisión.
   - Nombre de usuario: `root`
   - Contraseña: `sve`
3. Ejecute el comando `sva-setup`. Accederá a la interfaz de configuración del appliance.



Interfaz de configuración del Security Server (menú principal)

Para navegar por los menús y opciones, utilice las teclas de las flechas y el `Tabulador`. Para seleccionar una opción concreta, pulse `Intro`.

4. Configure los ajustes de la red.

   El Security Server utiliza el protocolo TCP/IP para comunicarse con los otros componentes de GravityZone. Puede configurar el appliance para que obtenga los ajustes de red automáticamente del servidor DHCP, o bien puede configurar los ajustes de red manualmente como se describe a continuación:

   a. Desde el menú principal, seleccione **Configuración de red**.

   b. Seleccione la interfaz de red.

   c. Seleccione el modo de configuración de IP:

      - **DHCP**, si desea que el Security Server obtenga automáticamente los ajustes de red del servidor DHCP.
      - **Estático**, si no hay servidor DHCP o si se ha reservado una IP para el appliance en el servidor DHCP. En este caso, debe configurar manualmente los ajustes de red.

        i. Introduzca el nombre de host, la dirección IP, la máscara de red, la puerta de enlace y los servidores DNS en los campos correspondientes.

        ii. Seleccione **Aceptar** para guardar los cambios.

Nota
Si está conectado al appliance por medio de un cliente SSH, al cambiar los ajustes de red se cerrará inmediatamente su sesión.

5. Configure los ajustes del proxy.

   Si se usa un servidor proxy en la red, debe proporcionar sus datos para que el Security Server pueda comunicarse con GravityZone Control Center.

   Nota
   Solo se admiten proxies con autenticación básica.

   a. En el menú principal, seleccione **Configuración del proxy de Internet**.
   b. Escriba el nombre de host, el nombre de usuario y el dominio en los campos correspondientes.
   c. Seleccione **Aceptar** para guardar los cambios.

6. Configure la dirección del Servidor de comunicaciones.
   a. En el menú principal, seleccione **Configuración del Servidor de comunicaciones**.
   b. Introduzca la dirección del Servidor de comunicaciones, incluyendo el número de puerto 8443, con el siguiente formato:

      ```
      https://IP-Servidor-comunicaciones:8443
      ```

      Como alternativa, puede utilizar el nombre de host del Servidor de comunicaciones en lugar de la dirección IP.
   c. Seleccione **Aceptar** para guardar los cambios.

Instalación remota

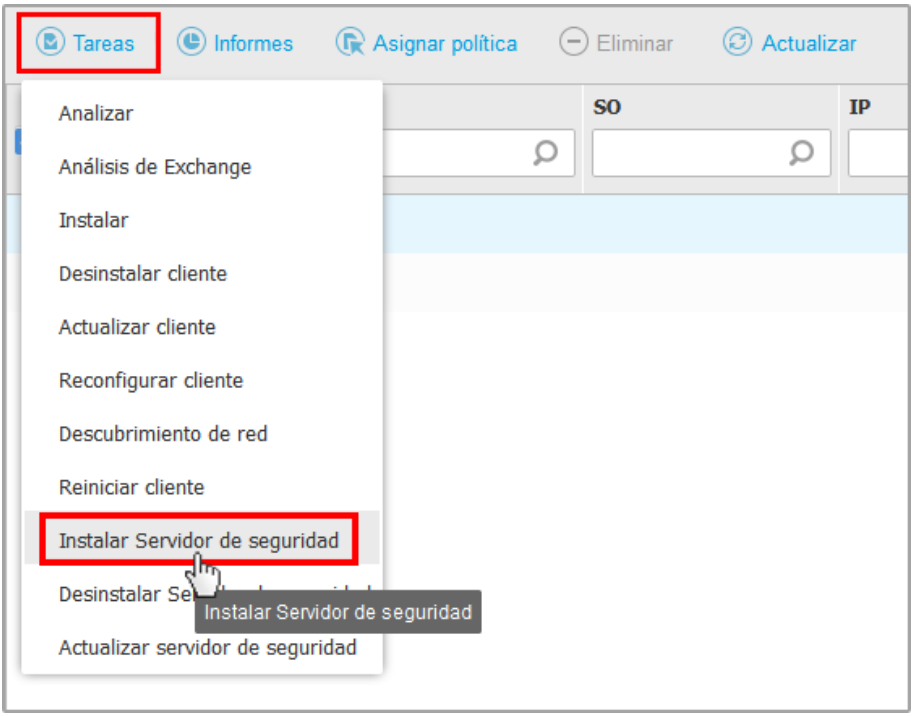
Control Center le permite instalar remotamente Security Server en los hosts visibles utilizando tareas de instalación.

Para instalar Security Server de forma remota en uno o varios hosts:

1. Diríjase a la página **Red**.
2. Seleccione **Máquinas virtuales** desde el selector de vistas.
3. Examine el inventario de VMware, Citrix o Nutanix y marque las casillas de selección correspondientes a los contenedores o hosts deseados (Nutanix Prism, vCenter Server, XenServer o centro de datos). Para una selección rápida, puede escoger directamente el contenedor raíz (inventario de VMware, Nutanix o Citrix). Podrá seleccionar hosts individualmente en el asistente de instalación.

Nota
No puede seleccionar los hosts de distintas carpetas.

4. Haga clic en el botón **Tareas** de la parte superior de la tabla y seleccione **Instalar Security Server** en el menú. Se muestra la ventana **Instalación de Security Server**.



Instalación de Security Server desde el menú Tareas

5. Seleccione los hosts en los que quiera instalar las instancias Security Server.
6. Elija los ajustes de configuración que quiera emplear.

Importante
Utilizar ajustes comunes para la implementación simultánea de instancias en múltiples Security Server requiere que los hosts compartan el mismo

almacenamiento, tengan sus direcciones IP asignadas por un servidor DHCP y formen parte de la misma red.

Si elige configurar cada Security Server de forma diferente, podrá definir los ajustes que desee para cada host en el siguiente paso del asistente. Los pasos descritos a continuación se aplican a cuando se utiliza la opción **Configurar cada Security Server**.

7. Haga clic en **Siguiente**.
8. Escriba un nombre descriptivo para Security Server.
9. Para entornos VMware, seleccione el contenedor en el que quiere incluir el Security Server desde el menú **Implementar contenedor**.
10. Seleccione el almacenamiento de destino.
11. Elija el tipo de provisión de disco. Se recomienda implementar el appliance usando aprovisionamiento con discos thick.

    Importante
    Si utiliza aprovisionamiento con discos thin y se queda sin espacio en disco en el datastore, el Security Server se detendrá y, en consecuencia, el host se quedará sin protección.

12. Configure la asignación de recursos de CPU y memoria basándose en el ratio de consolidación de la MV en el host. Escoja **Bajo**, **Medio** o **Alto** para cargar los ajustes de asignación de recursos recomendados o **Manual** para configurar la asignación de recursos manualmente.
13. Debe establecer una contraseña de administrador para la consola de Security Server. Establecer una contraseña administrativa anula la contraseña raíz predeterminada ("sve").
14. Establezca la zona horaria del appliance.
15. Seleccione el tipo de configuración de red para la red de Bitdefender. La dirección IP de Security Server no debe cambiarse a lo largo del tiempo, ya que los agentes de Linux la utilizan para comunicarse.

    Si escoge DHCP, asegúrese de configurar el servidor DHCP para que reserve una dirección IP para el appliance.

    Si escoge fija, debe introducir la información sobre la dirección IP, máscara de subred, puerta de enlace y DNS.

16. Seleccione la red vShield e introduzca las credenciales vShield. La etiqueta predeterminada para la red vShield es `vmservice-vshield-pg`.
17. Haga clic en **Guardar**.

Puede ver y administrar las tareas en la página **Red > Tareas**.

Nota
Para actualizar de VMware vShield a NSX, consulte este artículo de la base de conocimientos.

Importante
La instalación de Security Server en Nutanix a través de una tarea a distancia puede fallar si el cluster de Prism Element está registrado en Prism Central o por algún otro motivo. En estas situaciones, se recomienda realizar una implementación manual de Security Server. Para obtener más información, consulte este artículo de la base de conocimientos.

Instalación de Security Server para Amazon EC2

Puede usar Security Server para proteger sus instancias de Amazon EC2 de la siguiente manera:

- Configure el Security Server instalado en su red local para que se comunique con las instancias de Amazon EC2. Por lo tanto, podrá usar sus recursos locales, ya sean físicos o virtuales, para proteger también el inventario de Amazon EC2.
- Instale una o varias instancias de Security Server en su entorno Amazon EC2, en función de sus necesidades. En este caso, siga el procedimiento descrito en este artículo de la base de conocimientos.

  Importante
  - Para que funcione la comunicación entre las máquinas EC2 y las instancias de Security Server instaladas en su inventario de Amazon EC2, debe configurar correctamente sus conexiones Amazon VPC (Virtual Private Cloud) y Amazon VPN. Para más información, consulte la documentación de Amazon VPC.
  - Recomendamos instalar Security Server en la misma región de Amazon EC2 que las instancias que desee proteger.

El modo de análisis por defecto para las instancias de EC2 es Análisis local (todos los contenidos de seguridad se almacenan en el agente de seguridad instalado y el análisis se ejecuta localmente en la máquina). Si desea analizar sus instancias

de EC2 con un Security Server, deberá configurar en consecuencia el paquete de instalación del agente de seguridad y la política aplicada.

Instalación de Security Server para Microsoft Azure

Puede usar Security Server para proteger sus máquinas virtuales de Microsoft Azure de la siguiente manera:

- Configure el Security Server instalado en su red local para que se comunique con las máquinas virtuales de Microsoft Azure. Por lo tanto, podrá usar sus recursos locales, ya sean físicos o virtuales, para proteger también el inventario de Microsoft Azure.
- Instale una o varias instancias de Security Server en su entorno Microsoft Azure, en función de sus necesidades. En este caso, siga el procedimiento descrito en este artículo de la base de conocimientos.

Importante

- Para que funcione la comunicación entre las máquinas virtuales de Microsoft Azure y las instancias del Servidor de seguridad instaladas en su inventario de Microsoft Azure, debe configurar correctamente su red/subred virtual. Para obtener más información, consulte la documentación de la red virtual de Microsoft Azure.
- Recomendamos instalar Security Server en la misma región de Microsoft Azure que las máquinas virtuales que desee proteger.

El modo de análisis por defecto para las máquinas virtuales de Microsoft Azure es Análisis local (todos los contenidos de seguridad se almacenan en el agente de seguridad instalado y el análisis se ejecuta localmente en la máquina). Si desea analizar sus máquinas virtuales de Microsoft Azure con un Security Server, deberá configurar en consecuencia el paquete de instalación del agente de seguridad y la política aplicada.

5.3.2. Instalación de los agentes de seguridad

Para proteger sus endpoints físicos y virtuales, debe instalar un agente de seguridad en cada uno de ellos. Además de gestionar la protección del endpoint local, el agente de seguridad también se comunica con Control Center para recibir las órdenes del administrador y para comunicar los resultados de sus acciones.

Para más información sobre los agentes de seguridad disponibles, consulte "Agentes de seguridad" (p. 13).

En máquinas Windows y Linux, el agente de seguridad puede tener dos roles y es posible instalarlo de la siguiente manera:

1. Como un simple agente de seguridad para sus endpoints.
2. Como relay, actuando como agente de seguridad y también servidor de comunicaciones, de actualizaciones y proxy para otros endpoints de la red.

Puede instalar los agentes de seguridad en endpoints físicos y virtuales ejecutando los paquetes de instalación localmente o ejecutando las tareas de instalación remotamente desde Control Center.

Es muy importante leer y seguir cuidadosamente las instrucciones para prepararse para la instalación.

En el modo normal, los agentes de seguridad tienen una interfaz de usuario mínima. Sólo permite a los usuarios comprobar el estado de protección y ejecutar tareas de seguridad básicas (actualizaciones y análisis), sin permitir el acceso a la configuración.

Si el administrador de red lo habilita mediante el paquete de instalación y la política de seguridad, el agente de seguridad también se puede ejecutar en modo de Usuario avanzado en endpoints de Windows, lo que permite que el usuario del endpoint vea y modifique los ajustes de política. No obstante, el administrador de Control Center siempre puede controlar qué ajustes de política se aplican, imponiendo su criterio al modo de Usuario avanzado.

El idioma mostrado por la interfaz de usuario en los endpoints de Windows protegidos se define por defecto en el momento de la instalación en función del idioma de su cuenta de GravityZone.

En Mac, el idioma mostrado por la interfaz de usuario se define en el momento de la instalación en función del idioma del sistema operativo del endpoint. En Linux, el agente de seguridad no tiene una interfaz de usuario localizada.

Para instalar la interfaz de usuario en otro idioma en determinados endpoints de Windows, puede crear un paquete de instalación y establecer el idioma preferido en sus opciones de configuración. Esta opción no está disponible para endpoints Mac y Linux. Para obtener más información sobre la creación de paquetes de instalación, consulte "Crear paquetes de instalación" (p. 141).

Preparándose para la Instalación

Antes de la instalación, siga estos pasos preparatorios para asegurarse de que todo vaya bien:

1. Asegúrese de que los endpoints objetivo cumplen los requisitos mínimos del sistema. Para algunos endpoints, puede que necesite instalar el service pack del sistema operativo más reciente disponible o liberar espacio en disco. Configure una lista de endpoints que no cumplan los requisitos necesarios para que pueda excluirlos de la administración.
2. Desinstale (no vale simplemente inhabilitar) cualquier antimalware existente o software de seguridad de Internet de los endpoints objetivo. Ejecutar el agente de seguridad simultáneamente con otro software de seguridad en un endpoint puede afectar a su funcionamiento y causar serios problemas en el sistema.

   Muchos de los programas de seguridad incompatibles se detectan automáticamente y se eliminan durante la instalación.

   Para más información y para consultar la lista de software de seguridad detectado por Bitdefender Endpoint Security Tools para los sistemas operativos Windows actuales, consulte este artículo de la base de conocimientos.

   Importante
   Si desea implementar el agente de seguridad en un equipo con Bitdefender Antivirus for Mac 5.x, primero debe quitar manualmente este último. Para obtener una guía de los pasos a dar, consulte este artículo de la base de conocimientos.

3. La instalación requiere disponer de privilegios de administrador y acceso a Internet. Si los endpoints objetivo están en un dominio de Active Directory, debe usar las credenciales de administrador de dominio para la instalación remota. De no ser así, asegúrese de que tiene a mano las credenciales necesarias para todos los endpoints.
4. Los endpoints deben tener conexión de red con el appliance GravityZone.
5. Se recomienda utilizar una dirección IP fija para el servidor de relay. Si no establece una dirección IP fija, utilice el nombre de host de la máquina.
6. Para implementar el agente a través de un relay de Linux, deben cumplirse las siguientes condiciones adicionales:
   - El endpoint de relay debe tener instalado el paquete Samba (`smbclient`) versión 4.1.0 o superior y el comando/binario `net` para poder implementar agentes de Windows.

Nota
El comando/binario `net` viene generalmente con los paquetes samba-client o samba-common. En algunas distribuciones de Linux (como CentOS 7.4), el comando `net` solo se instala cuando se instala la suite completa de Samba (Common + Client + Server). Asegúrese de que su endpoint de relay disponga del comando `net`.

- Los endpoints de Windows objetivo deben tener habilitados el Recurso compartido de red y el Recurso compartido administrativo.
- Los endpoints objetivo de Linux y Mac deben tener SSH habilitado.

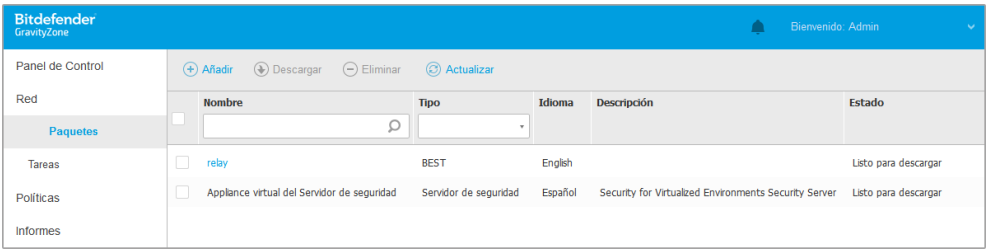
7. A partir de macOS High Sierra (10.13), después de instalar Endpoint Security for Mac de forma manual o remota, se solicita a los usuarios que aprueben las extensiones del kernel de Bitdefender en sus equipos. Mientras los usuarios no aprueben las extensiones del kernel de Bitdefender, no funcionarán algunas características de Endpoint Security for Mac. Para eliminar la intervención del usuario, puede aprobar previamente las extensiones del kernel de Bitdefender incluyéndolas en una lista blanca mediante una herramienta de administración de dispositivos móviles.
8. Al desplegar el agente en un inventario de Amazon EC2, configure los grupos de seguridad asociados con las instancias que desee proteger en el **Panel de control > Red y seguridad** de Amazon EC2 de la siguiente manera:
   - Para la instalación remota, permita el acceso SSH* desde la instancia de EC2.
   - Para la instalación local, permita el acceso SSH* y RDP (protocolo de escritorio remoto) en el equipo desde el que se conecta.

   * Para la instalación remota en instancias de Linux, debe permitir el inicio de sesión SSH usando nombre de usuario y contraseña.
9. Al implementar el agente en un inventario de Microsoft Azure:
   - La máquina virtual objetivo debe estar en la misma red virtual que el appliance GravityZone.
   - La máquina virtual objetivo debe estar en la misma red virtual que un relay, que se comunica con el appliance GravityZone cuando este último está en otra red.

Instalación local

Una forma de instalar el agente de seguridad en un endpoint es ejecutar un paquete de instalación localmente.

Puede crear y administrar paquetes de instalación en la página **Red > Paquetes**.



La página Paquetes

Una vez instalado el primer cliente, este se utilizará para detectar otros endpoints de la misma red, basándose en el mecanismo de Detección de redes. Para información detallada sobre la detección de redes, consulte "Cómo funciona la detección de red" (p. 159).

Para instalar el agente de seguridad localmente en un endpoint, siga estos pasos:

1. Cree un paquete de instalación según sus necesidades.

   Nota
   Este paso no es obligatorio si ya se ha creado un paquete de instalación para la red correspondiente a su cuenta.

2. Descargue el paquete de instalación en el endpoint objetivo.

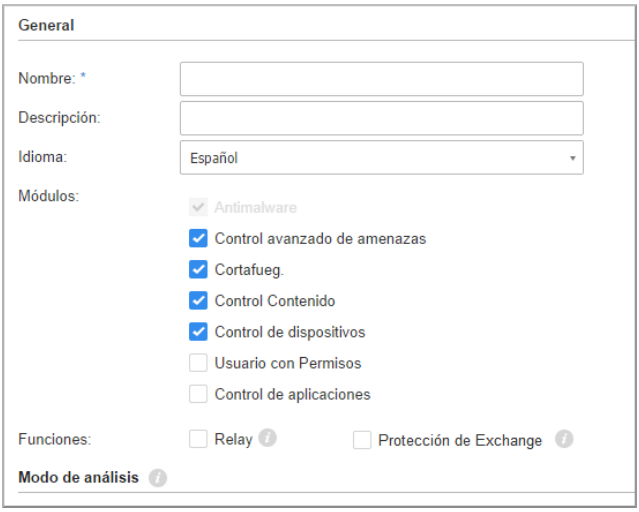
   Como alternativa, puede enviar por correo electrónico los enlaces de descarga del paquete de instalación a varios usuarios de su red.
3. Ejecute el paquete de instalación en el endpoint objetivo.

Crear paquetes de instalación

Para crear un paquete de instalación:

1. Conéctese e inicie sesión en Control Center.
2. Vaya a la página **Red > Paquetes**.

3. Haga clic en el botón ⊕ **Añadir** en la parte superior de la tabla. Aparecerá una nueva ventana de configuración.



Crear paquetes - Opciones

4. Escriba un nombre adecuado y una descripción para el paquete de instalación que quiere crear.
5. En el campo **Idioma**, seleccione el idioma deseado para la interfaz del cliente.

> **Nota**
> Esta opción solo está disponible para algunos sistemas operativos Windows.

6. Seleccione los módulos de protección que desea instalar.

> **Nota**
> Solo se instalarán los módulos soportados por cada sistema operativo. Para más información, diríjase a "Agentes de seguridad" (p. 13).

7. Seleccione el rol del endpoint objetivo:
   - **Relay**, para crear el paquete para un endpoint con rol de relay. Para más información, diríjase a "Relay" (p. 15)

- **Servidor de caché de Administración de parches**, para convertir al relay en un servidor interno de distribución de parches de software. Este rol se muestra cuando se selecciona el rol de relay. Para más información, diríjase a "Servidor de almacenamiento en caché de parches" (p. 15)
- **Protección de Exchange**, para instalar los módulos de protección para servidores de Microsoft Exchange, incluyendo antimalware, antispam, filtrado de contenidos y datos adjuntos para el tráfico de correo electrónico de Exchange y análisis antimalware bajo demanda de las bases de datos de Exchange. Para más información, diríjase a "Instalación de la Protección de Exchange" (p. 171).

8. **Eliminar productos de la competencia**. Se recomienda mantener marcada esta casilla de verificación para eliminar automáticamente cualquier software de seguridad incompatible mientras se instala el agente de Bitdefender en el endpoint. Si se desmarca esta opción, el agente de Bitdefender se instalará junto a la solución de seguridad existente. Más adelante, bajo su propia responsabilidad, puede eliminar manualmente la solución de seguridad instalada anteriormente.

   Importante
   Ejecutar el agente de Bitdefender simultáneamente con otro software de seguridad en un endpoint puede afectar a su funcionamiento y causar serios problemas en el sistema.

9. **Modo de análisis**. Elija la tecnología de análisis que mejor se adapte a su entorno de red y a los recursos de sus endpoints. Puede definir el modo de análisis eligiendo uno de los siguientes tipos:
   - **Automática**. En este caso, el agente de seguridad detectará automáticamente la configuración del endpoint y adaptará la tecnología de análisis en consecuencia:
     - Análisis centralizado en nube pública o privada (con Security Server) con reserva en Análisis híbrido (motores ligeros) para equipos físicos con hardware de bajo rendimiento y para máquinas virtuales. Este caso requiere al menos un Security Server implementado en la red.
     - Análisis local (con motores completos) para equipos físicos con hardware de alto rendimiento.

– Análisis local para instancias de EC2 y máquinas virtuales de Microsoft Azure.

> **Nota**
> Se consideran equipos de bajo rendimiento aquellos que tienen una frecuencia de CPU inferior a 1,5 GHz o menos de 1 GB de memoria RAM.

- **Personal**. En este caso, puede configurar el modo de análisis escogiendo entre diversas tecnologías de análisis para máquinas físicas y virtuales:
  – Análisis centralizado en nube pública o privada (con Security Server), que puede contar con reserva* en Análisis local (con motores completos) o en Análisis híbrido (con motores ligeros)
  – Análisis híbrido (con motores ligeros)
  – Análisis local (con motores completos)

  El modo de análisis por defecto para las instancias de EC2 es Análisis local (todos los contenidos de seguridad se almacenan en el agente de seguridad instalado y el análisis se ejecuta localmente en la máquina). Si desea analizar sus instancias de EC2 con un Security Server, deberá configurar en consecuencia el paquete de instalación del agente de seguridad y la política aplicada.

  El modo de análisis por defecto para las máquinas virtuales de Microsoft Azure es Análisis local (todos los contenidos de seguridad se almacenan en el agente de seguridad instalado y el análisis se ejecuta localmente en la máquina). Si desea analizar sus máquinas virtuales de Microsoft Azure con un Security Server, deberá configurar en consecuencia el paquete de instalación del agente de seguridad y la política aplicada.

  * Al utilizar análisis con motores duales, cuando el primer motor no esté disponible, se utilizará el motor de reserva. El consumo de recursos y la utilización de la red dependen de los motores empleados.

  Para obtener más información con respecto a las tecnologías de análisis disponibles, consulte"Motores de análisis" (p. 3)

10. **Implementar endpoint con vShield cuando se detecta un entorno VMware integrado con vShield**. Esta opción se puede utilizar cuando se implementa el paquete de instalación en una máquina virtual de un entorno VMware integrado

con vShield. En este caso, VMware vShield Endpoint se instalará en el equipo objetivo en lugar del agente de seguridad de Bitdefender.

Importante
Esta opción es solo para las implementaciones remotas, no para instalaciones locales. Cuando realice la instalación localmente en un entorno VMware integrado con vShield, tiene la opción de descargar el paquete integrado con vShield.

11. Al personalizar los motores de análisis para el uso de nube pública o privada (Security Server), se le solicita seleccionar los Security Server instalados localmente que desea usar y configurar su prioridad en la sección **Asignación de Security Server**:
    a. Haga clic en la lista Security Server en el encabezado de la tabla. Se mostrará la lista de Security Server detectados.
    b. Seleccione una entidad.
    c. Haga clic en el botón ⊕ **Añadir** del encabezado de la columna **Acciones**.
    El Security Server se añade a la lista.
    d. Siga los mismos pasos para añadir varios servidores de seguridad, si existiesen. En tal caso, puede configurar sus prioridades mediante las flechas ⌃ arriba y ⌄ abajo disponibles a la derecha de cada entidad. Cuando no esté disponible el primer Security Server, se utilizará el siguiente y así sucesivamente.
    e. Para eliminar una entidad de la lista, haga clic en el botón ⊗ **Borrar** correspondiente de la parte superior de la tabla.

    Puede optar por cifrar la conexión con el Security Server seleccionando la opción **Usar SSL**.
12. **Varios**. Puede configurar las siguientes opciones para los diversos tipos de archivos de los endpoints objetivo:
    - **Enviar volcados de errores**. Seleccione esta opción de forma que, si el agente de seguridad se bloquea, los archivos de volcado de memoria se envíen a los laboratorios de Bitdefender para su análisis. Los volcados de errores ayudarán a nuestros ingenieros a descubrir qué causó el problema y así evitar que éste vuelva a ocurrir. No sé enviará información personal.
    - **Enviar archivos en cuarentena a Bitdefender Labs cada (horas)**. Por omisión, los archivos de cuarentena se envían automáticamente al laboratorio de

Bitdefender cada hora. Puede modificar el intervalo de tiempo en el que se envían los archivos en cuarentena. Los investigadores de malware de Bitdefender analizarán los archivos de muestra. Si se confirma la presencia de malware, se publica una firma para permitir eliminar el malware.

- **Enviar ejecutables sospechosos a Bitdefender**. Seleccione esta opción para que los archivos que no parecen dignos de confianza o que presentan un comportamiento sospechoso se envíen a los laboratorios de Bitdefender para su análisis.

13. Seleccione **Analizar antes de la instalación** si quiere asegurarse de que las máquinas están limpias antes de instalar el cliente en ellas. Se ejecutará un análisis rápido en la nube de las máquinas objetivo correspondientes antes de empezar la instalación.
14. Bitdefender Endpoint Security Tools se instala en el directorio de instalación por defecto. Seleccione **Usar ruta de instalación personalizada** si desea instalar el agente Bitdefender en una ubicación diferente. Si la carpeta especificada no existe, se creará durante la instalación.

    - En Windows, la ruta por defecto es `C:\Archivos de programa\`. Para instalar Bitdefender Endpoint Security Tools en una ubicación personalizada, siga las convenciones de Windows al introducir la ruta. Por ejemplo, `D:\carpeta`.

    - En Linux, Bitdefender Endpoint Security Tools se instala por defecto en la carpeta `/opt`. Para instalar el agente de Bitdefender en una ubicación personalizada, siga las convenciones de Linux al introducir la ruta. Por ejemplo, `/carpeta`.

      Bitdefender Endpoint Security Tools no admite la instalación en las siguientes rutas personalizadas:
      - Cualquier ruta que no comience con una barra inclinada (/). La única excepción es la ubicación de Windows `%PROGRAMFILES%`, que el agente de seguridad interpreta como la carpeta por defecto de Linux `/opt`.
      - Cualquier ruta que esté en `/tmp` o `/proc`.
      - Cualquier ruta que contenga los siguientes caracteres especiales: `$, !, *, ?, ", ', `, \, (,), [,], {, }`.
      - El especificador de `systemd` (%).

En Linux, la instalación en una ruta personalizada requiere glibc 2.21 o superior.

Importante
Cuando utilice una ruta personalizada, asegúrese de tener el paquete de instalación adecuado para cada sistema operativo.

15. Si lo desea, puede establecer una contraseña para evitar que los usuarios desinstalen la protección. Seleccione **Contraseña de desinstalación** e introduzca la contraseña deseada en los campos correspondientes.
16. Si los endpoints objetivo se encuentran en el inventario de red de **Grupos personalizados**, puede elegir trasladarlos a una carpeta especificada inmediatamente después de haber finalizado la implementación de agentes de seguridad.

    Seleccione **Usar carpeta personalizada** y elija una carpeta en la tabla correspondiente.
17. En la sección **Implementador**, seleccione la entidad a la que se conectarán los endpoints objetivo para instalar y actualizar el cliente:
    - **Appliance GravityZone**, cuando los endpoints se conectan directamente al appliance GravityZone.

      Para este caso, también puede definir:

      – Un Servidor de comunicaciones personalizado introduciendo su IP o nombre de host, de ser necesario.

      – Ajustes de proxy, si los endpoints objetivo se comunican con el appliance GravityZone mediante un proxy. En este caso, seleccione **Utilizar un proxy para la comunicación** e introduzca los ajustes necesarios del proxy en los campos que figuran a continuación.
    - **Endpoint Security Relay**, si desea conectar los endpoints a un cliente de relay instalado en su red. Todas las máquinas con rol de relay detectadas en su red figurarán en la tabla que se muestra a continuación. Seleccione la máquina de relay que desee. Los endpoints conectados se comunicarán con Control Center solo mediante el relay especificado.

      Importante
      El puerto 7074 debe estar abierto para que funcione la implementación mediante Bitdefender Endpoint Security Tools Relay.

18. Haga clic en **Guardar**.

El nuevo paquete creado se añadirá a la lista de paquetes.

Nota
Los ajustes configurados en un paquete de instalación se aplicarán a los endpoints inmediatamente después de la instalación. En cuanto se aplique una política al cliente, se harán cumplir los ajustes configurados en la política en sustitución de determinados ajustes del paquete de instalación (como por ejemplo, servidores de comunicaciones o ajustes de proxy).

Descargar los paquetes de instalación

Para descargar los paquetes de instalación de los agentes de seguridad:

1. Inicie sesión en Control Center desde el endpoint en el que desee instalar la protección.
2. Vaya a la página **Red > Paquetes**.
3. Seleccione el paquete de instalación que desee descargar.
4. Haga clic en el botón **Descargar** en la zona superior de la tabla y seleccione el tipo de instalador que quiera utilizar. Hay disponibles dos tipos de archivos de instalación:
   - **Downloader**. El downloader primero descarga el kit de instalación completo desde los servidores de la nube de Bitdefender y luego inicia la instalación. Es pequeño en tamaño y puede ejecutarse tanto en sistemas de 32-bit como de 64-bit (lo que lo hace más fácil de distribuir). Por otro lado, requiere una conexión a Internet activa.
   - **Kit completo**. Los kits de instalación completos tienen mayor tamaño y han de ejecutarse en el tipo concreto de sistema operativo.

     El kit completo se utiliza para instalar la protección en los endpoints sin conexión a Internet o con conexiones lentas. Descargue este archivo en un endpoint conectado a Internet y distribúyalo a otros endpoints usando un medio de almacenamiento externo o compartiéndolo en la red.

     Nota
     Versiones de kit completo disponibles:
     - **SO Windows:** sistemas de 32 bits y 64 bits
     - **SO Linux:** sistemas de 32 bits y 64 bits

– **macOS:** solo sistemas de 64 bits

Asegúrese de usar la versión correcta para el sistema donde instala.

5. Guarde el archivo en el endpoint.

Aviso

- No hay que cambiar el nombre del ejecutable de descarga, pues de lo contrario no podrá descargar los archivos de instalación del servidor de Bitdefender.

6. Además, si ha elegido el Descargador, puede crear un paquete MSI para los endpoints de Windows. Para más información, consulte este artículo de la base de conocimiento.

Enviar enlaces de descarga de paquetes de instalación por correo electrónico

Es posible que tenga que informar rápidamente a otros usuarios de que hay un paquete de instalación listo para descargar. En tal caso, siga los pasos descritos a continuación:

1. Vaya a la página **Red > Paquetes**.
2. Seleccione el paquete de instalación que desee.
3. Haga clic en el botón **Enviar enlaces de descarga** en la zona superior de la tabla. Aparecerá una nueva ventana de configuración.
4. Introduzca la dirección de correo electrónico de cada usuario que desea que reciba el enlace de descarga del paquete de instalación. Pulse `Intro` tras cada dirección.

   Asegúrese de la validez de todas las direcciones de correo electrónico que introduzca.
5. Si desea ver los enlaces de descarga antes de enviarlos por correo electrónico, haga clic en el botón **Enlaces de instalación**.
6. Haga clic en **Enviar**. Se envía un correo electrónico que contiene el enlace de instalación a cada dirección de correo electrónico especificada.

Ejecutar los paquetes de instalación

Para que funcione la instalación, el paquete de instalación debe ejecutarse utilizando privilegios de administrador.

El paquete se instala de manera diferente en cada sistema operativo como se describe a continuación:

- En los sistemas operativos Windows y macOS:
  1. En el endpoint objetivo, descargue el archivo de instalación de Control Center o cópielo desde un recurso compartido de red.
  2. Si ha descargado el kit completo, extraiga los archivos del archivo comprimido.
  3. Ejecute el archivo ejecutable.
  4. Siga las instrucciones que aparecen en la pantalla.

  Nota
  En macOS, después de instalar Endpoint Security for Mac, se solicita a los usuarios que aprueben las extensiones del kernel de Bitdefender en sus equipos. Mientras los usuarios no aprueben las extensiones del kernel de Bitdefender, no funcionarán algunas características del agente de seguridad. Para más información, consulte este artículo de la base de conocimientos.

- En sistemas operativos Linux:
  1. Conéctese e inicie sesión en Control Center.
  2. Descargue o copie el archivo de instalación en el endpoint objetivo.
  3. Si ha descargado el kit completo, extraiga los archivos del archivo comprimido.
  4. Dótese de privilegios de root ejecutando el comando `sudo su`.
  5. Cambie los permisos del archivo de instalación para poder ejecutarlo:

     ```
     # chmod +x installer
     ```

  6. Ejecutar los archivos de instalación:

     ```
     # ./installer
     ```

  7. Para comprobar que el agente se ha instalado en el endpoint, ejecute este comando:

```
$ service bd status
```

Una vez instalado el agente de seguridad, el endpoint se mostrará como administrado en Control Center (página **Red**) en unos minutos.

Importante
Si utiliza la administración de VMware Horizon View Persona, se recomienda configurar la política de grupo de Active Directory para excluir los siguientes procesos de Bitdefender (sin la ruta completa):

- `bdredline.exe`
- `epag.exe`
- `epconsole.exe`
- `epintegrationservice.exe`
- `epprotectedservice.exe`
- `epsecurityservice.exe`
- `epupdateservice.exe`
- `epupdateserver.exe`

Estas exclusiones deben aplicarse siempre que el agente de seguridad se ejecute en el endpoint. Para más información, consulte esta página de la documentación de VMware Horizon.

Instalación remota

Control Center le permite instalar el agente de seguridad remotamente en endpoints de entornos integrados con Control Center y en otros endpoints detectados en la red mediante tareas de instalación. En entornos VMware, la instalación a distancia se basa en las VMware Tools, mientras que en los entornos Citrix XenServer y Nutanix Prism Element, se basa en los recursos compartidos administrativos de Windows y SSH.

Una vez que se instala el agente de seguridad en un endpoint, pueden tardarse unos minutos en que el resto de endpoints de la red aparezcan en Control Center.

Bitdefender Endpoint Security Tools incluye un mecanismo de detección de redes automático que permite detectar los endpoints que no estén en Active Directory. Los endpoints detectados se muestran como **no administrados** en la página **Red**, de la vista **Equipos**, bajo **Grupos personalizados**. Control Center elimina automáticamente los endpoints de Active Directory de la lista de endpoints detectados.

Para activar la detección de redes, primero debe tener instalado Bitdefender Endpoint Security Tools en al menos un endpoint de la red. Este endpoint se utilizará para analizar la red e instalar Bitdefender Endpoint Security Tools en los endpoints desprotegidos.

Para información detallada sobre la detección de redes, consulte "Cómo funciona la detección de red" (p. 159).

Requisitos de la instalación remota

Para que funcione la instalación remota:

- Para Windows:
  - Debe estar habilitado el recurso compartido administrativo `admin$`. Configure todas las estaciones de trabajo objetivo para que no utilicen el uso compartido de archivos avanzado.
  - Configure el Control de cuentas de usuario (UAC) según el sistema operativo que se ejecute en los endpoints objetivo. Si los endpoints están en un dominio de Active Directory, puede utilizar una política de grupo para configurar el Control de cuentas de usuario. Para más información, consulte este artículo de la base de conocimientos.
  - Inhabilite Windows Firewall o configúrelo para permitir el tráfico a través del protocolo Compartir archivos e impresoras.

    Nota
    La implementación remota solo funciona en los sistemas operativos modernos, a partir de Windows 7/Windows Server 2008 R2, para los cuales Bitdefender brinda soporte total. Para más información, diríjase a "Sistemas operativos soportados" (p. 30).

- En Linux, debe habilitarse SSH.
- En macOS deben estar habilitados el inicio de sesión remoto y el uso compartido de archivos.

Ejecución de tareas de instalación remota

Para ejecutar una tarea de instalación remota:

1. Conéctese e inicie sesión en Control Center.
2. Diríjase a la página **Red**.

3. Elija **Equipos y máquinas virtuales** en el selector de vistas.
4. Seleccione el grupo deseado desde el panel lateral izquierdo. Las entidades contenidas en el grupo seleccionado se muestran en la tabla del panel lateral derecho.

> **Nota**
> Opcionalmente, puede aplicar filtros para mostrar únicamente los endpoints no administrados. Haga clic en el menú **Filtros** y seleccione las siguientes opciones: **No administrados** de la pestaña **Seguridad** y **Todos los elementos recursivamente** de la pestaña **Profundidad**.

5. Seleccione las entidades (endpoints o grupos de endpoints) en las que desee instalar la protección.
6. Haga clic en el botón **Tareas** de la zona superior de la tabla y seleccione **Instalar**.

   El asistente de **Instalar cliente** se está mostrando.

Instalación de Bitdefender Endpoint Security Tools desde el menú Tareas

7. En la sección **Opciones**, configure el momento de la instalación:
   - **Ahora**, para poner en marcha la implementación de inmediato.
   - **Programado**, para configurar el intervalo de recurrencia de la implementación. En este caso, seleccione el intervalo de tiempo que desee (cada hora, a diario o semanalmente) y configúrelo según sus necesidades.

Nota
Por ejemplo, cuando hay que realizar determinadas operaciones en el equipo objetivo antes de instalar el cliente (como la desinstalación de otros programas y el reinicio del sistema operativo), puede programar la tarea de implementación para que se ejecute cada 2 horas. La tarea se lanzará en los equipos objetivo cada 2 horas hasta que culmine correctamente.

8. Si quiere que los endpoints objetivo se reinicien automáticamente para completar la instalación, seleccione **Reiniciar automáticamente (si es necesario)**.
9. En la sección **Administrador de credenciales**, especifique las credenciales administrativas necesarias para la autenticación remota en los endpoints objetivo. Puede añadir las credenciales escribiendo el usuario y contraseña para cada sistema operativo objetivo.

Importante
Para estaciones Windows 8.1, debe proporcionar las credenciales de la cuenta de administrador integrada o de una cuenta de administrador de dominio. Para obtener más información, consulte este artículo de la base de conocimientos.

Para añadir las credenciales del sistema operativo requeridas:

a. Introduzca el nombre de usuario y contraseña de una cuenta de administrador en los campos correspondientes del encabezado de la tabla.

Si los equipos están en un dominio, es suficiente con introducir las credenciales del administrador del dominio.

Utilice las normas de Windows cuando introduzca el nombre de una cuenta de usuario:

- Para las máquinas de Active Directory, utilice estas sintaxis: `usuario@dominio.com` y `dominio\usuario`. Para asegurarse de que las credenciales introducidas funcionarán, añádalas de ambas maneras (`nombredeusuario@dominio.com` y `dominio\nombredeusuario`).
- Para las máquinas del grupo de trabajo es suficiente con introducir solo el nombre de usuario, sin el nombre del grupo de trabajo.

Opcionalmente puede añadir una descripción que le ayudará a identificar más fácilmente cada cuenta.

b. Haga clic en el botón ⊕ **Añadir**. La cuenta se añade a la lista de credenciales.

Nota
Las credenciales especificadas se guardan automáticamente en su Gestor de credenciales para que no tenga que volver a introducirlas la próxima vez. Para acceder al Gestor de credenciales, señale su nombre de usuario en la esquina superior derecha de la consola.

Importante
Si las credenciales proporcionadas no son válidas, la implementación del cliente fallará en los endpoints correspondientes. Asegúrese de actualizar las credenciales del SO introducidas en el Gestor de credenciales cuando éstas cambien en los endpoints objetivo.

10. Marque las casillas de verificación correspondientes a las cuentas que desee usar.

Nota
Se mostrará un mensaje de advertencia si todavía no ha seleccionado credenciales. Este paso es obligatorio para instalar de forma remota el agente de seguridad en los endpoints.

11. En la sección **Implementador**, seleccione la entidad a la que se conectarán los endpoints objetivo para instalar y actualizar el cliente:
    - **Appliance GravityZone**, cuando los endpoints se conectan directamente al appliance GravityZone.

      En este caso, también puede definir:

      – Un Servidor de comunicaciones personalizado introduciendo su IP o nombre de host, de ser necesario.

      – Ajustes de proxy, si los endpoints objetivo se comunican con el appliance GravityZone mediante un proxy. En este caso, seleccione **Utilizar un proxy para la comunicación** e introduzca los ajustes necesarios del proxy en los campos que figuran a continuación.
    - **Endpoint Security Relay**, si desea conectar los endpoints a un cliente de relay instalado en su red. Todas las máquinas con rol de relay detectadas en su red figurarán en la tabla que se muestra a continuación. Seleccione la máquina de relay que desee. Los endpoints conectados se comunicarán con Control Center solo mediante el relay especificado.

Importante
El puerto 7074 debe estar abierto para que funcione la implementación mediante el agente de relay.

12. Utilice la sección **Objetivos adicionales** si quiere implementar el cliente en equipos concretos de su red que no se muestren en el inventario de red. Despliegue la sección e introduzca las direcciones IP o los nombres de host de esas máquinas en el campo correspondiente, separadas por una coma. Puede añadir tantas IPs como necesite.
13. Tiene que seleccionar un paquete de instalación para la implementación actual. Haga clic en la lista **Usar paquete** y seleccione el paquete de instalación que desee. Aquí puede encontrar todos los paquetes de instalación creados con anterioridad para su cuenta y también el paquete de instalación por defecto disponible con Control Center.
14. Si es necesario, puede modificar algunos de los ajustes del paquete de instalación seleccionado haciendo clic en el botón **Personalizar** junto al campo **Usar paquete**.

    Abajo aparecerán los ajustes del paquete de instalación y puede hacer los cambios que precise. Para más información sobre la modificación de paquetes de instalación, consulte "Crear paquetes de instalación" (p. 141).

    Si desea guardar las modificaciones como un paquete nuevo, seleccione la opción **Guardar como paquete**, situada en la parte inferior de la lista de ajustes de paquetes, e introduzca un nombre para el nuevo paquete de instalación.
15. Haga clic en **Guardar**. Aparecerá un mensaje de confirmación.

Puede ver y administrar las tareas en la página **Red > Tareas**.

Importante
Si utiliza la administración de VMware Horizon View Persona, se recomienda configurar la política de grupo de Active Directory para excluir los siguientes procesos de Bitdefender (sin la ruta completa):

- `bdredline.exe`
- `epag.exe`
- `epconsole.exe`
- `epintegrationservice.exe`
- `epprotectedservice.exe`
- `epsecurityservice.exe`
- `epupdateservice.exe`
- `epupdateserver.exe`

Estas exclusiones deben aplicarse siempre que el agente de seguridad se ejecute en el endpoint. Para más información, consulte esta página de la documentación de VMware Horizon.

Preparación de sistemas Linux para el análisis on-access

Bitdefender Endpoint Security Tools for Linux incluye posibilidades de análisis on-access que funcionan con determinadas distribuciones Linux y versiones del kernel. Para más información, consulte los requisitos del sistema.

A continuación aprenderá a compilar manualmente el módulo DazukoFS.

Compilación manual del módulo DazukoFS

Siga los siguientes pasos para compilar DazukoFS para la versión del kernel del sistema y luego cargar el módulo:

1. Descargue las cabeceras del kernel apropiadas.
   - En sistemas **Ubuntu**, ejecute este comando:

     ```
     $ sudo apt-get install linux-headers-`uname -r`
     ```

   - En sistemas **RHEL/CentOS**, ejecute este comando:

     ```
     $ sudo yum install kernel-devel kernel-headers-`uname -r`
     ```

2. En sistemas **Ubuntu**, necesita `build-essential`:

```
$ sudo apt-get install build-essential
```

3. Copie y extraiga el código fuente de DazukoFS en el directorio que prefiera:

```
# 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. Compile el módulo:

```
# make
```

5. Instale y cargue el módulo:

```
# make dazukofs_install
```

Requisitos para la utilización del análisis on-access con DazukoFS

Para que el análisis on-access funcione con DazukoFS, se deben cumplir una serie de condiciones. Compruebe si alguna de las afirmaciones que figuran a continuación corresponde a su sistema Linux y siga las instrucciones para evitar problemas.

- La política SELinux debe estar desactivada o configurada como **Tolerante**. Para consultar y ajustar la opción de política SELinux, edite el archivo `/etc/selinux/config`.
- Bitdefender Endpoint Security Tools es compatible exclusivamente con la versión DazukoFS incluida en el paquete de instalación. Si DazukoFS ya está instalado en el sistema, desinstálelo antes de instalar Bitdefender Endpoint Security Tools.
- DazukoFS es compatible con ciertas versiones del kernel. Si el paquete DazukoFS incluido con Bitdefender Endpoint Security Tools no es compatible

con la versión del kernel del sistema, el módulo dará error al cargarse. En dicho caso, puede actualizar el kernel a la versión soportada o recompilar el módulo DazukoFS para su versión del kernel. Puede encontrar el paquete DazukoFS en el directorio de instalación de Bitdefender Endpoint Security Tools:

`/opt/BitDefender/share/modules/dazukofs/dazukofs-modules.tar.gz`

- Al compartir archivos a través de servidores dedicados como NFS, UNFSv3 o Samba, tiene que iniciar los servicios en el siguiente orden:
  1. Activar el análisis on-access mediante política desde Control Center.

     Para más información, consulte la Guía del administrador de GravityZone.
  2. Inicie el servicio de uso compartido de red.

     Para NFS:

     ```
     # service nfs start
     ```

     Para UNFSv3:

     ```
     # service unfs3 start
     ```

     Para Samba:

     ```
     # service smbd start
     ```

Importante
Para el servicio NFS, DazukoFS solo es compatible con el Servidor de usuarios NFS.

Cómo funciona la detección de red

Además de la integración con Active Directory, GravityZone también incluye un mecanismo automático de detección de redes pensado para detectar los equipos del grupo de trabajo.

GravityZone se basa en el servicio **Microsoft Computer Browser** y en la herramienta **NBTscan** para realizar la detección de redes.

El servicio Computer Browser es una tecnología de red utilizada por los equipos basados en Windows para mantener listas actualizadas de dominios, grupos de trabajo y los equipos en ellos, y para suministrar estas listas a equipos cliente que lo soliciten. Los equipos detectados en la red por el servicio Computer Browser pueden visualizarse ejecutando el comando de **net view** en una ventana de símbolo del sistema.

El comando Net view

La herramienta NBTscan analiza las redes de equipos con NetBIOS. Consulta a todos los endpoints de la red y recupera información como la dirección IP, el nombre NetBIOS del equipo y la dirección MAC.

Para activar la detección automática de red, primero debe tener instalado Bitdefender Endpoint Security Tools Relay en al menos un equipo de la red. Este equipo se utilizará para analizar la red.

Importante

Control Center no utiliza la información de red de Active Directory o de la característica de mapa de red. El mapa de red se basa en una tecnología de detección de red diferente: el protocolo Link Layer Topology Discovery (LLTD).

Control Center no está directamente implicado en la operativa del servicio Computer Browser. Bitdefender Endpoint Security Tools solo consulta al servicio Computer Browser respecto a la lista de estaciones de trabajo y servidores visible actualmente en la red (conocida como lista de examen) y luego la envía a Control Center. Control Center procesa la lista de examen, añadiendo nuevos equipos detectados a su lista de **Equipos no administrados**. Los equipos anteriormente detectados no se borran después de una nueva consulta de detección de red, así que deberá excluir y borrar manualmente los equipos que ya no estén en la red.

La consulta inicial de la lista de examen la lleva a acabo el primer Bitdefender Endpoint Security Tools instalado en la red.

- Si el relay está instalado en un equipo de un grupo de trabajo, solo se verán en Control Center los equipos de ese grupo de trabajo.
- Si el relay está instalado en un equipo de un dominio, solo se verán en Control Center los equipos de ese dominio. Los equipos de otros dominios pueden detectarse si hay una relación de confianza con el dominio donde está instalado el relay.

Las consultas posteriores sobre detección de red se realizan regularmente cada hora. Para cada nueva consulta, Control Center divide el espacio de equipos administrados en áreas de visibilidad y luego designa un relay en cada área donde realizar la tarea. Un área de visibilidad es un grupo de equipos que se detectan entre ellos. Normalmente, un área de visibilidad se define por un grupo de trabajo o dominio, pero esto depende de la topología de la red y su configuración. En algunos casos, un área de visibilidad puede consistir en múltiples dominios y grupos de trabajo.

Si un relay seleccionado falla al realizar la consulta, Control Center espera a la siguiente consulta programada, sin escoger otro relay para intentarlo de nuevo.

Para una visibilidad de toda la red, el relay debe estar instalado en al menos un equipo de cada grupo de trabajo o dominio de su red. Lo ideal sería que Bitdefender Endpoint Security Tools estuviera instalado en al menos un equipo en cada subred.

Más sobre el servicio Microsoft Computer Browser

Datos sobre el servicio Computer Browser:

- Funciona independientemente de Active Directory.
- Funciona exclusivamente en redes IPv4 y opera independientemente dentro de los límites de un grupo LAN (grupo de trabajo o dominio). Se compila y mantiene una lista de examen para cada grupo LAN.
- Normalmente utiliza transmisiones del servidor sin conexión para comunicarse entre nodos.
- Utiliza NetBIOS en TCP/IP (NetBT).
- Requiere resolución de nombre de NetBIOS. Se recomienda tener una infraestructura de Servicio de Windows de nombre de Internet (WINS) funcionando en la red.
- No está habilitado por omisión en Windows Server 2008 y 2008 R2.

Para información detallada sobre el servicio Computer Browser, compruebe la Referencia técnica del servicio de navegador del equipo en Microsoft Technet.

Requisitos de descubrimiento de red

Para detectar satisfactoriamente todos los equipos (servidores y estaciones de trabajo) que se administrarán desde Control Center, se necesita lo siguiente:

- Los equipos deben estar unidos a un grupo de trabajo o dominio y conectados a través de una red local IPv4. El servicio Computer Browser no funciona en redes IPv6.
- Varios equipos en cada grupo LAN (grupo de trabajo o dominio) deben ejecutar el servicio Computer Browser. Los controladores de dominio primario también deben ejecutar el servicio.
- Las NetBIOS en TCP/IP (NetBT) deben estar habilitadas en los equipos. El cortafuegos local debe permitir el tráfico NetBT.
- Si utiliza un relay de Linux para detectar otros endpoints de Linux o Mac, debe instalar Samba en los endpoints objetivo, o incorporarlos a Active Directory y utilizar DHCP. De esta forma, NetBIOS se configurará automáticamente para ellos.
- La compartición de archivos debe estar habilitada en los equipos. El cortafuegos local debe permitir la compartición de archivos.
- Hay que establecer una infraestructura de Windows Internet Naming Service (WINS) que funcione correctamente.
- La detección de red ha de estar activada (**Panel de control > Centro de redes y recursos compartidos > Cambiar ajustes de compartición avanzados**).

  Para habilitar esta característica, han de iniciarse los siguientes servicios:
  - Cliente DNS
  - Publicación de recurso de detección de función
  - Descubrimiento de SSDP
  - Host de dispositivo UPnP
- En entornos con múltiples dominios, se recomienda establecer relaciones de confianza entre dominios de manera que los equipos puedan acceder a las listas de examen de otros dominios.

Los equipos desde los cuales Bitdefender Endpoint Security Tools accede al servicio Computer Browser deben poder resolver nombres NetBIOS.

Nota
El mecanismo de detección de redes funciona en todos los sistemas operativos soportados, incluyendo las versiones de Windows Embedded, siempre que se cumplan los requisitos.

5.4. Instalar Sandbox Analyzer On-Premises

Para asegurar que la instalación se realiza de forma correcta, siga estos pasos:

1. Preparándose para la instalación
2. Implementar el appliance virtual Sandbox Analyzer
3. Implementar el Network Security Virtual Appliance

5.4.1. Preparándose para la instalación

Antes de instalar Sandbox Analyzer On-Premises, asegúrese de lo siguiente:

- El hipervisor VMware ESXi está instalado y configurado. Para obtener más información, consulte la documentación de la Instalación y configuración de vSphere, sección 2: "Instalación y configuración de ESXi".
- El appliance virtual de Bitdefender GravityZone está implementado y configurado.

Nota
En cuanto al hipervisor VMware ESXi, asegúrese de lo siguiente:

- La versión de ESXi es la 6.5 o posterior.
- La versión del datastore de VMFS es la 5.
- SSH está habilitado en la **Política de Inicio** con la configuración **Iniciar y parar con el host**.
- El servicio NTP está activo y configurado.

La clave de licencia de Sandbox Analyzer On-Premises controla el número máximo de detonaciones simultáneas. Dado que cada detonación requiere una instancia de máquina virtual en ejecución, la cantidad de detonaciones simultáneas se refleja en el número de máquinas virtuales creadas. Para obtener más información sobre cómo añadir claves de licencia en GravityZone Control Center, consulte “Introducción de sus claves de licencia” (p. 124).

5.4.2. Implementar el appliance virtual Sandbox Analyzer

Para implementar el appliance virtual Sandbox Analyzer:

1. Inicie sesión en GravityZone Control Center.
2. Vaya a la página **Red > Paquetes**.
3. Marque la casilla de verificación **Sandbox Analyzer** de la tabla.
4. Haga clic en el botón **Descargar** de arriba a la izquierda de la página. Seleccione la opción **Appliance de seguridad (ESXi independiente)**.
5. Use su herramienta de administración de la virtualización (por ejemplo, vSphere Client) para importar el archivo OVA descargado a su entorno virtual.

   Nota
   Al implementar el archivo OVA, configure las redes de la siguiente manera:

   - **Red Bitdefender**: Esta es la red donde residen otros componentes de Bitdefender (interfaz `eth0`). Sandbox Analyzer y el appliance GravityZone deben estar en la misma red y han de comunicarse a través de `eth0`.
   - **Red de detonación privada**: Sandbox Analyzer utiliza esta red para la comunicación interna (interfaz `eth1`). Esta red debe estar aislada de cualquier otro segmento de red.
   - **Red de acceso a Internet**: Sandbox Analyzer utiliza esta red para obtener las últimas actualizaciones (interfaz `eth2`). La interfaz `eth2` no debe tener la misma IP o red que la `eth0`.

6. Encender el appliance.
7. Desde su herramienta de administración de la virtualización, acceda a la interfaz de la consola del appliance virtual Sandbox Analyzer.
8. Cuando se le soliciten las credenciales, use `root` como nombre de usuario y `sve` como contraseña.
9. Acceda al menú de configuración ejecutando el siguiente comando:

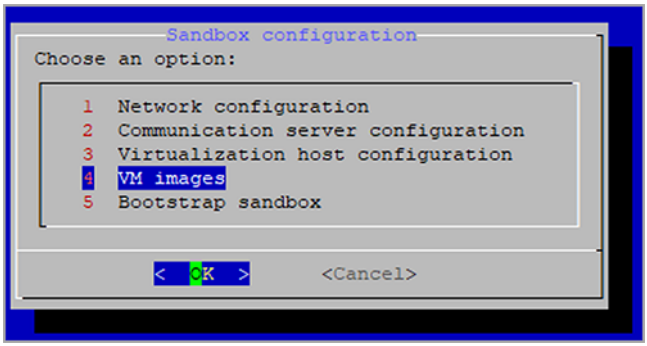
   ```
   /opt/bitdefender/bin/sandbox-setup
   ```

10. En el menú de **Configuración del espacio aislado**, realice los siguientes ajustes:

a. **Configuración de red**. Seleccione esta opción para configurar la NIC de administración. Sandbox Analyzer usará esta interfaz de red para comunicarse con GravityZone.

   La dirección IP se puede especificar manualmente o automáticamente a través de DHCP.

   > **Nota**
   > Si el appliance GravityZone está en otra red que no sea `eth0`, debe añadir una ruta estática en **Configuración de red > Red Bitdefender > Rutas** para que Sandbox Analyzer funcione correctamente.



Consola del appliance Sandbox Analyzer

b. **Configuración del proxy de Internet**. Para una correcta instalación, Sandbox Analyzer requiere conexión a Internet. De ser necesario, puede configurar Sandbox Analyzer para usar un servidor proxy especificando estos datos:

   - **Host**: La IP o nombre de dominio completo del servidor proxy. Utilice la siguiente sintaxis: `http://<IP/Nombredehost>:<Puerto>`.
   - **Usuario y contraseña**: Debe escribir la contraseña dos veces.
   - **Dominio**: El dominio de Active Directory, de ser el caso.

c. **Configuración del Servidor de comunicaciones**. Especifique la dirección IP o el nombre de host del appliance que ejecuta el rol de Servidor de comunicaciones.

Utilice la siguiente sintaxis: `http://<IP/Nombredelhost>:<Puerto>`. El puerto predeterminado es `8443`.

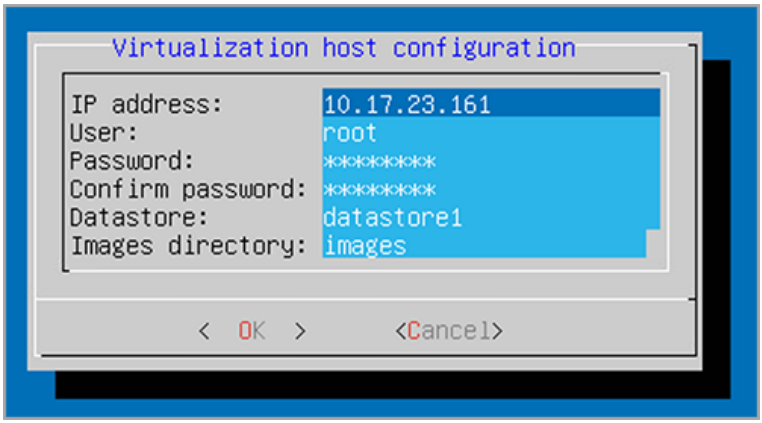
> **Nota**
> Tan pronto como se especifique la dirección IP o el nombre de host y se guarde la configuración, la instancia de Sandbox Analyzer aparecerá en GravityZone Control Center, en la página **Sandbox Analyzer > Infraestructura**.

d. **Configuración de host virtualizado** Sandbox Analyzer usa el servidor ESXi para aprovisionar la infraestructura de análisis de malware. Mediante la **Configuración de host virtualizado**, conecta el appliance Sandbox Analyzer al host ESXi proporcionando la siguiente información:

- La dirección IP del servidor ESXi.
- Credenciales de raíz para acceder al host ESXi.
- Datastore dedicado a Sandbox Analyzer.

  Escriba el nombre del datastore tal como lo muestra ESXi.
- Nombre de la carpeta utilizada en el datastore para almacenar imágenes de máquinas virtuales.

  Si esta carpeta no existe, debe crearla en el datastore antes de guardar la configuración de Sandbox Analyzer.



Consola del appliance Sandbox Analyzer

e. **Imágenes de máquinas virtuales**. Para crear las máquinas virtuales de detonación para Sandbox Analyzer, debe copiar los archivos VMDK que contienen las imágenes deseadas a la carpeta de **Imágenes** especificada en el menú de **Configuración de host virtualizado**. Para cada imagen, puede realizar los siguientes ajustes en el menú **Imágenes de máquinas virtuales**:

   i. En el menú de **Configuración de imágenes**, especifique el nombre de la imagen (como aparecerá en GravityZone Control Center) y el sistema operativo.

   > **Nota**
   > La carpeta que contiene las imágenes de máquinas virtuales se analiza periódicamente y se informa de las nuevas entradas a GravityZone. Estas entradas pueden verse en Control Center, en la página **Sandbox Analyzer > Infraestructura > Administración de imágenes**.

   En ciertas situaciones, al usar Sandbox Analyzer, puede encontrar problemas con las máquinas virtuales de detonación. Para abordar estos problemas, debe inhabilitar la opción contra huellas digitales. Para obtener información, consulte "Técnicas contra huellas digitales" (p. 167).

   ii. En el menú de **Hosts DMZ**, puede incluir en la lista blanca los nombres de host que requieren los servicios y componentes de terceros incrustados en las máquinas virtuales para comunicarse con Sandbox Manager. Para obtener información, consulte "Hosts DMZ" (p. 168).

   iii. En el menú **Limpieza**, puede eliminar las imágenes de máquinas virtuales que ya no necesite.

f. **Poner en marcha el espacio aislado**. Una vez que haya añadido los datos de configuración de Sandbox Analyzer, continúe con la instalación seleccionando esta opción. El estado de la instalación se reflejará en GravityZone Control Center, en la página **Sandbox Analyzer > Infraestructura**.

Técnicas contra huellas digitales

Durante el proceso de creación de imágenes, Sandbox Analyzer habilitará por defecto varias técnicas contra huellas digitales. Ciertos tipos de malware son capaces de determinar si se están ejecutando en un espacio aislado para, de ser así, no activar sus rutinas maliciosas.

El propósito de las técnicas contra huellas digitales es simular varias condiciones con el fin de imitar un entorno del mundo real. Debido a una combinación virtual

de software implementado y configuración del entorno, una combinación que no se puede prever ni controlar de antemano, es posible que ciertas técnicas no sean compatibles con el software instalado en la imagen maestra. Puede reconocer situaciones tan raras por los siguientes síntomas:

- Errores durante el proceso de creación de la imagen.
- Errores al intentar ejecutar el software dentro de la imagen.
- Mensajes de error devueltos al detonar muestras.
- El software bajo licencia ya no funciona debido a claves de licencia no válidas.

Un remedio rápido para estos casos atípicos consiste en reconstruir la imagen con las técnicas contra huellas digitales inhabilitadas. Para ello, siga los pasos indicados a continuación:

1. Inicie sesión en GravityZone Control Center y elimine la imagen.
2. Inicie sesión en el appliance Sandbox Analyzer y lance la consola del appliance Sandbox Analyzer ejecutando el siguiente comando:

   ```
   /opt/bitdefender/bin/sandbox-setup
   ```

3. Acceda a **Imágenes de máquinas virtuales > Configuración de imágenes**.
4. Seleccione la imagen que ocasiona problemas.
5. Acceda a la opción **Contra huellas digitales**.
6. Desmarque la casilla de verificación correspondiente para inhabilitar las técnicas contra huellas digitales.

Hosts DMZ

Durante el proceso de creación de imágenes, se creará una infraestructura virtual para facilitar la comunicación entre Sandbox Manager y las máquinas virtuales. Desde la perspectiva de la red, esto se traduce en un entorno de red aislado que contendrá toda la comunicación potencial que podría crear una muestra detonada.

El menú de servidores DMZ permite incluir en la lista blanca los nombres de host con los que necesitan comunicarse los servicios y componentes de terceros incrustados en las máquinas virtuales para funcionar correctamente.

Un ejemplo de esta situación serían los servidores de licencias KMS utilizados por las licencias de Windows, si se aplica una licencia por volumen en las máquinas virtuales suministradas.

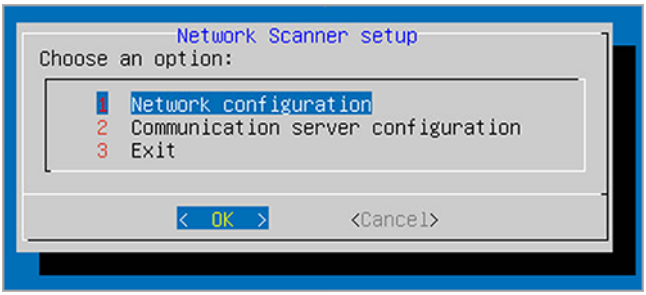
5.4.3. Implementar el Network Security Virtual Appliance

En esta sección se describe cómo implementar el Network Security Virtual Appliance, un componente de Sandbox Analyzer que captura el tráfico de la red y envía muestras sospechosas para el análisis de su comportamiento.

Para implementar el Network Security Virtual Appliance:

1. Inicie sesión en GravityZone Control Center.
2. Vaya a la página **Red > Paquetes**.
3. Marque la casilla de verificación **Network Security Virtual Appliance** en la tabla.
4. Haga clic en el botón **Descargar** en la parte superior izquierda de la tabla y seleccione la opción **(VMware OVA)**.
5. Use su herramienta de administración de la virtualización (por ejemplo, vSphere Client) para importar el archivo OVA descargado a su entorno virtual.
6. En el asistente de implementación, seleccione la tarjeta de interfaz de red (NIC) utilizada para la comunicación con GravityZone y la NIC utilizada para capturar el tráfico.
7. Encender el appliance.
8. Desde su herramienta de administración de la virtualización, acceda a la interfaz de la consola del GravityZone SVE SVA Network Security Virtual Appliance.
9. Cuando se le soliciten las credenciales, use `root` como nombre de usuario y `sve` como contraseña.
10. Acceda al menú de configuración ejecutando el siguiente comando:

```
/opt/bitdefender/bin/nsva-setup
```



Consola del appliance de seguridad de red

11. Acceda a la opción del menú **Configuración del Servidor de comunicaciones**.
12. Especifique la dirección IP o el nombre de host y el puerto de un Servidor de comunicaciones de GravityZone.

    Utilice la siguiente sintaxis: `http://<IP/Nombredelhost>:<Puerto>`. El puerto predeterminado es `8443`.
13. Guarde la configuración.

Configure el sensor de red para detonar archivos pcap

El sensor de red puede extraer contenido de los archivos de captura de red (pcap) y enviarlo automáticamente para su detonación a la instancia de Sandbox Analyzer.

Para detonar contenido de archivos pcap:

1. Inicie sesión en el Network Security Virtual Appliance.
2. Cuando se le soliciten las credenciales, use `root` como nombre de usuario y `sve` como contraseña.
3. Ejecute el siguiente comando:

   ```
   /opt/bitdefender/bin/scan-pcap <local pcap path>
   ```

   En el comando anterior, `<local pcap path>` representa la ubicación donde se carga el archivo pcap en el Network Security Virtual Appliance.

Para obtener más información sobre el uso del sensor de red, consulte el capítulo **Políticas > Sandbox Analyzer** de la Guía del administrador de GravityZone.

5.5. Instalación del Cifrado de disco completo

El Cifrado de disco completo de GravityZone se proporciona como servicio que requiere su activación según la clave de licencia. Para ello, debe acceder a **Configuración > Licencia** e introducir la clave de licencia.

Para obtener información detallada sobre las claves de licencia, consulte "Administración de Licencias" (p. 123).

Los agentes de seguridad de Bitdefender admiten el Cifrado de disco completo desde la versión 6.2.22.916 en Windows y 4.0.0173876 en Mac. Para asegurarse de que los agentes son totalmente compatibles con este módulo, tiene dos opciones:

- Instale los agentes de seguridad con el módulo de Cifrado incluido.
- Utilice la tarea **Reconfigurar**.

Para obtener información detallada sobre el uso del Cifrado de disco completo en su red, consulte el capítulo **Políticas de seguridad > Cifrado** de la Guía del administrador de GravityZone.

5.6. Instalación de la Protección de Exchange

Security for Exchange se integra automáticamente con los servidores de Exchange, dependiendo del rol del servidor. Solo se instalan las características compatibles para cada rol, como se describe aquí:

Características	Microsoft Exchange 2019/2016/2013		Microsoft Exchange 2010/2007		
	Perimetral	Buzón de Correo	Perimetral	Concentrador	Buzón de Correo
Nivel de transporte					
Filtrado antimalware	x	x	x	x	
Filtros Antispam	x	x	x	x	
Filtro de Contenido	x	x	x	x	
Filtro de Adjuntos	x	x	x	x	
Almacén de Exchange					
Análisis antimalware bajo demanda		x			x

5.6.1. Preparándose para la Instalación

Antes de instalar Security for Exchange, asegúrese de que se cumplen todos los requisitos, pues de lo contrario Bitdefender Endpoint Security Tools podría instalarse sin el módulo de protección de Exchange.

Para que el módulo de protección de Exchange se ejecute sin problemas y para evitar conflictos y resultados imprevistos, elimine todos los agentes antimalware y de filtrado de correo electrónico.

Bitdefender Endpoint Security Tools detecta y elimina automáticamente la mayoría de los productos antimalware y desactiva el agente antimalware integrado en Exchange Server desde la versión 2013. Para obtener más información sobre la lista del software de seguridad detectado, consulte este artículo de la base de conocimientos.

Puede volver a activar manualmente el agente antimalware integrado en Exchange en cualquier momento, aunque no es recomendable.

5.6.2. Instalación de la protección de servidores de Exchange

Para proteger sus servidores de Exchange, debe instalar Bitdefender Endpoint Security Tools con rol de protección de Exchange en cada uno de ellos.

Tiene varias opciones para implementar Bitdefender Endpoint Security Tools en los servidores de Exchange:

- Instalación local, con la descarga y ejecución del paquete de instalación en el servidor.
- Instalación remota, mediante la ejecución de una tarea **Instalar**.
- Remota, mediante la ejecución de la tarea **Reconfigurar el cliente**, si Bitdefender Endpoint Security Tools ya ofrece protección del sistema de archivos en el servidor.

Para conocer los pasos de instalación detallados, consulte "Instalación de los agentes de seguridad" (p. 137).

5.7. Instalación de HVI

Para poder utilizar HVI en máquinas virtuales de sus hosts Xen, tiene que llevar a cabo los siguientes pasos:

1. Comprobar los requisitos previos de instalación
2. Instalar Security Server
3. Instalar el paquete suplementario de HVI

Requisitos

- XenServer está integrado con GravityZone.
- XenCenter está instalado en su máquina.

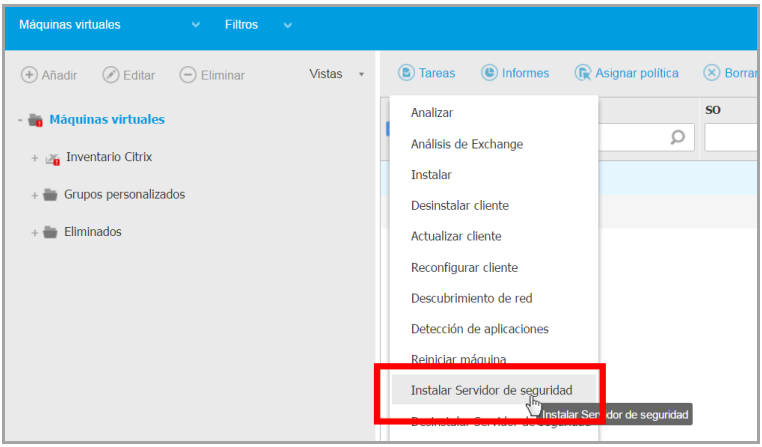
Instalación de Security Server

Para instalar Security Server en uno o varios hosts:

1. Diríjase a la página **Red**.
2. Seleccione **Máquinas virtuales** desde el selector de vistas.
3. Examine el inventario Citrix y marque las casillas de selección correspondientes a los contenedores o hosts deseados. Para una selección rápida, puede seleccionar directamente el contenedor raíz (Inventario Citrix). Podrá seleccionar hosts individualmente en el asistente de instalación.

Nota
No puede seleccionar los hosts de distintas carpetas.

4. Haga clic en el botón **Tareas** de la parte superior de la tabla y seleccione **Instalar Security Server** en el menú. Se muestra la ventana **Instalación de Security Server**.



Instalación de Security Server

5. Seleccione los hosts en los que quiera instalar las instancias Security Server.
6. Elija los ajustes de configuración que quiera emplear.

Importante
Utilizar ajustes comunes para la implementación simultánea de instancias en múltiples Security Server requiere que los hosts compartan el mismo almacenamiento, tengan sus direcciones IP asignadas por un servidor DHCP y formen parte de la misma red.

Si elige configurar cada Security Server de forma diferente, podrá definir los ajustes que desee para cada host en el siguiente paso del asistente. Los pasos descritos a continuación se aplican a cuando se utiliza la opción **Configurar cada Security Server**.

7. Haga clic en **Siguiente**.

Nota
Dependiendo de la selección realizada anteriormente, algunas de las opciones descritas aquí podrían no ser aplicables a su situación.

8. Escriba un nombre descriptivo para Security Server.
9. Seleccione el contenedor en el que quiere incluir el Security Server en el menú **Contenedor**.
10. Seleccione el almacenamiento de destino.
11. Elija el tipo de provisión de disco. Se recomienda implementar el appliance usando aprovisionamiento con discos thick.

    Importante
    Si utiliza aprovisionamiento con discos thin y se queda sin espacio en disco en el datastore, el Security Server se detendrá y, en consecuencia, el host se quedará sin protección.

12. Configure la asignación de recursos de CPU y memoria basándose en el ratio de consolidación de la MV en el host. Escoja **Bajo**, **Medio** o **Alto** para cargar los ajustes de asignación de recursos recomendados o **Manual** para configurar la asignación de recursos manualmente.
13. Establezca la zona horaria del appliance.
14. Establezca una contraseña de administrador para la consola de Security Server. Establecer una contraseña administrativa anula la contraseña raíz predeterminada ("sve").
15. Seleccione el tipo de configuración de red para la red de Bitdefender. La dirección IP de Security Server no debe cambiarse a lo largo del tiempo, ya que los agentes de Linux la utilizan para comunicarse.

    Si escoge DHCP, asegúrese de configurar el servidor DHCP para que reserve una dirección IP para el appliance.

    Si escoge fija, debe introducir la información sobre la dirección IP, máscara de subred, puerta de enlace y DNS.
16. Haga clic en **Guardar**.

Puede ver y administrar las tareas en la página **Red > Tareas**.

Instalar el paquete suplementario de HVI

1. Acceda a la página **Configuración > Actualización**.
2. Seleccione el paquete suplementario de HVI en la lista de **Componentes** y haga clic en el botón **Descargar** de la zona superior de la tabla.
3. Acceda a la página **Red** y seleccione **Máquinas virtuales** en el selector de vistas.
4. Seleccione **Servidor** en el menú de **Vistas** del panel izquierdo.
5. Seleccione uno o más hosts Xen del inventario de red. Puede ver fácilmente los hosts disponibles seleccionando la opción **Tipo > Hosts** en el menú **Filtros**.
6. Haga clic en el botón **Tareas** del panel derecho y seleccione **Instalar el paquete suplementario de HVI**. Se abre la ventana de instalación.
7. Programe cuándo debe ejecutarse la tarea de instalación. Puede optar por ejecutar la tarea inmediatamente después de guardarla, o en un momento determinado. En caso de que no se pueda completar la instalación en el momento especificado, la tarea se repite automáticamente según los ajustes de recurrencia. Por ejemplo, si selecciona varios hosts y uno no está disponible cuando esté programada la instalación del paquete, la tarea se ejecutará de nuevo a la hora especificada.
8. Debe reiniciarse el host para aplicar los cambios y completar la instalación. Si desea que el host se reinicie de forma desatendida, seleccione **Reiniciar el host automáticamente**.
9. Haga clic en **Guardar**. Aparecerá un mensaje de confirmación.

   Puede ver y administrar las tareas en la página **Red > Tareas**.

5.8. Instalación de la Protección de almacenamiento

Security for Storage es un servicio de Bitdefender diseñado para proteger los dispositivos de almacenamiento conectado a la red (NAS) y los sistemas de uso compartido de archivos compatibles con el protocolo de adaptación de contenido de Internet (ICAP). Para conocer los sistemas de uso compartido de archivos compatibles, consulte “Protección de almacenamiento” (p. 57).

Para usar Security for Storage con su solución GravityZone, debe hacer lo siguiente:

1. Instale y configure al menos dos Security Server en su entorno para que actúen como servidores ICAP. Los Security Server de Bitdefender analizan los archivos, envían veredictos a los sistemas de almacenamiento y adoptan las medidas

adecuadas de ser necesario. En caso de sobrecarga, el primer Security Server redirige el excedente de datos al segundo.

> **Nota**
> Le recomendamos que instale Security Server dedicados para la protección del almacenamiento, independientes de los Security Server utilizados para otros roles, como el análisis antimalware.

Para obtener más información sobre el procedimiento de instalación de Security Server, consulte la sección **Instalación de Security Server** de esta guía.

2. Configure el módulo de **Protección de almacenamiento** desde los ajustes de política de GravityZone.

   Para obtener más información, consulte el capítulo **Políticas de seguridad > Políticas de equipos y máquinas virtuales > Protección de almacenamiento** de la Guía del administrador de GravityZone.

Para obtener más información sobre la configuración y administración de servidores ICAP en determinado dispositivo NAS o sistema de uso compartido de archivos, consulte la documentación de esa plataforma específica.

5.9. Instalación de la protección para dispositivos móviles

Security for Mobile es una solución de administración de dispositivos móviles diseñada para iPhone, iPad y dispositivos Android. Para obtener una lista completa de las versiones soportadas del sistema operativo, consulte requisitos del sistema.

Para administrar Security for Mobile desde Control Center, hay que añadir los dispositivos móviles a Active Directory o a usuarios personalizados y, a continuación, instalar la aplicación GravityZone Mobile Client en los dispositivos. Después de configurar el servicio, puede ejecutar tareas de administración en los dispositivos móviles.

Antes de empezar, asegúrese de configurar una dirección pública (externa) para el Servidor de comunicaciones.

Para instalar Security for Mobile:

1. Si no tiene integración con Active Directory, debe crear usuarios para los propietarios de dispositivos móviles.
2. Añada dispositivos a los usuarios.
3. Instale GravityZone Mobile Client en los dispositivos y actívelo.

5.9.1. Configurar una dirección externa para el Servidor de comunicaciones

En la configuración predeterminada de GravityZone, los dispositivos móviles pueden gestionarse solamente cuando están conectados directamente a la red corporativa (vía Wi-Fi o VPN). Esto ocurre porque al inscribir los dispositivos móviles están configurados para conectarse a la dirección local del appliance Servidor de comunicaciones.

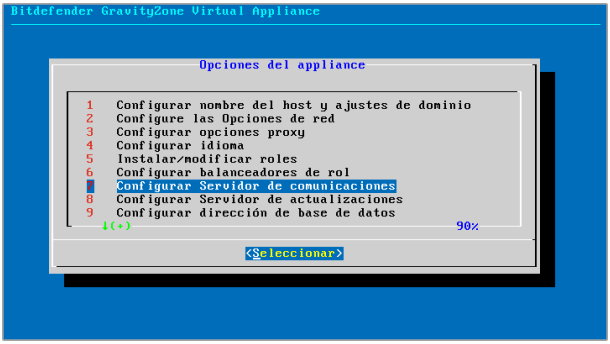
Para poder gestionar dispositivos móviles a través de Internet, con independencia de dónde estén localizados, debe configurar el Servidor de comunicaciones con una dirección accesible públicamente.

Para poder administrar dispositivos móviles cuando no están conectados a la red de la empresa, están disponibles las siguientes opciones:

- Configurar un puerto de envío en la puerta de enlace corporativa para el appliance que ejecuta el rol de Servidor de comunicaciones.
- Añadir un adaptador de red adicional al appliance que desempeña el rol de Servidor de comunicaciones y asignarle una dirección IP pública.

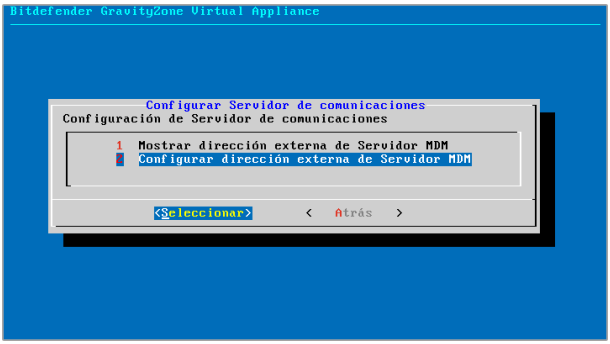
En ambos casos debe configurar el Servidor de comunicaciones con la dirección externa para utilizar la gestión de dispositivos móviles:

1. Acceda a la consola del appliance desde su herramienta de administración de la virtualización (por ejemplo, vSphere Client).
2. Desde le menú principal, seleccione **Configurar Servidor de comunicaciones**.



Ventana de opciones de la aplicación

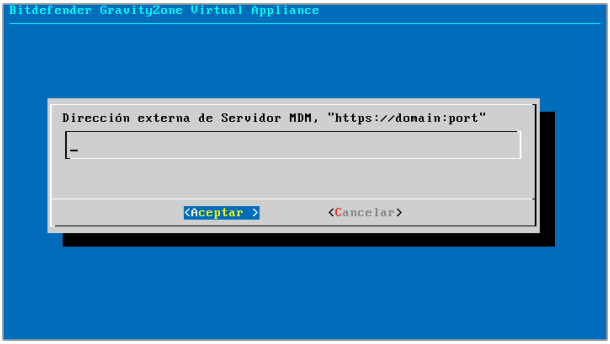
3. Seleccione **Configurar dirección externa del Servidor MDM**.



Ventana de configuración del servidor de comunicaciones

4. Escriba la dirección externa.

   Utilice la siguiente sintaxis: `https://<IP/Dominio>:<Puerto>`.



Ventana de introducción de dirección externa de Servidor MDM

   - Si utiliza reenvío de puertos, debe escribir la dirección IP pública o el nombre de dominio y el puerto abierto en la puerta de enlace.
   - Si utiliza una dirección pública para el Servidor de comunicaciones, debe escribir la dirección IP pública o nombre de dominio y el puerto del Servidor de comunicaciones. El puerto predeterminado es `8443`.

5. Seleccione **Aceptar** para guardar los cambios.

5.9.2. Cree y organice los usuarios personalizados

En situaciones sin Active Directory, primero debe crear usuarios personalizados para disponer de un medio para identificar a los propietarios de los dispositivos móviles. Los usuarios especificados de dispositivos móviles no están vinculados de ninguna forma con Active Directory o con usuarios definidos en Control Center.

Creación de usuarios personalizados

Para crear un usuario personalizado:

1. Diríjase a la página **Red**.
2. Seleccione **Dispositivos móviles** desde el selector de vistas.
3. En el panel izquierdo, seleccione **Grupos personalizados**.
4. Haga clic en el icono **Añadir usuario** en la barra de herramientas de acción. Aparecerá una nueva ventana de configuración.
5. Especifique los detalles de usuario necesarios:
   - Un nombre de usuario descriptivo (por ejemplo, el nombre completo del usuario)
   - La dirección de correo del usuario

   Importante
   - Asegúrese de proporcionar una dirección de correo válida. Se enviarán al usuario las instrucciones de instalación por correo cuando añada un dispositivo.
   - Cada dirección de email puede asociarse únicamente a un usuario.

6. Haga clic en **Aceptar**.

Organización de usuarios personalizados

Para organizar los usuarios personalizados:

1. Cree grupos personalizados.
   a. Seleccione **Grupos personalizados** en el panel lateral izquierdo y haga clic en el icono **Añadir** en la barra de herramientas de acción (encima del panel).

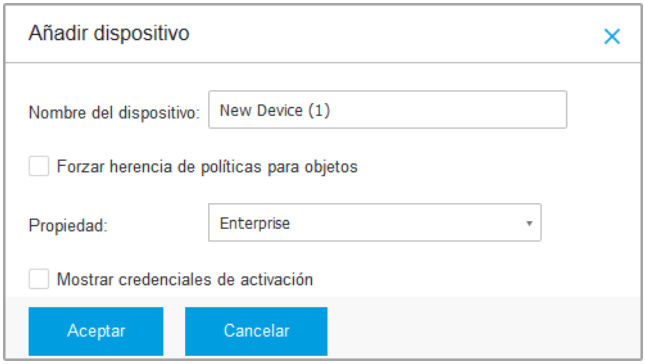
b. Escriba un nombre descriptivo para el grupo y haga clic en **Aceptar**. El nuevo grupo se muestra bajo **Grupos personalizados**.

2. Mueva los usuarios personalizados a los grupos personalizados adecuados.
   a. Seleccione los usuarios en el panel derecho.
   b. Arrastre y suelte la selección sobre el grupo deseado en el panel lateral izquierdo.

5.9.3. Añada dispositivos a los usuarios

Para añadir un dispositivo a un usuario:

1. Diríjase a la página **Red**.
2. Seleccione **Dispositivos móviles** desde el selector de vistas.
3. Busque el usuario en las carpetas Active Directory o en los Grupos personalizados.
4. Haga clic en el icono ⊕ **Añadir dispositivo** en la parte superior de la tabla de red. Aparecerá una nueva ventana de configuración.



Añadir un dispositivo móvil a un usuario

5. Escriba un nombre descriptivo para el dispositivo.
6. Utilice la opción **Autoconfigurar nombre** si desea que el nombre del dispositivo se genere automáticamente. Al añadirlo, el dispositivo tiene un nombre genérico. Una vez que se activa el dispositivo, se renombra automáticamente con la información correspondiente de fabricante y modelo.

7. Seleccione el tipo de propiedad del dispositivo (empresa o personal).
8. Seleccione la opción **Mostrar credenciales de activación** tras hacer clic en el botón **OK** si va a instalar el GravityZone Mobile Client en el dispositivo del usuario.
9. Haga clic en **Aceptar**. Se envía inmediatamente un correo al usuario con las instrucciones de instalación y los detalles de activación para configurarlos en el dispositivo. Los detalles de activación incluyen el token de activación y la dirección del servidor de comunicaciones (y el código QR correspondiente).

Nota

- Puede ver los detalles de activación de un dispositivo en cualquier momento haciendo clic en su nombre en Control Center.
- Puede también añadir dispositivos móviles a una selección de usuarios y grupos. En tal caso, la ventana de configuración permitirá solo definir la propiedad de los dispositivos. Los dispositivos móviles creados por selección múltiple recibirán de forma predeterminada un nombre genérico. En cuanto se registre el dispositivo, su nombre cambiará automáticamente, incluyendo la información correspondiente al fabricante y modelo.

5.9.4. Instale GravityZone Mobile Client en los dispositivos

La aplicación GravityZone Mobile Client se distribuye exclusivamente en el Apple App Store y Google Play.

Para instalar GravityZone Mobile Client en un dispositivo:

1. Busque la aplicación en la tienda oficial de apps.
   - Enlace de Google Play
   - Enlace Apple App Store
2. Descargue e instale la aplicación en el dispositivo.
3. Inicie la aplicación y lleve a cabo la configuración requerida:
   a. En dispositivos Android, toque **Activar** para habilitar GravityZone Mobile Client como administrador del dispositivo. Lea cuidadosamente la información proporcionada.

Nota

- La tarea de bloqueo para dispositivos Android (7.0 o superior) aplicará la contraseña configurada en su consola GravityZone solo si no se ha configurado una protección de bloqueo en el dispositivo. De lo contrario, se utilizarán las opciones de bloqueo de pantalla existentes, como Patrón, PIN, Contraseña, Huella dactilar o Smart Lock, para proteger el dispositivo.
- La tarea de desbloqueo ya no está disponible para dispositivos Android (7.0 o superior).
- Debido a limitaciones técnicas, las tareas de bloqueo y borrado no están disponibles en Android 11.

b. Escriba el token de activación y la dirección del servidor de comunicaciones, o bien escanee el código QR recibido por correo.

c. Toque **Confiar** cuando se le pida que acepte el certificado del Servidor de comunicaciones. De este modo, GravityZone Mobile Client valida el Servidor de comunicaciones y solo aceptará mensajes de él, para evitar ataques man-in-the-middle.

d. Toque **Activar**.

e. En los dispositivos iOS, se le pedirá que instale el perfil MDM. Si su dispositivo está protegido por contraseña, se le pedirá que la proporcione. Además, debe permitir que GravityZone acceda a los ajustes de su dispositivo; de lo contrario, el proceso de instalación volverá al paso anterior. Siga las instrucciones que aparecen en pantalla para completar la instalación del perfil.

Nota
Para que la función de localización opere correctamente, los usuarios deben permitir la ubicación de los dispositivos en segundo plano, no solo mientras usan la aplicación.

5.10. Instalación del Generador de informes

El Generador de informes le permite crear y gestionar consultas e informes detallados basados ??en consultas en GravityZone.

El Generador de informes consta de dos roles, Base de datos y Procesadores, que vienen con el appliance virtual GravityZone y deben instalarse por separado el uno del otro y también independientemente de otros roles de GravityZone. Después de

instalar el Generador de informes, su entorno GravityZone debe ejecutar al menos tres instancias del appliance virtual GravityZone, de la siguiente manera:

- Una o más instancias del appliance virtual GravityZone con todos los roles instalados, excepto la Base de datos del Generador de informes y los Procesadores del Generador de informes.
- Una instancia del appliance virtual GravityZone con el rol de Base de datos del Generador de informes instalado.
- Una instancia del appliance virtual GravityZone con el rol de Procesadores del Generador de informes instalado.

Para una instalación sin problemas, asegúrese en primer lugar de que su entorno virtual cumple con los requisitos de hardware y software. Luego, debe tener a mano:

- La imagen del appliance virtual GravityZone, que utilizará para instalar tanto el rol de Base de datos como el de Procesadores del Generador de informes.
- El nombre de DNS o la dirección IP del appliance virtual GravityZone que tiene el rol de base de datos de GravityZone instalado.
- Nombre de usuario y contraseña de un administrador de dominio.
- Contraseña para la base de datos GravityZone. Si la olvida, puede crear otra en la interfaz de consola del appliance GravityZone.

La instalación del Generador de informes se desarrolla en dos fases:

- Instalación del rol de Base de datos del Generador de informes
- Instalación del rol de Procesadores del Generador de informes

Se recomienda que instale primero GravityZone y configure Control Center (si es preciso) y, luego, actualice GravityZone, implemente la protección en los endpoints y, finalmente, instale los roles del Generador de informes.

Importante
Se requiere instalar primero el rol de Base de datos del Generador de informes y, luego, el de Procesadores del Generador de informes.

5.10.1. Instalación del rol de Base de datos del Generador de informes

La Base de datos del Generador de informes es el primer rol que debe instalar. Para instalar este rol:

1. Importe el appliance virtual GravityZone en su entorno virtualizado.
2. Encender el appliance.
3. Desde su herramienta de administración de la virtualización, acceda a la interfaz de la consola del appliance virtual GravityZone.
4. Configure la contraseña para el administrador de sistema `bdadmin` incorporado.
5. Inicie sesión con la contraseña que ha configurado para acceder a la interfaz de configuración del appliance. Utilice las teclas de flecha y la tecla `Tabulador` para navegar por los menús y opciones. Pulse `Intro` para seleccionar una opción específica.

   Inicialmente, la interfaz del appliance está en inglés.

   Para cambiar el idioma de la interfaz:
   a. Seleccione **Configurar idioma** en el menú principal.
   b. Seleccione el idioma deseado entre las opciones disponibles. Aparecerá un mensaje de confirmación.

      Nota
      Es posible que tenga que desplazarse hacia abajo para ver su idioma.

   c. Seleccione **Aceptar** para guardar los cambios.
6. Acceda a **Ajustes avanzados** y seleccione **Conectarse a la base de datos existente**.
7. Introduzca la dirección IP y la contraseña de la base de datos de GravityZone.
8. En el menú de **Ajustes avanzados**, seleccione **Instalar/Desinstalar roles**.
9. Acceda a **Añadir o eliminar roles** y elija **Base de datos del Generador de informes**. Pulse la `barra espaciadora` para seleccionar instalar este rol y, a continuación, pulse `Intro` para continuar. Pulse `Intro` otra vez para confirmar y espere a que finalice la instalación.

Nota
El rol de Base de datos del Generador de informes se instala y se ejecuta como instancia independiente. No se admiten las copias de seguridad de conjuntos de réplicas.

5.10.2. Instalación del rol de Procesadores del Generador de informes

El de Procesadores del Generador de informes es el segundo rol que debe instalar. Para instalar este rol:

1. Importe el appliance virtual GravityZone en su entorno virtualizado.
2. Encender el appliance.
3. Desde su herramienta de administración de la virtualización, acceda a la interfaz del appliance virtual GravityZone.
4. Configure la contraseña para el administrador de sistema `bdadmin` incorporado.
5. Inicie sesión con la contraseña que ha establecido. Accederá a la interfaz de configuración del appliance. Utilice las teclas de flecha y la tecla `Tabulador` para navegar por los menús y opciones. Pulse `Intro` para seleccionar una opción específica.

   Inicialmente, la interfaz del appliance está en inglés.

   Para cambiar el idioma de la interfaz:
   a. Seleccione **Configurar idioma** en el menú principal.
   b. Seleccione el idioma deseado entre las opciones disponibles. Aparecerá un mensaje de confirmación.

      Nota
      Es posible que tenga que desplazarse hacia abajo para ver su idioma.

   c. Seleccione **Aceptar** para guardar los cambios.
6. Acceda a **Ajustes avanzados** y seleccione **Conectarse a la base de datos existente**.
7. Introduzca la dirección IP y la contraseña de la base de datos de GravityZone.
8. En el menú de **Ajustes avanzados**, seleccione **Instalar/Desinstalar roles**.
9. Acceda a **Añadir o eliminar roles** y elija **Procesadores del Generador de informes**. Pulse la `barra espaciadora` para seleccionar instalar este rol y, a continuación, pulse `Intro` para continuar. Pulse `Intro` otra vez para confirmar y espere a que finalice la instalación.

Nota
El rol de Procesadores del Generador de informes se instala y se ejecuta como instancia independiente.

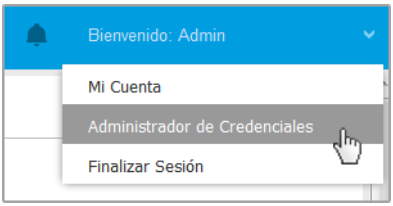
Después de instalar el Generador de informes, se muestra la nueva opción de menú **Consultas** en la sección **Informes** de Control Center.

Los roles de Base de datos y Procesadores del Generador de informes se muestran en la sección **Infraestructura** de la página **Configuración > Actualizar**, junto con los otros roles de GravityZone.

5.11. Administrador de Credenciales

El Gestor de credenciales le ayuda a definir las credenciales necesarias para acceder a los inventarios del vCenter Server disponibles y también para la autenticación remota en los distintos sistemas operativos de su red.

Para abrir el Gestor de credenciales, haga clic en su nombre de usuario en la esquina superior derecha de la página y seleccione **Gestor de credenciales**.



El menú Gestor de credenciales

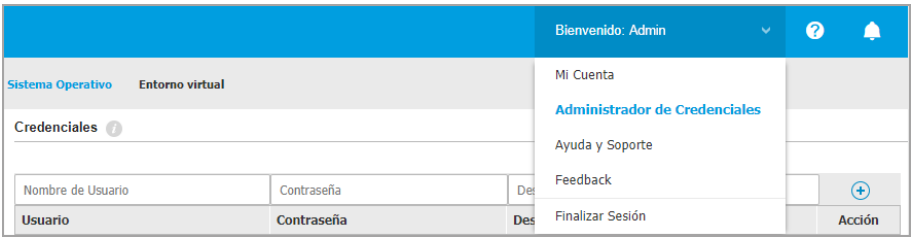
La ventana **Gestor de credenciales** contiene dos pestañas:

- Sistema Operativo
- Entorno virtual

5.11.1. Sistema Operativo

En la pestaña **Sistema operativo** puede gestionar las credenciales de administrador necesarias para la autenticación remota cuando se envían tareas de instalación a equipos y máquinas virtuales de su red.

Para añadir un conjunto de credenciales:



Administrador de Credenciales

1. Escriba el nombre de usuario y contraseña de una cuenta de administrador para cada uno de los sistemas operativos objetivo en los campos correspondientes de la zona superior del encabezado de la tabla. Opcionalmente puede añadir una descripción que le ayudará a identificar más fácilmente cada cuenta. Si los equipos están en un dominio, es suficiente con introducir las credenciales del administrador del dominio.

   Utilice las normas de Windows cuando introduzca el nombre de una cuenta de usuario:

   - Para las máquinas de Active Directory, utilice estas sintaxis: `usuario@dominio.com` y `dominio\usuario`. Para asegurarse de que las credenciales introducidas funcionarán, añádalas de ambas maneras (`nombredeusuario@dominio.com` y `dominio\nombredeusuario`).
   - Para las máquinas del grupo de trabajo es suficiente con introducir solo el nombre de usuario, sin el nombre del grupo de trabajo.

2. Haga clic en el botón ⊕ **Añadir** del lateral derecho de la tabla. El nuevo conjunto de credenciales se añade a la tabla.

> **Nota**
> Si no ha especificado las credenciales de autenticación, necesitará introducirlas cuando ejecute tareas de instalación. Las credenciales especificadas se guardan automáticamente en su Gestor de credenciales para que no tenga que volver a introducirlas la próxima vez.

5.11.2. Entorno virtual

Desde la pestaña Entorno virtual, puede administrar las credenciales de autenticación para los sistemas servidores virtualizados disponibles.

Para acceder a la infraestructura virtualizada integrada con Control Center, debe proporcionar sus credenciales de usuario para cada sistema de servidor virtualizado disponible. Control Center usa sus credenciales para conectar con la infraestructura virtualizada, mostrando solamente los recursos a los que tiene acceso (según se define en el servidor virtualizado).

Para especificar las credenciales necesarias para conectarse a un servidor virtualizado:

1. Seleccione el servidor en el menú correspondiente.

   Nota
   Si el menú no está disponible, o bien no se ha configurado todavía la integración, o todas las credenciales necesarias ya han sido configuradas.

2. Escriba su nombre de usuario y contraseña, y una descripción adecuada.
3. Haga clic en el botón ⊕ **Añadir**. El nuevo conjunto de credenciales se añade a la tabla.

   Nota
   Sí no configura sus credenciales de autenticación en el Gestor de credenciales, tendrá que introducirlas cada vez que quiera examinar el inventario de cualquier sistema servidor virtualizado. Una vez introducidas las credenciales, se guardan automáticamente en su Gestor de credenciales para que no tenga que volver a introducirlas la próxima vez.

   Importante
   Siempre que cambie su contraseña de usuario del servidor virtualizado, recuerde actualizarla también en el Gestor de credenciales.

5.11.3. Eliminación de credenciales del Gestor de credenciales

Para eliminar credenciales obsoletas del Gestor de credenciales:

1. Vaya a la fila de la tabla que contiene las credenciales que desea eliminar.
2. Haga clic en el botón ⊗ **Eliminar** a la derecha de la fila de la tabla correspondiente. La cuenta seleccionada se eliminará.

6. ACTUALIZACIÓN DE GRAVITYZONE

Bitdefender publica todas las actualizaciones del producto y de los contenidos de seguridad a través de los servidores de Bitdefender en Internet. Todas las actualizaciones van cifradas y firmadas digitalmente, por lo que es imposible manipularlas.

GravityZone incluye un rol de Servidor de actualización, diseñado para servir de punto de distribución de actualizaciones centralizado para su implementación de GravityZone. El Servidor de actualización comprueba y descarga todas las actualizaciones de GravityZone disponibles desde los servidores de actualización Bitdefender de Internet, poniéndolas a disposición de la red local. Los componentes GravityZone pueden configurarse para que se actualicen automáticamente desde el servidor de actualización local en lugar de desde Internet.

Cuando hay una nueva actualización disponible, el appliance GravityZone, el agente de seguridad o el Security Server, comprueban la autenticidad de la firma digital de la actualización, así como la integridad del contenido del paquete. A continuación, se analizan las actualizaciones y se comprueban sus versiones respecto a las instaladas. Los archivos nuevos se descargan localmente y se comprueban sus hash MD5 para cerciorarse de que no han sido alterados.

Si en cualquier momento no se superase una comprobación, el proceso de actualización se detendría y comunicaría un mensaje. De lo contrario, la actualización se considerará válida y lista para instalarse.

Para actualizar los appliances GravityZone instalados en su entorno y los paquetes de instalación de los componentes de GravityZone, inicie sesión con una cuenta de administrador de empresa y acceda a la página **Configuración > Actualizar**.

6.1. Actualizar appliances GravityZone

Mediante las actualizaciones del appliance GravityZone, Bitdefender lanza nuevas características y mejoras. Estas son visibles en Control Center.

Antes de ejecutar una actualización, se recomienda que compruebe lo siguiente:

- El estado de la actualización
- Cualquier información o mensaje de advertencia que pueda aparecer.
- El registro de cambios

Para comprobar el estado de la actualización:

1. Acceda a la página **Configuración > Actualizar > Roles de GravityZone**.
2. En la sección **Estado actual**, observe el mensaje que indica el estado general de su implementación. Si GravityZone necesita actualizarse, el botón **Actualizar** estará disponible.
3. En la sección **Infraestructura**, inspeccione los detalles de cada rol de GravityZone implementado en su red. Dado que los roles se actualizan de forma independiente, para cada rol puede ver lo siguiente: el nombre del appliance que lo aloja, su dirección IP, la versión actual, la última versión disponible y el estado de la actualización.

Para comprobar el registro de cambios:

1. Acceda a la página **Configuración > Actualizar > Roles de GravityZone**.
2. Haga clic en el enlace **Ver registro de cambios**. Una ventana emergente muestra una lista con todas las versiones y los cambios que incluyeron.

   Las notas de la versión para cada nueva versión del producto también se publican en el Centro de soporte de Bitdefender.

Puede actualizar GravityZone de dos maneras:

- Manualmente
- Automáticamente

6.1.1. Actualización Manual

Elija este método si desea tener un control total de cuándo debe iniciarse la actualización.

Para actualizar GravityZone manualmente:

1. Acceda a la página **Configuración > Actualizar > Roles de GravityZone**.
2. Haga clic en el botón **Cambiar** (si está disponible).

   La actualización podría tardar un poco. Espere hasta que haya finalizado.
3. Limpie la caché del navegador.

Durante la actualización, Control Center cierra la sesión de todos los usuarios y les informa de que hay una actualización en curso. Podrá ver un progreso detallado del proceso de actualización.

Cuando finaliza la actualización, Control Center muestra la página de inicio de sesión.

6.1.2. Actualizaciones automáticas

Si instala las actualizaciones automáticamente, se asegurará de que GravityZone siempre esté actualizado con las últimas características y parches de seguridad.

GravityZone tiene dos tipos de actualizaciones automáticas:

- Actualizaciones de producto
- Actualizaciones de software de terceros

Actualizaciones de producto

Estas actualizaciones aportan nuevas características a GravityZone y resuelven los problemas resultantes de dichas características.

Dado que las actualizaciones perturban el trabajo de los usuarios de GravityZone, están diseñadas para ejecutarse de forma programada. Puede programar la actualización para que tenga lugar en horarios que le convengan. Por defecto, las actualizaciones automáticas del producto están inhabilitadas.

Para habilitar y programar actualizaciones del producto:

1. Acceda a la página **Configuración > Actualizar > Roles de GravityZone**.
2. Marque la casilla de verificación **Habilitar actualizaciones automáticas del producto GravityZone**.
3. Establezca la **Recurrencia** en **Diaria**, **Semanal** (seleccione uno o más días de la semana) o **Mensual**.
4. Defina un **Intervalo**. Puede programar un momento para que comience el proceso de actualización cuando haya una nueva actualización disponible.

GravityZone muestra por defecto un mensaje de advertencia a todos los usuarios de Control Center treinta minutos antes de que comience la actualización automática. Para desactivar la advertencia, desmarque la casilla de verificación **Habilitar la alerta de inactividad treinta minutos antes de la actualización**.

Actualizaciones de software de terceros

El appliance virtual GravityZone incorpora una serie de productos de software proporcionados por otros proveedores. Este tipo de actualizaciones pretenden parchear dicho software lo antes posible para disminuir los posibles riesgos para la seguridad.

Estas actualizaciones se ejecutan de forma silenciosa y no interrumpen el trabajo con Control Center.

Esta opción está habilitada por defecto. Para inhabilitar esta opción:

1. Acceda a la página **Configuración > Actualizar > Roles de GravityZone**.
2. Desmarque la casilla de verificación **Habilitar las actualizaciones automáticas de seguridad para los componentes de terceros de GravityZone**.

   Así, los parches de software de terceros se lanzarán una vez con la actualización del producto GravityZone.

6.2. Configurar el Servidor de actualización

De forma predeterminada, el Servidor de actualización descarga las actualizaciones desde Internet cada hora. Se recomienda no cambiar los ajustes predeterminados del Servidor de actualización.

Para consultar y configurar los ajustes del Servidor de actualización:

1. Acceda a la página **Actualizar** en Control Center y haga clic en la pestaña **Componentes**.
2. Haga clic en el botón **Ajustes** de la zona superior del panel de la izquierda para mostrar la ventana **Ajustes del Servidor de actualizaciones**.
3. En **Configuración del Servidor de actualizaciones** puede consultar y configurar los ajustes principales.
   - **Dirección de paquetes.** La dirección desde la que se descargan los paquetes.
   - **Dirección de Actualización.** El Servidor de actualizaciones está configurado para consultar y descargar actualizaciones desde `upgrade.bitdefender.com:80`. Se trata de una dirección genérica que resuelve automáticamente al servidor más cercano que almacena actualizaciones de Bitdefender en su región.
   - **Puerto.** Cuando se configuran los diversos componentes GravityZone para actualizarse desde el Servidor de actualización, debe proporcionarse este puerto. El puerto predeterminado es `7074`.
   - **IP.** La dirección IP del Servidor de actualizaciones.

- **Periodo de actualización (horas).** Si desea cambiar el periodo de actualización, escriba un nuevo valor en este campo. El valor por defecto es 1.

4. Puede configurar el Servidor de actualizaciones para que descargue automáticamente los kits de endpoints y Security Server.
5. El Servidor de actualizaciones de Bitdefender puede actuar como puerta de enlace para los datos enviados por los productos cliente de Bitdefender instalados en la red a los servidores de Bitdefender. Estos datos pueden incluir informes anónimos con respecto a la actividad de virus, informes de bloqueos del producto y datos utilizados para el registro online. Activar los roles de la puerta de enlace es muy útil para el control del tráfico y en redes sin acceso a Internet.

   Nota
   Puede desactivar los módulos del producto y enviar datos estadísticos o de bloqueos al laboratorio de Bitdefender siempre que lo desee. Puede utilizar políticas para controlar remotamente estas opciones en los equipos y máquinas virtuales gestionadas por Control Center.

6. Haga clic en **Guardar**.

6.3. Descarga de actualizaciones de productos

Puede consultar información sobre los paquetes de componentes de GravityZone existentes en la pestaña **Componentes**. La información disponible incluye versiones actuales, versiones de actualización (si las hubiera) y el estado de operaciones de actualización que haya iniciado.

Para actualizar un componente GravityZone:

1. Acceda a la página **Actualizar** en Control Center y haga clic en la pestaña **Componentes**.
2. Haga clic en el componente que desee actualizar en la lista **Producto**. En la tabla **Paquetes** se mostrarán todas las versiones disponibles. Marque la casilla de verificación correspondiente a la versión que desee descargar.

Nota
Los nuevos paquetes estarán en el estado **No descargado**. En cuanto Bitdefender publique una nueva versión, se eliminará de la tabla la versión más antigua no descargada.

3. Haga clic en **Acciones** en la zona superior de la tabla y seleccione **Publicar**. Se descargará la versión seleccionada y cambiará el estado en consecuencia. Actualice los contenidos de la tabla haciendo clic en el botón **Actualizar** y compruebe el estado correspondiente.

Importante
El appliance GravityZone no incluye de forma predeterminada los paquetes Security Server. Debe descargar de forma manual los paquetes Security Server necesarios para su entorno.

6.4. Ensayo de actualizaciones

El ensayo permite probar los kits o actualizaciones de productos más recientes en un entorno cerrado y controlado antes de que se publiquen en la red. El entorno de ensayo debe reflejar el de producción de la forma más fiel posible al realizar las pruebas. Gracias a ello, aumentan las posibilidades de encontrar cualquier problema que pueda surgir en su entorno antes de poner la versión en producción.

Los ensayos también le permiten crear una política para los endpoints críticos en producción. Puede actualizar estos endpoints solo después de haber probado los cambios en el entorno de ensayo y en las máquinas que no sean críticas para producción. Para obtener más información, consulte “Publicación con anillos de actualización” (p. 202).

Nota
- El ensayo está desactivado por defecto.
- Security Server (VMware con NSX) no admite ensayos.
- BEST for Windows Legacy no es compatible con ensayos. Los endpoints antiguos en ubicaciones de ensayo deben moverse a la ubicación de producción.

6.4.1. Requisitos

El modo de ensayo requiere que la infraestructura de GravityZone cumpla con las siguientes condiciones:

- El Servidor de actualizaciones debe instalarse en solitario en el dispositivo virtual.

  Si tiene el Servidor de actualizaciones junto con otros roles en el appliance, debe seguir estos pasos:

  1. Elimine el rol de Servidor de actualizaciones antiguo.
  2. Implemente un nuevo appliance GravityZone.

     Importante
     No instale ningún rol todavía.

  3. Conecte el nuevo appliance a la base de datos de GravityZone existente.
  4. Instale el rol de Servidor de actualizaciones en el nuevo appliance.

  Para obtener más información sobre la instalación de los roles de GravityZone, consulte "Administrar el appliance GravityZone" (p. 109).
- El appliance del Servidor de actualizaciones debe ser al menos de 120 GB.
- El appliance de la consola Web debe ser al menos de 120 GB.

6.4.2. Uso de los ensayos

Para configurar el entorno de ensayos y probar las últimas actualizaciones necesita:

1. Habilitar los ensayos y definir los ajustes del servidor de actualizaciones.
2. Definir una política de ensayos para los endpoints de prueba.
3. Instalar los paquetes en los endpoints de prueba.
4. Asignar la política de ensayos a los endpoints de prueba.
5. Actualizar los endpoints de prueba a la versión más reciente y probar la actualización en el entorno de ensayos.
6. Ejecutar una segunda prueba antes de actualizar todos los endpoints de producción. Puede probar primero la actualización en los endpoints que no sean críticos.

Activación de ensayos

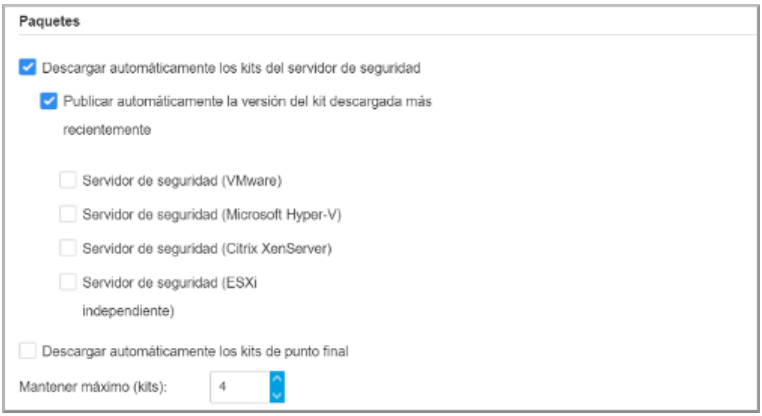
Para activar el modo de ensayos para las actualizaciones de GravityZone:

1. Acceda a la página **Configuración** > **Actualizar** y haga clic en la pestaña **Componentes**.
2. Haga clic en el botón **Ajustes** de la zona superior del panel de la izquierda para mostrar la ventana **Ajustes del Servidor de actualizaciones**.
3. Marque la casilla de verificación **Activar ensayos**.
4. En **Configuración del servidor de producción**, configure los ajustes principales:
   - **Dirección de paquetes.** La dirección desde la que se descargan los paquetes: `download.bitdefender.com/SMB/Hydra/release`
   - **Dirección de Actualización.** La dirección desde la que se descargan las actualizaciones de productos: `upgrade.bitdefender.com:80`.
   - **Puerto.** El puerto predeterminado es `7074`. No puede modificar este campo.
   - **IP.** La dirección IP del Servidor de actualizaciones. No puede modificar este campo.
   - **Periodo de actualización (horas).** Si desea cambiar el periodo de actualización, escriba un nuevo valor en este campo. El valor por defecto es 1.
5. Los servidores de actualizaciones y de producción pueden actuar como puertas de enlace para los datos enviados por los productos cliente de Bitdefender instalados en la red a los servidores de Bitdefender. Estos datos pueden incluir informes anónimos con respecto a la actividad de virus, informes de bloqueos del producto y datos utilizados para el registro online. Activar los roles de la puerta de enlace es muy útil para el control del tráfico y en redes sin acceso a Internet.

   Nota
   Puede desactivar los módulos del producto y enviar datos estadísticos o de bloqueos al laboratorio de Bitdefender siempre que lo desee. Puede utilizar políticas para controlar remotamente estas opciones en los equipos y máquinas virtuales gestionadas por Control Center.

6. En **Configuración del servidor de ensayo**, configure los siguientes ajustes:
   - **Puerto.** El puerto por defecto es el `7077`.
   - **IP.** La dirección IP del Servidor de actualizaciones. No puede modificar este campo.

7. En **Paquetes**, puede configurar el Servidor de actualizaciones para que descargue y publique automáticamente los kits de endpoints y Security Server.



Paquetes - Publicar automáticamente

También puede configurar el número máximo de kits que se pueden almacenar en el appliance GravityZone. Introduzca un número entre 4 y 10 en el menú **Mantener máximo (kits)**.

8. En **Actualización de productos** puede configurar el Servidor de actualizaciones para que descargue automáticamente las actualizaciones de los agentes de seguridad.

Paquetes - Publicar automáticamente

Puede optar por publicar automáticamente también las versiones descargadas más recientes:

a. Seleccione al menos un agente de seguridad de la lista a su disposición.

b. Defina los anillos de fuente y destino:

- **Anillo de fuente**. El anillo que se utiliza para enviar las actualizaciones en el entorno de ensayo. Cuando una versión haya sido validada por sus primeros usuarios, se publicará en el anillo lento. Este es el valor por defecto. Las actualizaciones más recientes disponibles se publicarán en el anillo rápido.
- **Anillo de destino**. El anillo utilizado para publicar las actualizaciones en producción. Puede elegir entre rápido y lento.

También puede configurar el número máximo de actualizaciones que se pueden almacenar en el appliance GravityZone. Introduzca un número entre 4 y 10 en el menú **Mantener máximo (actualizaciones)**.

9. Haga clic en **Guardar**.

Una vez activados los ensayos, cree su entorno de ensayo para empezar a probar las actualizaciones y kits de productos disponibles.

Importante
Desactivar los ensayos eliminará todas las actualizaciones de productos y paquetes no publicados.

Definición de la política de ensayos

Es necesario definir una política de ensayos:

1. Diríjase a la página **Políticas**.
2. Seleccione o cree una política para su uso en el entorno de pruebas.
3. En la sección **General** > **Actualización**, introduzca la dirección del servidor de ensayo en la tabla de **Ubicaciones de actualización**.
4. Configure los otros ajustes de la política según sea preciso. Para más información, consulte el capítulo **Políticas de seguridad** de la Guía del administrador de GravityZone.
5. Haga clic en **Guardar**.

Paquetes de ensayo

Para instalar el último paquete en los endpoints de prueba:

1. Acceda a la página **Configuración > Actualizar** y seleccione la pestaña **Componentes**.
2. Haga clic en **Buscar actualizaciones** para asegurarse de que está viendo la versión del producto publicada más recientemente.
3. Haga clic en el componente que desee actualizar en la lista **Producto**.
4. Seleccione un paquete disponible en la tabla **Paquetes** que desee probar. Puede descargar varios kits para cada producto, hasta el límite especificado en la ventana **Ajustes del Servidor de actualizaciones**. Cuando se alcanza ese límite, se elimina de la tabla la versión más antigua.
5. Haga clic en **Acciones** y seleccione **Descargar** para llevar el paquete a su appliance GravityZone.
6. Con el paquete seleccionado, haga clic en **Guardar en el disco**. Se muestra la ventana de configuración del paquete.
7. Configure el paquete. Para más información, diríjase a “Crear paquetes de instalación” (p. 141).
8. Instale el kit en los endpoints de prueba.
9. Monitorice el comportamiento de los endpoints.

10. Si el paquete se ha instalado correctamente y los endpoints presentan un comportamiento normal, puede publicar el paquete en la red de producción.

    Para publicar un paquete, selecciónelo en la tabla **Paquetes**, haga clic en **Acciones** en la parte superior de la tabla y seleccione **Publicar**.

    Importante
    No es posible publicar paquetes más antiguos que el que ya esté publicado.

11. Si ha tenido problemas con el paquete, puede abrir un ticket de soporte. Para obtener más información, consulte "Obtener Ayuda" (p. 225).

    Para eliminar un paquete del appliance GravityZone, haga clic en el botón **Acciones** y seleccione **Eliminar del disco**.

Asignación de la política de ensayos

Para asignar la política de ensayos a los endpoints de prueba:

1. Diríjase a la página **Red**.
2. Elija **Equipos y máquinas virtuales** en el selector de vistas.
3. Seleccione el grupo que desee del panel de la izquierda. Todos los equipos del grupo seleccionado se muestran en la tabla del panel lateral derecho.
4. Marque la casilla de verificación del equipo o grupo que desee. Puede seleccionar uno o varios objetos del mismo tipo solamente desde el mismo nivel.
5. Haga clic en el botón **Asignar política** de la zona superior de la tabla.
6. Haga los ajustes necesarios en la ventana de Asignación de política. Para obtener más información, consulte el capítulo de **Políticas de seguridad > Administración de políticas > Asignación de políticas a los endpoints** de la Guía del administrador de GravityZone.

Ensayo de actualizaciones de productos

Para instalar las últimas actualizaciones:

1. Acceda a la página **Configuración > Actualizar** y seleccione la pestaña **Componentes**.
2. Haga clic en **Buscar actualizaciones** para asegurarse de que está viendo la actualización del producto publicada más recientemente.

3. Seleccione el producto de Bitdefender que desee en la lista **Producto**.

   Nota
   Solo puede utilizar los ensayos con actualizaciones de agentes de seguridad y no para los Security Server.

4. Seleccione una actualización disponible en la tabla **Actualizaciones** que desee probar.
5. Haga clic en **Acciones** y seleccione **Descargar** para llevar la actualización a su appliance GravityZone.

   Puede descargar varias actualizaciones para cada producto, hasta el límite especificado en la ventana **Ajustes del Servidor de actualizaciones**. Cuando se alcanza ese límite, se elimina de la tabla la versión más antigua.
6. Con una actualización seleccionada, haga clic en **Acciones** y seleccione **Añadir al ensayo**. La actualización se instalará en los endpoints de prueba, de acuerdo con los ajustes de política. Para obtener más información, consulte "Definición de la política de ensayos" (p. 200).
7. Si la actualización se ha instalado correctamente y los endpoints presentan un comportamiento normal, empiece a enviar la actualización a las máquinas en producción. En primer lugar, actualice las máquinas que no sean críticas, para ejecutar otra prueba antes de actualizar los endpoints críticos. Para obtener más información, consulte "Publicación con anillos de actualización" (p. 202).
8. Si ha tenido problemas con la actualización, puede abrir un ticket de soporte. Para obtener más información, consulte "Obtener Ayuda" (p. 225).

   Para eliminar una actualización sin publicar del appliance GravityZone, haga clic en el botón **Acciones** y seleccione **Eliminar**. Solo puede eliminar las actualizaciones sin publicar.

Publicación con anillos de actualización

Para probar la actualización en los endpoints que no sean críticos para la producción, debe editar primero las políticas existentes y asignarles una política de anillo rápido.

Nota
Automáticamente, se asigna una política de anillo lento a todas las políticas que crea.

1. Diríjase a la página **Políticas**.
2. Modifique el ajuste de política para los endpoints que no son críticos en producción. En la sección de **Anillo de actualización** seleccione **Anillo rápido**.

   Nota
   La actualización publicada en el anillo rápido no puede ser más antigua que la publicada en el anillo lento.

3. Publique la actualización en el anillo rápido:
   a. Acceda a la página **Configuración** > **Actualizar** y seleccione la pestaña **Componentes**.
   b. Seleccione la actualización en la tabla de Actualizaciones, haga clic en el botón **Acciones** de la zona superior de la tabla y elija **Publicar**.
   c. Seleccione la opción de anillo rápido.

      Nota
      Cuando publique una actualización por primera vez, estará disponible en el anillo rápido y en el lento.

      En este momento, todos los endpoints con política de anillo rápido se actualizan a la versión publicada.
4. Monitorice el comportamiento de los endpoints del anillo rápido.
5. Si la actualización se ha instalado correctamente y los endpoints presentan un comportamiento normal, puede publicar la actualización en el anillo lento:
   a. Acceda a la página **Configuración** > **Actualizar** y seleccione la pestaña **Componentes**.
   b. Seleccione la actualización en la tabla de Actualizaciones, haga clic en el botón **Acciones** de la zona superior de la tabla y elija **Publicar**.
   c. Seleccione la opción de anillo lento.

      Todos los endpoints de producción se actualizan ahora a la versión que ha publicado.
6. Si ha tenido problemas con el paquete, puede abrir un ticket de soporte. Para obtener más información, consulte “Obtener Ayuda” (p. 225).

6.5. Actualizaciones de productos sin conexión

GravityZone utiliza por defecto un sistema de actualización con conexión a Internet. Para redes aisladas, Bitdefender ofrece una alternativa para que las actualizaciones de contenidos de seguridad y componentes estén también disponibles sin conexión.

6.5.1. Requisitos

Para utilizar las actualizaciones sin conexión, necesita:

- Una instancia de GravityZone instalada en una red con acceso a Internet ("instancia online"). La instancia online debe tener:
  - Acceso directo a Internet
  - Acceso a los puertos 80 y 443. Para obtener más información sobre los puertos utilizados por GravityZone, consulte este artículo de la base de conocimientos.
  - Solo los roles de Base de datos y de Servidor de actualizaciones instalados
- Una o varias instancias de GravityZone instaladas en una red sin acceso a Internet ("instancias sin conexión").
- Ambas instancias de GravityZone deben tener la misma versión del appliance.

6.5.2. Preparación de la instancia online de GravityZone

Durante esta fase, implementará una instancia de GravityZone en una red con acceso a Internet y luego la configurará para que actúe como Servidor de actualizaciones sin conexión.

1. Implemente GravityZone en una máquina con conexión a Internet.
2. Instale solo los roles de Base de datos y de Servidor de actualizaciones.
3. Acceda al terminal TTY de la máquina en su entorno virtual (o conéctese mediante SSH).
4. Inicie sesión con el usuario `bdadmin` y la contraseña que haya establecido.
5. Ejecute el comando `sudo su` para obtener privilegios de **root**.
6. Ejecute los siguientes comandos para instalar el paquete `gzou-mirror` sin conexión:

```
# apt update # gzcli update # apt install gzou-mirror
```

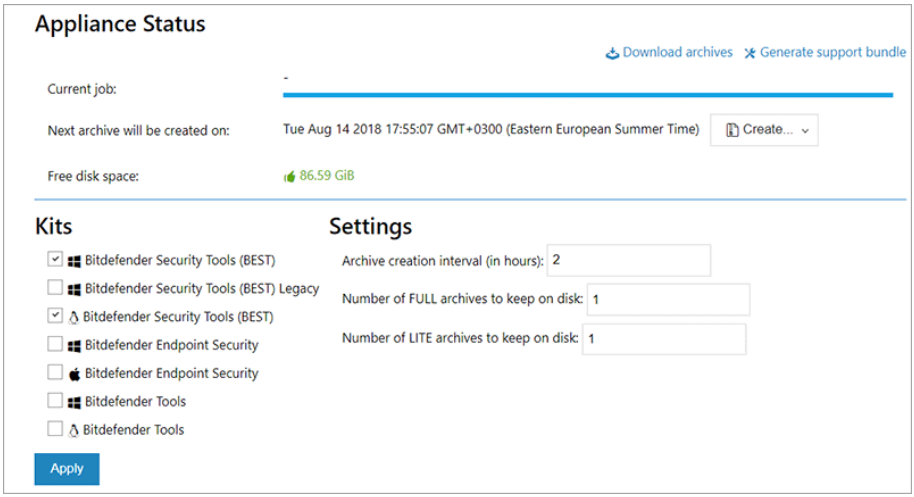
El paquete `gzou-mirror` tiene los siguientes roles:

- Configure el Servidor de actualizaciones para generar automáticamente archivos de actualización sin conexión.
- Configure un servicio web para la instancia online proporcionando opciones de configuración y descarga para los archivos de actualización sin conexión.

6.5.3. Configuración y descarga de los archivos de actualización iniciales

Durante esta fase, configurará los ajustes de archivos de actualizaciones a través del servicio web instalado en la instancia online y, luego, creará los archivos de almacenamiento necesarios para configurar la instancia sin conexión. Posteriormente, tendrá que descargar los archivos de actualización y ponerlos en un dispositivo de multimedia portátil (memoria USB).

1. Acceda al servicio web a través de una URL de esta forma: `https://Nombre-de-host-o-IP-del-Servidor-de-actualizaciones-de-la-instancia-online`, con el nombre de usuario `bdadmin` y la contraseña que haya establecido.



La instancia online - Servicio web

2. Configure el archivo de actualización sin conexión de la siguiente manera:
   - En **Kits**, seleccione los kits de agente de endpoint que desea incluir en el archivo de actualización sin conexión.
   - En **Ajustes**, edite las preferencias de su archivo de actualización.

     Una tarea programada (CRON) instalada en la instancia online comprobará cada minuto si hay nuevos archivos de actualización disponibles y si el espacio libre en el disco es superior a 10 GB. En cada período establecido por la opción **Intervalo de creación de archivos (en horas)**, la tarea programada (CRON) creará los siguientes archivos:

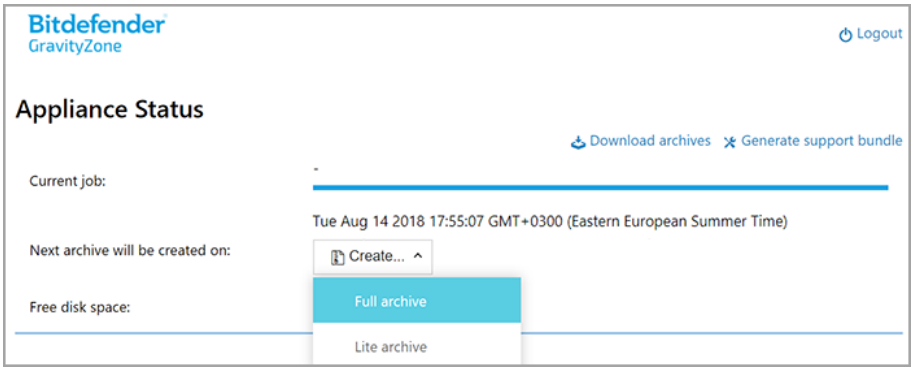
     – **Archivo completo (producto y contenidos de seguridad)**, cuando hay nuevos archivos de actualización disponibles

     – **Archivo reducido** (solo contenidos de seguridad), cuando no hay nuevos archivos de actualización

     Los archivos se crearán en la siguiente ubicación:

     https://Nombre-de-host-o-IP-del-Servidor-de-actualizaciones-de-la-instancia-online/snapshots

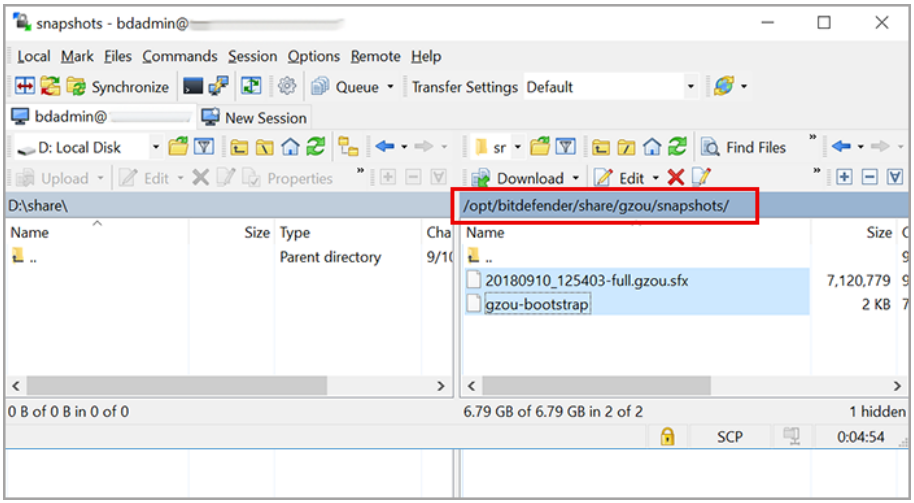
3. Haga clic en **Crear > Archivo completo** para crear el primer archivo completo. Espere hasta que se cree el archivo.



La instancia online - Servicio web: Creación del archivo

4. Descargue el archivo de actualización completo y el archivo `gzou-bootstrap` de la instancia online. Dispone de varias opciones:
   - A través del servicio web: Haga clic en **Descargar archivos** para acceder a la página que contiene los enlaces a los archivos de actualización. Haga clic en los enlaces al archivo de actualización completo y al archivo `gzou-bootstrap` para descargarlos en su endpoint.
   - Utilice el cliente SCP/SCTP que prefiera (WinSCP, por ejemplo) para establecer una sesión SCP con la instancia online y transferir los archivos mencionados anteriormente a cualquier ubicación de su red online. La ruta por defecto en la instancia online es:

     `/opt/bitdefender/share/gzou/snapshots`



Transferencia de archivos de actualización mediante SCP

- A través de un recurso compartido de SAMBA. Utilice un recurso compartido de SAMBA de solo lectura para recuperar los archivos de actualización sin conexión desde la siguiente ubicación:

  `\\Nombre-de-host-o-IP-del-Servidor-de-actualizaciones-de-la-instancia-online\gzou-snapshots`

  Nota
  Las credenciales para acceder al recurso compartido de SAMBA, si se solicitan, son las mismas que las de la instancia online (usuario `bdadmin` y contraseña).

6.5.4. Preparación de la instancia sin conexión de GravityZone

Durante este paso, implementará y configurará la instancia sin conexión para recibir actualizaciones a través de los archivos generados por la instancia online. A menos que se indique lo contrario, hay que ejecutar todos los comandos como **root**.

1. Implemente GravityZone en una máquina desde un entorno aislado.
2. Instale solo los roles de Base de datos y de Servidor de actualizaciones.

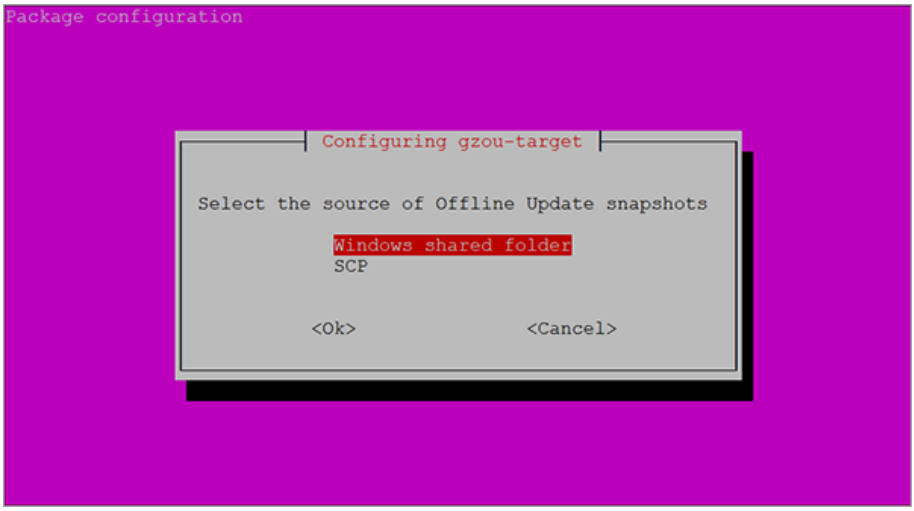
3. Transfiera el archivo de actualización y el archivo `gzou-bootstrap` descargados de la instancia online al `directorio /home/bdadmin` de la instancia sin conexión mediante un dispositivo de multimedia portátil (memoria USB).

   Importante
   Para que funcione la actualización sin conexión, asegúrese de lo siguiente:
   - El archivo de actualización y el archivo `gzou-bootstrap` están en la misma carpeta.
   - El archivo de actualización es un archivo **completo**.

4. Ejecute el archivo `gzou-bootstrap` de la siguiente manera:
   a. Acceda al terminal TTY de la máquina en su entorno virtual (o conéctese mediante SSH).
   b. Transformar `gzou-bootstrap` en un archivo ejecutable:

   ```
   #
   chmod +x gzou-bootstrap
   ```

   c. Ejecutar: `./gzou-bootstrap`
5. Elija el método de transferencia de los archivos de actualización a la instancia sin conexión:
   - Seleccione la **carpeta compartida de Windows** (recurso compartido de Samba). En este caso, deberá especificar la ruta a un recurso compartido de Windows desde la red aislada, donde la instancia sin conexión se conectará automáticamente para recuperar los archivos de actualización. Introduzca las credenciales requeridas para acceder a la ubicación especificada.
   - Seleccione SCP si va a transferir manualmente los archivos a la carpeta `/opt/bitdefender/share/gzou/snapshots/` de la instancia sin conexión a través de SCP.



Instancia GravityZone sin conexión - Configuración del modo de transferencia de los archivos de actualización

Nota
Si desea cambiar el método de transferencia más adelante:

a. Acceda al terminal TTY de la instancia sin conexión en su entorno virtual (o conéctese mediante SSH).
b. Inicie sesión con el usuario `bdadmin` y la contraseña que haya establecido.
c. Ejecute el comando `sudo su` para obtener privilegios de root.
d. Ejecute:

```
# rm -f /opt/bitdefender/etc/gzou-target.json # dpkg-recon
```

Aparecerá el cuadro de diálogo de configuración, donde puede realizar los cambios que desee.

6. Pase a la línea de comandos de la consola de GravityZone sin conexión e instale el resto de los roles.

7. Acceda a la consola sin conexión desde su navegador e introduzca su clave de licencia (en el modo sin conexión).

6.5.5. Uso de las actualizaciones sin conexión

Una vez que haya configurado las instancias de GravityZone, siga estos pasos para actualizar su instalación sin conexión:

1. Descargue el último archivo de actualización sin conexión de la instancia online al recurso compartido de red que prefiera. Para obtener más información, consulte "Configuración y descarga de los archivos de actualización iniciales" (p. 205).
2. Utilice una memoria USB para transferir el archivo de actualización al recurso compartido de Samba configurado desde la red aislada. Para obtener más información, consulte "Preparación de la instancia sin conexión de GravityZone" (p. 208).

   Los archivos se extraerán automáticamente en el siguiente directorio de la instancia sin conexión:

   ```
   /opt/bitdefender/share/gzou/snapshots/
   ```

6.5.6. Uso de la consola web

Acceda a la consola web introduciendo la IP o el nombre de host del appliance en el navegador web. Puede modificar las opciones disponibles:

- Centro de control
- Configuración general

Centro de control

El **Estado del appliance** muestra la información de la última tarea realizada (tipo de archivo, fecha y hora), y la siguiente tarea programada.

Tiene la opción de:

- **Crear archivos de contenidos de seguridad**
- **Crear un archivo completo**

En la sección **Archivos creados**, puede descargar tanto archivos de contenidos de seguridad como completos.

Seleccione los archivos de la lista disponible y haga clic en el botón **Descargar**.

También puede ver el espacio disponible en el disco del appliance.

Configuración general

Puede definir una programación de descarga para los kits de GravityZone.

1. Haga clic en el botón **Editar configuración**.
2. Seleccione uno o más kits de la lista de **Kits disponibles**.
3. En la sección **Programación**, puede definir un intervalo para la creación de los archivos, así como el número archivos que desea conservar en el disco.
4. Haga clic en el botón **Aplicar** para guardar sus cambios.

7. DESINSTALACIÓN DE LA PROTECCIÓN

Puede desinstalar y volver a instalar los componentes de GravityZone en ciertos casos, como cuando necesite utilizar una clave de licencia para otra máquina, para corregir errores o cuando se actualice.

Para desinstalar correctamente la protección de Bitdefender de los endpoints de su red, siga las instrucciones descritas en este capítulo.

- Desinstalación de la protección en endpoints
- Desinstalación de HVI
- Desinstalación de la Protección de Exchange
- Desinstalación de la protección para dispositivos móviles
- Desinstalación de Sandbox Analyzer On-Premises
- Desinstalación del Generador de informes
- Desinstalar roles de servidor de GravityZone

7.1. Desinstalación de la protección en endpoints

Para eliminar de forma segura la protección de Bitdefender, primero tiene que desinstalar los agentes de seguridad y, luego, Security Server, si es preciso. Si desea desinstalar solo el Security Server, asegúrese de conectar antes sus agentes a otro Security Server.

- Desinstalación de los agentes de seguridad
- Desinstalación de Security Server

7.1.1. Desinstalación de los agentes de seguridad

Tiene dos opciones para desinstalar los agentes de seguridad:

- Remotamente en Control Center
- Manualmente en la máquina objetivo

Aviso
Los agentes de seguridad y los servidores de seguridad son esenciales para mantener los endpoints a salvo de cualquier amenaza, por lo que desinstalarlos puede poner en peligro toda la red.

Desinstalación remota

Para desinstalar la protección de Bitdefender de cualquier endpoint administrado de forma remota:

1. Acceda a la página **Red**.
2. Elija **Equipos y máquinas virtuales** en el selector de vistas.
3. Seleccione el contenedor que desee del panel de la izquierda. Todos los equipos del contenedor seleccionado se muestran en la tabla del panel de la derecha.
4. Seleccione los endpoints de los que desea desinstalar el agente de seguridad de Bitdefender.
5. Haga clic en **Tareas**, en la zona superior de la tabla, y elija **Desinstalar cliente**. Se muestra una ventana de configuración.
6. En la ventana de la tarea **Desinstalar agente** puede elegir si desea conservar los archivos en cuarentena en el endpoint o borrarlos.

   En el caso de entornos integrados vShield, debe seleccionar las credenciales necesarias para cada máquina, pues de lo contrario fallará la desinstalación. Seleccione **Usar credenciales para integración vShield** y, a continuación, añada los datos necesarios en la tabla del Gestor de credenciales que se muestra debajo.
7. Haga clic en **Guardar** para crear la tarea. Aparecerá un mensaje de confirmación.

Puede ver y administrar la tarea en **Red > Tareas**.

Si desea volver a instalar los agentes de seguridad, consulte "Instalación de la protección de endpoints" (p. 126).

Desinstalación local

Para desinstalar manualmente el agente de seguridad de Bitdefender de una máquina con Windows:

1. Dependiendo de su sistema operativo:
   - En Windows 7, acceda a **Inicio > Panel de control > Desinstalar un programa** en la categoría **Programas**.
   - En Windows 8, acceda a **Configuración > Panel de control > Desinstalar un programa** en la categoría **Programas**.

- En Windows 8.1, haga clic con el botón derecho en el botón **Inicio** y, a continuación, seleccione **Panel de control > Programas y características**.
- En Windows 10, acceda a **Inicio > Configuración > Sistema > Aplicaciones y características**.

2. En la lista de programas, seleccione el agente de Bitdefender que desee.
3. Haga clic en **Desinstalar**.
4. Introduzca la contraseña de Bitdefender, en caso de que se hubiese habilitado en la política de seguridad. Durante la desinstalación, puede ver el progreso de la tarea.

Para desinstalar manualmente el agente de seguridad de Bitdefender de una máquina con Linux:

1. Abra el terminal.
2. Obtenga acceso root mediante los comandos `su` o `sudo su`.
3. Desplácese mediante el comando `cd` hasta la siguiente ruta: `/opt/BitDefender/bin`
4. Ejecute el script:

```
# ./remove-sve-client
```

5. Introduzca la contraseña de Bitdefender para continuar, en caso de que se hubiese habilitado en la política de seguridad.

Para desinstalar manualmente el agente de Bitdefender de un Mac:

1. Acceda a **Finder > Aplicaciones**.
2. Abra la carpeta Bitdefender.
3. Haga doble clic en **Desinstalación de Bitdefender para Mac**.
4. En la ventana de confirmación, haga clic en **Comprobar** y **Desinstalar** para continuar.

Si desea volver a instalar los agentes de seguridad, consulte “Instalación de la protección de endpoints” (p. 126).

7.1.2. Desinstalación de Security Server

Puede desinstalar Security Server de la misma manera que se instaló, ya sea desde Control Center o desde la interfaz de menú del appliance virtual GravityZone.

Para desinstalar Security Server en Control Center:

1. Diríjase a la página **Red**.
2. Seleccione **Máquinas virtuales** desde el selector de vistas.
3. Seleccione el centro de datos o carpeta que contiene el host en el que se ha instalado el Security Server . Los endpoints se muestran en el panel de la derecha.
4. Marque la casilla de verificación correspondiente al host en que está instalado el Security Server.
5. En el menú **Tareas**, seleccione **Desinstalar Security Server**.
6. Introduzca las credenciales de vShield (si procede) y haga clic en **Sí** para crear la tarea.

Puede ver y administrar la tarea en **Red > Tareas**.

Cuando Security Server está instalado en el mismo appliance virtual que los otros roles de GravityZone, puede eliminarlo mediante la interfaz de línea de comandos del appliance. Siga estos pasos:

1. Acceda a la consola del appliance desde su herramienta de administración de la virtualización (por ejemplo, vSphere Client).

   Utilice las teclas de flecha y la tecla `Tabulador` para navegar por los menús y opciones. Pulse `Intro` para seleccionar una opción específica.
2. En el menú **Opciones del appliance**, acceda a **Configuración avanzada**.
3. Seleccione **Desinstalar Servidor de seguridad**. Se muestra una ventana de confirmación.
4. Pulse la tecla `S`, o pulse `Intro` mientras tiene la opción **Sí** seleccionada para continuar. Espere hasta que finalice la desinstalación.

7.2. Desinstalación de HVI

Para desinstalar HVI de un host, es suficiente con desinstalar el paquete suplementario de HVI. Puede seguir utilizando el Security Server como servidor de

análisis siempre y cuando tenga una clave de licencia válida para Security for Virtualized Environments.

Si desea eliminar Bitdefender por completo, tiene que desinstalar tanto el paquete suplementario de HVI como Security Server.

Desinstalación del paquete suplementario de HVI

Tiene dos opciones para eliminar el paquete suplementario:

- Remotamente desde Control Center, mediante la ejecución de una tarea de desinstalación.
- Remotamente desde XenCenter, mediante la ejecución de un par de comandos en el host objetivo.

Para eliminar el paquete de HVI desde Control Center:

1. Iniciar sesión en Control Center.
2. Acceda a la página **Red** y seleccione **Máquinas virtuales** en el selector de vistas.
3. Seleccione **Servidor** en el menú de **Vistas** del panel izquierdo.
4. Seleccione uno o más hosts Xen del inventario de red. Puede ver fácilmente los hosts disponibles seleccionando la opción **Tipo > Hosts** en el menú **Filtros**.
5. Haga clic en el botón **Tareas** del panel derecho y seleccione **Desinstalar el paquete suplementario de HVI**. Se abre la ventana de configuración.
6. Programe cuándo eliminar el paquete. Puede optar por ejecutar la tarea inmediatamente después de guardarla, o en un momento determinado. En caso de que no se pueda completar la desinstalación en el momento especificado, la tarea se repite automáticamente según los ajustes de recurrencia. Por ejemplo, si selecciona varios hosts y uno no está disponible cuando esté programada la desinstalación del paquete, la tarea se ejecutará de nuevo a la hora especificada.
7. Se debe reiniciar el host para completar la eliminación. Si desea que el host se reinicie de forma desatendida, seleccione **Reiniciar automáticamente (si es necesario)**.
8. Haga clic en **Guardar**. Aparecerá un mensaje de confirmación.

   Puede ver y administrar las tareas en la página **Red > Tareas**.

Para eliminar el paquete de HVI desde XenCenter:

1. Inicie sesión en XenCenter.
2. Abra la consola del host Xen.
3. Introduzca la contraseña para el host XenServer.
4. Ejecute los siguientes comandos:

```
# rpm -ebitdefender-xen-dom0 # rm -rf /etc//xensource/installed-
  /bitdefender\:bitdefender-hvi/ # rm -rf/opt/bitdef* # servicio
```

Desinstalación de Security Server

Para desinstalar Security Server en uno o varios hosts:

1. Iniciar sesión en Control Center.
2. Diríjase a la página **Red**.
3. Seleccione **Máquinas virtuales** desde el selector de vistas.
4. Examine el inventario Citrix y marque las casillas de selección correspondientes a los contenedores o hosts deseados. Para una selección rápida, puede filtrar el inventario de red para ver solamente los Security Server.
5. Haga clic en el botón **Tareas** de la zona superior de la tabla y seleccione **Desinstalar Security Server** en el menú. Aparecerá un mensaje de confirmación. Haga clic en **Sí** para continuar.

Puede ver y administrar las tareas en la página **Red > Tareas**.

7.3. Desinstalación de la Protección de Exchange

Puede eliminar la Protección de Exchange de cualquier servidor de Microsoft Exchange que tenga Bitdefender Endpoint Security Tools con este rol instalado. Puede realizar la desinstalación en Control Center.

1. Diríjase a la página **Red**.
2. Elija **Equipos y máquinas virtuales** en el selector de vistas.
3. Seleccione el contenedor que desee del panel de la izquierda. Se mostrarán las entidades en la tabla del panel derecho.
4. Seleccione el endpoint del que desea desinstalar la Protección de Exchange.

5. Haga clic en **Reconfigurar el cliente** en el menú **Tareas**, en el panel superior de la tabla. Se muestra una ventana de configuración.
6. En la sección **General**, deje sin marcar la casilla de verificación **Protección de Exchange**.

   Aviso
   En la ventana de configuración, asegúrese de haber seleccionado todos los demás roles activos en el endpoint. De lo contrario, se desinstalarán también.

7. Haga clic en **Guardar** para crear la tarea.

Puede ver y administrar la tarea en **Red > Tareas**.

Si desea volver a instalar la Protección de Exchange, consulte "Instalación de la Protección de Exchange" (p. 171).

7.4. Desinstalación de Sandbox Analyzer On-Premises

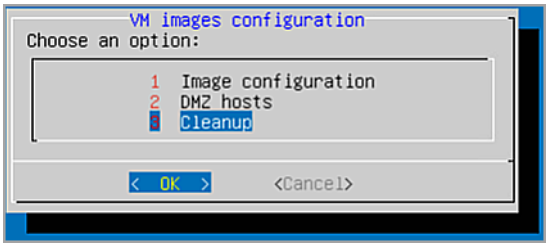
Para desinstalar Sandbox Analyzer On-Premises:

1. Elimine las imágenes de máquinas virtuales (VM) de la consola del appliance Sandbox Analyzer.
   a. Inicie sesión en la interfaz del appliance Sandbox Analyzer.

      Utilice las teclas de flecha y la tecla `Tabulador` para navegar por los menús y opciones.

      Pulse `Intro` para seleccionar una opción específica.

   b. En el menú de **Configuración del espacio aislado**, vaya a la opción de **Imágenes de máquinas virtuales**.
   c. En el menú de **Configuración de imágenes de máquinas virtuales**, vaya a la opción de **Limpieza**.



Consola del appliance Sandbox Analyzer - Configuración del espacio aislado - Limpieza

d. Confirme que desea eliminar las imágenes de máquinas virtuales instaladas.

   Espere a que finalice esta acción. Durante esta acción, también se eliminarán los datos asociados con las imágenes de las máquinas virtuales.

2. Elimine el appliance virtual Sandbox Analyzer:
   a. Apague el appliance virtual Sandbox Analyzer.
   b. Elimine el appliance del inventario de ESXi.

7.5. Desinstalación de la protección para dispositivos móviles

Para eliminar la protección de Bitdefender de un dispositivo móvil, necesita hacerlo tanto en Control Center como en el dispositivo.

Cuando elimina un dispositivo de Control Center:

- Se desvincula GravityZone Mobile Client, pero no se elimina del dispositivo.
- Todos los registros relacionados con el dispositivo eliminado siguen estando disponibles.
- Su información personal y sus aplicaciones no se ven afectados.
- En los dispositivos iOS, se elimina el perfil MDM. Si el dispositivo no está conectado a Internet, el perfil MDM permanece instalado hasta que haya una nueva conexión disponible.

Aviso

- No puede restaurar los dispositivos móviles eliminados.

- Antes de la eliminación, asegúrese de que el dispositivo objetivo no está bloqueado. Si elimina accidentalmente un dispositivo bloqueado, tendrá que reestablecer los ajustes de fábrica en el dispositivo para desbloquearlo.

1. Diríjase a la página **Red**.
2. Seleccione **Dispositivos móviles** en el selector de vistas.
3. Haga clic en **Filtros** en la zona superior del panel de red y seleccione **Dispositivos** en la categoría **Ver**. Haga clic en **Guardar**.
4. Seleccione el contenedor que desee del panel de la izquierda. Todos los dispositivos se muestran en la tabla del panel de la derecha.
5. Marque la casilla de verificación del dispositivo del cual desee eliminar la protección.
6. Haga clic en ⊖ **Eliminar** en la zona superior de la tabla.

A continuación, tiene que desinstalar el software del dispositivo.

Para desinstalar la protección de Bitdefender de un dispositivo Android:

1. Acceda a **Seguridad > Administradores del dispositivo**.
2. Deje sin marcar la casilla de verificación de GravityZone. Aparecerá una ventana de confirmación.
3. Toque **Desactivar**. Se muestra un mensaje de advertencia que le informa de que dejarán de funcionar las características antirrobo y perderá el acceso a los datos y a las redes corporativas.
4. Desinstale GravityZone Mobile Client como cualquier otra aplicación.

Para desinstalar la protección de Bitdefender de un dispositivo iOS:

1. Mantenga pulsado el icono de Bitdefender GravityZone Mobile Client durante unos segundos.
2. Toque el círculo ⊗ adjunto cuando aparezca. Se elimina la aplicación.

Si desea volver a instalar la protección para dispositivos móviles, consulte"Instalación de la protección para dispositivos móviles" (p. 177)

7.6. Desinstalación del Generador de informes

Para eliminar correctamente el Generador de informes de su solución GravityZone, primero debe desinstalar el rol de Procesadores del Generador de informes y luego el de Base de datos del Generador de informes.

Para desinstalar el rol de Procesadores del Generador de informes:

1. Inicie sesión en la interfaz de consola de Procesadores del Generador de informes desde su herramienta de administración de la virtualización (por ejemplo, vSphere Client). Utilice las teclas de flecha y la tecla `Tabulador` para navegar por los menús y opciones. Pulse `Intro` para seleccionar una opción específica.
2. En el menú principal, seleccione **Configuración avanzada**.
3. Acceda a **Instalar/Desinstalar roles** y, a continuación, proceda a **Añadir o eliminar roles**.
4. Utilizando la `barra espaciadora`, desmarque el rol **Procesadores del Generador de informes** y pulse `Intro`. Aparecerá una ventana de configuración.
5. Seleccione **Sí** y pulse `Intro` para continuar y espere a que finalice la desinstalación.

Para desinstalar el rol Base de datos del Generador de informes:

1. Inicie sesión en la interfaz de consola de Base de datos del Generador de informes desde su herramienta de administración de la virtualización (por ejemplo, vSphere Client). Utilice las teclas de flecha y la tecla `Tabulador` para navegar por los menús y opciones. Pulse `Intro` para seleccionar una opción específica.
2. En el menú principal, seleccione **Configuración avanzada**.
3. Acceda a **Instalar/Desinstalar roles** y, a continuación, proceda a **Añadir o eliminar roles**.
4. Utilizando la `barra espaciadora`, desmarque el rol **Base de datos del Generador de informes** y pulse `Intro`. Aparecerá una ventana de configuración.
5. Seleccione **Sí** y pulse `Intro` para continuar y espere a que finalice la desinstalación.

Aviso
Si apaga los appliances del Generador de informes en el entorno de virtualización sin desinstalar los roles de Base de datos y Procesadores, no podrá conectarse con GravityZone Control Center.

7.7. Desinstalación de los roles del appliance virtual GravityZone

Puede desinstalar los roles del appliance virtual GravityZone mediante la interfaz de menú. Incluso si elimina uno de ellos, su red seguirá protegida. No obstante, necesita al menos una instancia de cada rol para que GravityZone funcione correctamente.

En el caso de un único appliance que tenga todos los roles de GravityZone, al quitar un rol, los endpoints seguirán protegidos, aunque no estarán disponibles algunas de las características del appliance, dependiendo del rol del que se trate.

En el caso de varios appliances GravityZone, puede desinstalar con seguridad un rol, siempre y cuando esté disponible otra instancia del mismo rol. Intencionadamente, se pueden instalar varias instancias de los roles de Consola Web y del Servidor de comunicaciones en diferentes appliances y conectarlos a los otros roles mediante un equilibrador de roles. Por lo tanto, si desinstala una instancia de un rol determinado, otros asumen su función.

Cuando haga falta, puede desinstalar el Servidor de comunicaciones de un appliance, mientras que asigna su función a otra instancia de este rol. Para una migración fluida, siga estos pasos:

1. En Control Center, acceda a la página **Políticas**.
2. Seleccione una política existente o haga clic en **Añadir** para crear una nueva.
3. En la sección **General**, acceda a **Comunicación**.
4. En la tabla de **Asignación de comunicación de endpoint**, haga clic en el campo **Nombre**. Se mostrará la lista de servidores de comunicaciones detectados.
5. Seleccione el Servidor de comunicaciones que desea conectar con los endpoints.
6. Haga clic en el botón **Añadir** del lateral derecho de la tabla. En caso de que tenga varios servidores de comunicaciones en la lista, puede configurar sus prioridades mediante las flechas arriba y abajo situadas a la derecha de cada entidad.

7. Haga clic en **Guardar** para crear la política. Los endpoints se comunicarán con Control Center mediante el servidor de comunicaciones especificado.
8. En la interfaz de línea de comandos de GravityZone, desinstale el antiguo rol del Servidor de comunicaciones.

> **Aviso**
> Si desinstala el Servidor de comunicaciones antiguo sin configurar antes la política, se perderá la comunicación permanentemente y tendrá que volver a instalar los agentes de seguridad.

Para desinstalar los roles del appliance virtual GravityZone:

1. Inicie sesión en la interfaz de la consola desde su herramienta de administración de la virtualización (por ejemplo, vSphere Client). Utilice las teclas de flecha y la tecla `Tabulador` para navegar por los menús y opciones. Pulse `Intro` para seleccionar una opción específica.
2. Seleccione **Configuración avanzada**.
3. Seleccione **Instalar/desinstalar roles**.
4. Acceda a **Añadir o eliminar roles**.
5. Utilizando la barra de `Espacio`, anule la selección de cualquier rol que desee desinstalar y, a continuación, pulse `Intro`. Aparece una ventana de confirmación que le informa del rol que será eliminado.
6. Pulse `Intro` para continuar y espere a que finalice la desinstalación.

Si desea volver a instalar un rol, consulte “Instalar/desinstalar roles” (p. 113).

8. OBTENER AYUDA

Bitdefender se esfuerza en proporcionar a sus clientes un incomparable soporte rápido y eficiente. Si experimenta algún problema o si tiene cualquier duda sobre su producto Bitdefender, diríjase a nuestro Centro de soporte online. Dispone de muchos recursos que puede utilizar para encontrar rápidamente una solución o respuesta a su problema. O, si lo prefiere, puede contactar con el equipo de Atención al Cliente de Bitdefender. Nuestro soporte responderá a todas sus preguntas en un corto periodo y le proporcionarán la asistencia que necesite.

Nota
Puede encontrar información sobre los servicios y políticas de soporte que ofrecemos en nuestro Centro de Soporte técnico.

8.1. Centro de soporte de Bitdefender

El Centro de soporte de Bitdefender es el lugar al que acudir para obtener toda la asistencia técnica que necesite para su producto de Bitdefender.

Podrá encontrar rápidamente una solución o una respuesta a su consulta:

- Artículos de la base de conocimiento
- Foro de soporte de Bitdefender
- Documentación del Producto

Puede además usar su motor de búsqueda favorito para encontrar más información sobre seguridad informática, los productos Bitdefender y la empresa.

Artículos de la base de conocimiento

La Base de conocimientos de Bitdefender es un repositorio de información online sobre los productos Bitdefender. Almacena, en un formato de fácil acceso, los informes sobre los resultados del soporte técnico en curso y las actividades de solución de errores por los equipos de soporte y desarrollo de Bitdefender, junto con artículos más generales sobre prevención de virus, la administración de las soluciones Bitdefender con explicaciones detalladas, y muchos otros artículos.

La Base de conocimiento de Bitdefender es de acceso público y puede consultarse gratuitamente. La amplia información que contiene es otro medio de proporcionar a los clientes de Bitdefender el soporte técnico y el conocimiento que necesitan. Las solicitudes de información general o informes de errores de los clientes de

Bitdefender se incluyen en la Base de conocimientos de Bitdefender en forma de soluciones a los bugs, instrucciones de depuración de errores o artículos informativos como apoyo a los archivos de ayuda de los productos.

La base de conocimientos de Bitdefender para productos corporativos está permanentemente disponible en http://www.bitdefender.com/support/business.html.

Foro de soporte de Bitdefender

El Foro de Soporte de Bitdefender proporciona a los usuarios de Bitdefender una forma fácil de obtener ayuda y ayudar a otros. Puede publicar cualquier problema o consulta relacionada con su producto Bitdefender.

El soporte técnico de Bitdefender monitoriza el foro en busca de nuevas publicaciones con el fin de ayudarle. Podrá obtener una respuesta o una solución de un usuario de Bitdefender con más experiencia.

Antes de postear su problema o pregunta, por favor, busque en el foro un tema similar o relacionado.

El Foro de Soporte de Bitdefender está disponible en http://forum.bitdefender.com, en 5 idiomas diferentes: Inglés, Alemán, Francia, España y Rumano. Haga clic en el enlace **Protección empresarial** para acceder a la sección dedicada a los productos corporativos.

Documentación del Producto

La documentación del producto es la fuente más completa de información sobre su producto.

La forma más sencilla de acceder a la documentación es desde la página **Ayuda y soporte** de Control Center. Haga clic en su nombre de usuario en la esquina superior derecha de la consola, seleccione **Ayuda y soporte** y, a continuación, elija el enlace de la guía en la que está interesado. La guía se abrirá en una nueva pestaña de su navegador.

También puede consultar y descargar la documentación en el Centro de soporte, en la sección **Documentación** disponible en las páginas de soporte de todos los productos.

8.2. Solicitar ayuda

Puede solicitar ayuda a través de nuestro Centro de soporte técnico online: Rellene el formulario de contacto y envíelo.

8.3. Usar la herramienta de soporte

La herramienta de soporte GravityZone está diseñada para ayudar a los usuarios y a los técnicos de soporte a obtener fácilmente la información que necesitan para la resolución de problemas. Ejecute la herramienta de soporte en los equipos afectados, y envíe el archivo resultante con la información de la resolución del problema al representante de soporte de Bitdefender.

8.3.1. Uso de la herramienta de soporte en sistemas operativos Windows

Ejecución de la aplicación de la herramienta de soporte

Para generar el registro en el equipo afectado, siga uno de estos métodos:

- Línea de comandos

  Para cualquier problema con BEST, instalado en el equipo.

- Incidencia de instalación

  En casos en los que BEST no esté instalado en el equipo y falle la instalación.

Método de línea de comandos

Mediante la línea de comandos puede recopilar registros directamente desde el equipo afectado. Este método es útil en situaciones en las que no se tiene acceso al GravityZone Control Center o en las que el equipo no se comunica con la consola.

1. Abra el símbolo del sistema con privilegios administrativos.
2. Diríjase a la carpeta de instalación del producto. La ruta por defecto es:

   `C:\Archivos de programa\Bitdefender\Endpoint Security`
3. Recopile y guarde los registros ejecutando este comando:

```
Product.Support.Tool.exe collect
```

Los registros se guardan por defecto en `C:\Windows\Temp`.

Como alternativa, si desea guardar el registro de la herramienta de soporte en una ubicación personalizada, use la ruta opcional:

```
Product.Support.Tool.exe collect [path="<path-to-file>"]
```

Ejemplo:

```
Product.Support.Tool.exe collect path="D:\Test"
```

Mientras se ejecuta el comando, podrá ver una barra de progreso en la pantalla. Tras finalizar el proceso, se muestra el nombre del archivo comprimido que contiene los registros y su ubicación.

Para enviar los registros al soporte empresarial de Bitdefender, acceda a `C:\Windows\Temp` o a la ubicación personalizada y busque el archivo comprimido `ST_[computername]_[currentdate]`. Adjunte el archivo comprimido a su ticket de soporte para proceder a la resolución del problema.

Incidencia de instalación

1. Para descargar la herramienta de soporte de BEST, haga clic aquí.
2. Ejecute como administrador el archivo ejecutable. Aparecerá una ventana.
3. Elija una ubicación para guardar el archivo comprimido con los registros.

   Mientras se recopilan los registros, podrá ver una barra de progreso en la pantalla. Tras finalizar el proceso, se muestra el nombre del archivo comprimido y su ubicación.

Para enviar los registros al soporte empresarial de Bitdefender, acceda a la ubicación seleccionada y busque el archivo comprimido `ST_[computername]_[currentdate]`. Adjunte el archivo comprimido a su ticket de soporte para proceder a la resolución del problema.

8.3.2. Uso de la herramienta de soporte en sistemas operativos Linux

En el caso de los sistemas operativos Linux, la herramienta de soporte va integrada con el agente de seguridad de Bitdefender.

Para recopilar información del sistema Linux mediante la herramienta de soporte, ejecute el siguiente comando:

```
# /opt/BitDefender/bin/bdconfigure
```

con las siguientes opciones disponibles:

- `--help` para obtener una lista con todos los comandos de la herramienta de soporte
- `enablelogs` para activar los registros del módulo de comunicaciones y del producto (todos los servicios se reiniciarán automáticamente)
- `enablelogs` para desactivar los registros del módulo de comunicación y del producto (todos los servicios se reiniciarán automáticamente)
- `deliverall` para crear:
  - Un archivo comprimido que contiene los registros de instalación, depositado en la carpeta `/var/log/BitDefender` con el siguiente formato: `bitdefender_nombreMáquina_hora.tar.gz`.

  Una vez creado el archivo comprimido:

  1. Se le preguntará si desea desactivar los registros. De ser necesario, los servicios se reiniciarán automáticamente.
  2. Se le preguntará si desea eliminar los registros.
- `deliverall -default` proporciona la misma información que en la opción anterior, pero se adoptarán las acciones por defecto para los registros, sin preguntar al usuario (los registros se desactivan y se eliminan).

También puede ejecutar el comando `/bdconfigure` directamente desde el paquete BEST (completo o downloader) sin tener el producto instalado.

Para informar de un problema de GravityZone que afecte a los sistemas Linux, siga los siguientes pasos, usando las opciones descritas anteriormente:

1. Active los registros del módulo de comunicaciones y del producto.
2. Trate de reproducir el problema.
3. Desactive los registros.
4. Cree el archivo comprimido con los registros.

5. Abra un ticket de soporte de correo electrónico mediante el formulario disponible en la página **Ayuda y soporte** de Control Center, con una descripción del problema y adjuntando el archivo comprimido de los registros.

La herramienta de soporte para Linux ofrece la siguiente información:

- Las carpetas `etc`, `var/log`, `/var/crash` (si existe) y `var/epag` de `/opt/BitDefender`, que contienen los ajustes y registros de Bitdefender
- El archivo `/var/log/BitDefender/bdinstall.log`, que contiene la información sobre la instalación
- El archivo `Network.txt`, que contiene los ajustes de red y la información de conectividad de la máquina
- El archivo `product.txt`, que incluye el contenido de todos los archivos `update.txt` de `/opt/BitDefender/var/lib/scan` y una lista recursiva completa de todos los archivos de `/opt/BitDefender`.
- El archivo `system.txt`, que contiene información general del sistema (versiones del kernel y de la distribución, RAM disponible y espacio libre en el disco duro)
- El archivo `users.txt`, que contiene información sobre el usuario
- Otra información referente al producto en relación con el sistema, como por ejemplo las conexiones externas de los procesos y el uso de la CPU
- Registros del sistema.

8.3.3. Uso de la herramienta de soporte en sistemas operativos Mac

Para enviar una solicitud al equipo de soporte técnico de Bitdefender, ha de proporcionar lo siguiente:

- Una descripción detallada del problema que se ha encontrado.
- Una captura de pantalla (si procede) del mensaje de error exacto que aparece.
- El registro de la herramienta de soporte.

Para obtener información del sistema Mac mediante la herramienta de soporte:

1. Descargue el archivo ZIP que contiene la herramienta de soporte.
2. Extraiga el archivo **BDProfiler.tool** del archivo comprimido.

3. Abra una ventana de Terminal.
4. Acceda a la ubicación del archivo **BDProfiler.tool**.

   Por ejemplo:

   ```
   cd /Users/Bitdefender/Desktop;
   ```

5. Dote al archivo de permisos de ejecución:

   ```
   chmod +x BDProfiler.tool;
   ```

6. Ejecute la herramienta.

   Por ejemplo:

   ```
   /Users/Bitdefender/Desktop/BDProfiler.tool;
   ```

7. Pulse `Y` e introduzca la contraseña cuando se le pida que proporcione la contraseña del administrador.

   Espere un par de minutos a que la herramienta acabe de generar el registro. Hallará el archivo comprimido resultante (**Bitdefenderprofile_output.zip**) en su escritorio.

8.4. Información de contacto

La eficiente comunicación es la clave para un negocio con éxito. Durante los últimos 18 años, Bitdefender se ha forjado una reputación incuestionable de lucha constante para mejorar la comunicación y así aumentar las expectativas de nuestros clientes y partners. Por favor no dude en contactar con nosotros.

8.4.1. Direcciones

Departamento de ventas: enterprisesales@bitdefender.com
Centro de soporte:http://www.bitdefender.com/support/business.html
Documentación: gravityzone-docs@bitdefender.com
Distribuidores locales:http://www.bitdefender.es/partners
Programa de Partners: partners@bitdefender.com
Relaciones con la Prensa: prensa@bitdefender.es

Envío de virus: virus_submission@bitdefender.com
Envío de Spam: spam_submission@bitdefender.com
Notificar abuso: abuse@bitdefender.com
Sitio Web: http://www.bitdefender.com

8.4.2. Distribuidor Local

Los distribuidores locales de Bitdefender están preparados para responder a cualquier pregunta relacionada con su área, tanto a nivel comercial como en otras áreas.

Para encontrar un distribuidor de Bitdefender en su país:

1. Visite http://www.bitdefender.es/partners.
2. Ir a **Localizador de Partner**.
3. La información de contacto de los distribuidores locales de Bitdefender debería mostrarse automáticamente. Si esto no sucede, seleccione el país en el que reside para ver la información.
4. Si no encuentra un distribuidor Bitdefender en su país, no dude en contactar con nosotros por correo en enterprisesales@bitdefender.com.

8.4.3. Oficinas de Bitdefender

Las oficinas de Bitdefender están listas para responder a cualquier pregunta relativa a sus áreas de acción, tanto a nivel comercial como en otros asuntos. Sus direcciones y contactos están listados a continuación.

Estados Unidos

Bitdefender, LLC
PO Box 667588
Pompano Beach, Fl 33066
United States
Teléfono (comercial&soporte técnico): 1-954-776-6262
Comercial: sales@bitdefender.com
Web: http://www.bitdefender.com
Centro de soporte: http://www.bitdefender.com/support/business.html

Francia

Bitdefender

49, Rue de la Vanne
92120 Montrouge
Fax: +33 (0)1 47 35 07 09
Teléfono: +33 (0)1 47 35 72 73
Correo: b2b@bitdefender.fr
Página web: http://www.bitdefender.fr
Centro de soporte: http://www.bitdefender.fr/support/business.html

España

Bitdefender España, S.L.U.
Avda. Diagonal, 357, 1º 1ª
08037 Barcelona
España
Fax: (+34) 93 217 91 28
Tel (oficina&comercial): (+34) 93 218 96 15
Teléfono (soporte técnico): (+34) 93 502 69 10
Comercial: comercial@bitdefender.es
Página web: http://www.bitdefender.es
Centro de soporte: http://www.bitdefender.es/support/business.html

Alemania

Bitdefender GmbH
Technologiezentrum Schwerte
Lohbachstrasse 12
D-58239 Schwerte
Deutschland
Tel (oficina&comercial): +49 (0) 2304 94 51 60
Teléfono (soporte técnico): +49 (0) 2304 99 93 004
Comercial: firmenkunden@bitdefender.de
Página web: http://www.bitdefender.de
Centro de soporte: http://www.bitdefender.de/support/business.html

Reino Unido e Irlanda

Genesis Centre Innovation Way
Stoke-on-Trent, Staffordshire
ST6 4BF
UK

Teléfono (comercial&soporte técnico): (+44) 203 695 3415
Correo: info@bitdefender.co.uk
Comercial: sales@bitdefender.co.uk
Página web: http://www.bitdefender.co.uk
Centro de soporte: http://www.bitdefender.co.uk/support/business.html

Rumania

BITDEFENDER SRL
Orhideea Towers
15A Orhideelor Street
060071 Bucharest, Sector 6
Fax: +40 21 2641799
Teléfono (comercial&soporte técnico): +40 21 2063470
Comercial: sales@bitdefender.ro
Página web: http://www.bitdefender.ro
Centro de soporte: http://www.bitdefender.ro/support/business.html

Emiratos Árabes Unidos

Bitdefender FZ-LLC
Dubai Internet City, Building 17
Office # 160
Dubai, UAE
Teléfono (comercial&soporte técnico): 00971-4-4588935 / 00971-4-4589186
Fax: 00971-4-44565047
Comercial: sales@bitdefender.com
Web: http://www.bitdefender.com
Centro de soporte: http://www.bitdefender.com/support/business.html

A. Apéndices

A.1. Tipos de archivo compatibles

Los motores de análisis antimalware incluidos en las soluciones de seguridad de Bitdefender pueden analizar todos los tipos de archivo que puedan contener amenazas. La lista siguiente incluye los tipos de archivo que se analizan más comúnmente.

{*; 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. Objetos Sandbox Analyzer

A.2.1. Tipos de archivo y extensiones admitidas para el envío manual

Las siguientes extensiones de archivo se admiten y pueden detonarse manualmente en Sandbox Analyzer:

Lotes, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML (Unicode), JAR (comprimido), JS, LNK, MHTML (doc), MHTML (ppt), MHTML (xls), Microsoft Excel, Microsoft PowerPoint, Microsoft Word, archivos MZ/PE (ejecutable), PDF, PEF (ejecutable), PIF (ejecutable), RTF, SCR, URL (binario), VBE, VBS, WSF, WSH, WSH-VBS y XHTML.

Sandbox Analyzer es capaz de detectar los tipos de archivo antes mencionados también si se incluyen en archivos de los siguientes tipos: 7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, archivo comprimido LZMA, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (multivolumen), ZOO y XZ.

A.2.2. Tipos de archivos admitidos por el prefiltrado de contenidos para los envíos automáticos

El prefiltrado de contenidos determinará un tipo de archivo en particular atendiendo tanto al contenido del objeto como a su extensión. Eso significa que un ejecutable que tenga la extensión `.tmp` será reconocido como una aplicación y, si parece sospechoso, se enviará a Sandbox Analyzer.

- Aplicaciones: archivos que tienen el formato PE32, incluyendo, entre otras, las extensiones exe, dll y com.
- Aplicaciones: archivos que tienen el formato de documento, incluyendo, entre otras, las extensiones xlsx, xls, ppt, doc, docx, dot, chm, xlm, docm, dotm, potm, potx, ppam, ppax, pps, ppsm, pptx, sldm, sldx, xlam, xlm, xltm, rtf y pdf.

- Scripts: `ps, wsf, ws, php, py, js, vb, vbs, pyc, pyo, wsc, wsh, psc1, jse y vbe.`
- Archivos comprimidos: `zip, jar, 7z, bz, bz2, tgz , msi, rar, rev, z, arj, iso, lha, lhz, uu, uue, xxe, lzma, ace y r00.`
- Correos electrónicos (guardados en el sistema de archivos): `eml y tnef.`

A.2.3. Exclusiones predeterminadas del envío automático

`asc, avi, bmp, gif, jpeg, jpg, mkv, mp4, pgp, png y txt.`

A.2.4. Aplicaciones recomendadas para las máquinas virtuales de detonación

Sandbox Analyzer On-Premises requiere que se instalen ciertas aplicaciones en las máquinas virtuales de detonación para que abran las muestras enviadas.

Aplicaciones	Tipos archivo
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
Windows por defecto	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