Bitdefender

GravityZone

INSTALLATIONSANLEITUNG

Bitdefender GravityZone Installationsanleitung

Veröffentlicht 2021.04.20

Rechtlicher Hinweis

Rechtlicher Hinweis

Alle Rechte vorbehalten. Bestandteile dieses Handbuches dürfen weder in elektronischer noch mechanischer Form reproduziert werden. Dies gilt auch für das Fotokopieren, Aufnehmen oder jegliche andere Form von Datenspeicherung oder Informationsbeschaffung, ohne die Zustimmung von Bitdefender. Ausnahmen gelten für Zitate in Verbindung mit Testberichten. Der Inhalt darf in keiner Weise verändert werden.

Inhaltsverzeichnis

Vorwort

Dieses Handbuch richtet sich an IT-Administratoren, die mit der Installation von GravityZone innerhalb ihres Unternehmens betraut sind. IT-Administratoren finden in diesem Handbuch Informationen zu GravityZone sowie zu den Installationsanforderungen und den in GravityZone verfügbaren Sicherheitsmodulen.

In diesem Dokument wird erklärt, wie Sie die GravityZone-Lösung und ihre Sicherheitsagenten auf sämtlichen Arten von Endpunkten in Ihrem Unternehmen installieren und konfigurieren können.

1. In diesem Handbuch verwendete Konventionen

Typografie

In diesem Handbuch werden zur besseren Lesbarkeit verschiedene Schriftarten verwendet. In der unten stehenden Tabelle erfahren Sie, was welche Schriftart bedeutet.

Erscheinungsbild	Beschreibung
`Beispiel`	Einzugebende Befehle und Syntaxen, Pfade und Dateinamen, Konfigurationen, Dateiausgaben und andere Eingabetexte sind in `nicht-proportionaler` Schrift gedruckt.
http://www.bitdefender.com	Verweise (Links) auf externe Inhalte wie z.B. Web-Seiten oder FTP-Server.
gravityzone-docs@bitdefender.com	Verweise auf E-Mail-Adressen, z.B. zur Kontaktaufnahme.
„Vorwort“ (S. viii)	Interne Verweise (Links) auf beliebige Stellen innerhalb dieses Dokuments.
Option	Alle Produktoptionen werden **fett gedruckt** dargestellt.
Stichwort	Optionen der Benutzeroberfläche, Stichwörter oder Tastenkombinationen werden durch **Fettdruck** hervorgehoben.

Hinweise

Hierbei handelt es sich um Hinweise innerhalb des Textflusses, welche mit einer kleinen Grafik markiert sind. Es handelt sich um Informationen, die Sie in jedem Fall beachten sollten.

Beachten Sie
Diese Bemerkung dient lediglich zur Überprüfung. Notizen enthalten in der Regel nützliche Informationen wie zum Beispiel einen Verweis auf ein verwandtes Thema.

Wichtig
Diese Art von Hinweis sollte in jedem Fall gelesen werden. Es werden wichtige Informationen zum jeweiligen Thema gegeben, die nicht übersprungen werden sollten.

Warnung
Diese kritische Information erfordert größtmögliche Aufmerksamkeit. Hier angegebenen Anweisungen und Informationen sollten Sie auf jeden Fall Beachtung schenken. Sie sollten diese Informationen sorgsam lesen und verstanden haben, da es sich um eine höchst kritische Thematik handelt.

1. ÜBER GRAVITYZONE

GravityZone ist eine Sicherheitslösung für Unternehmen, die speziell auf virtuelle und Cloud-Umgebungen zugeschnitten ist, und bietet Sicherheitsdienste für physische Endpunkte, Mobilgeräte und virtuelle Maschinen in der Private und der Public Cloud sowie für Exchange-Mail-Server.

GravityZone ist ein umfassendes Produkt mit einer zentralen Verwaltungskonsole, die entweder von Bitdefender in der Cloud gehostet oder als virtuelle Appliance innerhalb des Unternehmens installiert wird. Über diese Konsole können von zentraler Stelle aus Sicherheitsrichtlinien für eine beliebige Zahl an Endpunkten erstellt, zugewiesen und verwaltet werden, unabhängig vom Typ und geographischen Ort dieser Endpunkte.

GravityZone bietet Sicherheit für Endpunkte und Microsoft-Exchange-Mail-Server in mehreren Schichten: Malware-Schutz mit Verhaltensüberwachung, Schutz vor Zero-Day-Attacken, Anwendungssteuerung und Sandboxing, Firewall, Gerätesteuerung, Inhaltssteuerung sowie Phishing- und Spam-Schutz.

2. GRAVITYZONE-SICHERHEITSEBENEN

GravityZone umfasst die folgenden Sicherheitsebenen:

- Malware-Schutz
- Advanced Threat Control
- HyperDetect
- Erweiterter Exploit-Schutz
- Firewall
- Inhalts-Steuerung
- Patch-Verwaltung
- Gerätesteuerung
- Full Disk Encryption
- Security for Exchange
- Anwendungssteuerung
- Sandbox Analyzer
- Hypervisor Memory Introspection (HVI)
- Network Traffic Security Analytics (NTSA)
- Security for Storage
- Security for Mobile

2.1. Malware-Schutz

Das Anti-Malware-Sicherheitsebene setzt Signatur-Scans und heuristische Analysen (B-HAVE, ATC) ein, um Schutz vor Viren, Würmern, Trojanern, Spyware, Adware, Keyloggern, Rootkits und anderer bösartiger Software zu gewährleisten.

Bitdefenders Malware-Scans setzen auf die folgenden Technologien:

- Zunächst kommt eine herkömmliche Scan-Methode zum Einsatz, bei der die überprüften Inhalte mit der Signaturdatenbank abgeglichen werden. Die Signaturdatenbank enthält die Byte-Folgen, die für bekannte Bedrohungen spezifisch sind, und wird von Bitdefender regelmäßig aktualisiert. Diese Scan-Methode erkennt sehr effektiv bestätigte Bedrohung, die bereits erforscht und dokumentiert wurden. Doch auch wenn die Signaturdatenbank immer umgehend aktualisiert wird, gibt es zwischen der Entdeckung der Bedrohung und der Problemlösung immer ein Zeitfenster, in dem das System eine Schwachstelle hat.
- Neue, bisher noch nicht dokumentierte Bedrohungen werden in einer zweiten Schutzebene aufgefangen. Dabei handelt es sich um **B-HAVE**, die heuristische

Engine von Bitdefender. Heuristische Algorithmen erkennen Malware anhand bestimmter Verhaltensweisen. B-HAVE führt verdächtige Dateien in einer virtuellen Umgebung aus, um ihre Auswirkungen auf das System zu untersuchen und eine Bedrohung auszuschließen. Sollte eine Bedrohung erkannt werden, wird eine Ausführung des Programms verhindert.

Scan-Engines

Bitdefender GravityZone ist in der Lage, die Scan-Engines beim Erstellen der Pakete für die Sicherheitsagenten entsprechend der Endpunktkonfiguration automatisch anzupassen.

Administratoren können die Scan-Engines auch manuell anpassen. Dabei können sie unter den folgenden Optionen wählen:

1. **Lokaler Scan**: für Scans, die auf lokalen Endpunkten durchgeführt werden. Der lokale Scan-Modus eignet sich für leistungsstarke Maschinen, auf denen alle Signaturen und Engines lokal gespeichert sind.
2. **Hybrid-Scan mit leichten Engines (Public Cloud)**: mittlerer Ressourcenverbrauch; gescannt wird in der Cloud und zum Teil auch mithilfe lokaler Signaturen. Dieser Scan-Modus reduziert den Ressourcenverbrauch durch Auslagerung der Scan-Aktivität.
3. **Zentralisierter Scan in der Public oder Private Cloud**: geringer Ressourcenverbrauch; benötigt einen Security Server zum Scan. In diesem Fall werden keine Signaturen lokal gespeichert. Die Scan-Aktivität wird auf den Security Server ausgelagert.

   Beachten Sie
   Es gibt eine Mindestanzahl an lokal gespeicherten Engines, die zum Entpacken der komprimierten Dateien benötigt werden.

4. **Zentralisierter Scan (Scan in der Public oder Private Cloud mit Security Server) mit Ausweichmöglichkeit* auf lokalen Scan (Full Engines)**
5. **Zentralisierter Scan (Scan in der Public oder Private Cloud mit Security Server) mit Ausweichmöglichkeit* auf Hybrid-Scan (Public Cloud mit leichten Engines)**

* Bei Scans mit zwei Engines wird die Ausweich-Engine verwendet, wenn die erste Engine nicht verfügbar ist. Der Ressourcenverbrauch und die Netzwerknutzung hängen von den verwendeten Engines ab.

2.2. Advanced Threat Control

Für Bedrohungen, die selbst von der heuristischen Engine nicht erkannt werden, wurde mit Advanced Threat Control (ATC) eine weitere Sicherheitsebene eingerichtet.

Advanced Threat Control überwacht ununterbrochen laufende Prozesse und bewertet verdächtige Verhaltensweisen wie zum Beispiel Verbergen des Prozesstyps, Ausführung von Code im Adressraum eines anderen Prozesses (Übernahme des Prozessspeichers zur Erweiterung von Rechten), Replikationsversuche, Ablegen von Dateien, Verbergen vor Anwendungen zur Prozessübersicht usw. Jedes verdächtige Verhalten steigert den Verdachtswert des Prozesses. Bei Überschreiten einer Schwelle wird ein Alarm ausgelöst.

2.3. HyperDetect

Bitdefender HyperDetect ist eine zusätzliche Sicherheitsebene, die speziell entwickelt wurde, um komplexe Angriffe und verdächtige Aktivitäten noch vor der Ausführungsphase zu erkennen. HyperDetect enthält maschinelle Lernmodelle und Technologien zur Erkennung von getarnten Angriffen zur Abwehr von Bedrohungen wie Zero-Day-Angriffen, Advanced Persistent Threats (APT), verschleierter Malware, dateilosen Angriffen (Missbrauch von PowerShell, Windows Management Instrumentation usw.), Diebstahl von Anmeldeinformationen, gezielten Angriffen, Custom Malware, skriptbasierten Angriffen, Exploits, Hacking-Tools, verdächtigem Netzwerkverkehr, potenziell unerwünschten Anwendungen (PUA) und Ransomware.

Beachten Sie
Dieses Modul ist ein Add-on, das mit einem eigenen Lizenzschlüssel erhältlich ist.

2.4. Erweiterter Exploit-Schutz

Diese neue proaktive Technologie nutzt maschinelle Lernverfahren und stoppt so Zero-Day-Angriffe, die nur schwer zu findende Exploits ausnutzen. Der erweiterte Exploit-Schutz findet auch die neuesten Exploits in Echtzeit und behebt Memory-Corruption-Schwachstellen, die vorhandene Sicherheitslösungen umgehen können. Schützt die gebräuchlichsten Anwendungen, wie Browser, Microsoft Office oder Adobe Reader, sowie andere, die Ihnen einfallen. Überwacht Systemprozesse und schützt vor Sicherheitseinbrüchen und Prozess-Hijacking.

2.5. Firewall

Die Firewall steuert den Zugriff von Anwendungen auf das Netzwerk sowie auf das Internet. Eine umfangreiche Datenbank enthält eine Liste bekannter, vertrauenswürdiger Anwendungen, denen automatisch Zugriff gewährt wird. Zudem kann die Firewall das System vor Port-Scans schützen, die gemeinsame Nutzung der Internet-Verbindung (ICS) beschränken und Benachrichtigungen generieren, sobald neue Knoten mit dem Drahtlosnetzwerk verbunden werden.

2.6. Inhalts-Steuerung

Mit dem Modul Inhaltssteuerung können Unternehmensrichtlinien für zugelassenen Datenverkehr, Internetzugriff, Datenschutz und Anwendungssteuerung durchgesetzt werden. Administratoren können Scan-Optionen und -Ausschlüsse für den Datenverkehr festlegen, den Internetzugriff auf bestimmte Zeiten beschränken, einzelne Internetkategorien oder URLs blockieren, Identitätsschutzregeln konfigurieren und Rechte für die Verwendung bestimmter Anwendungen festlegen.

2.7. Network Attack Defense

Das Network Attack Defense-Modul nutzt eine Bitdefender-Technologie zur Erkennung von Angriffen auf das Netzwerk, mit denen versucht wird, über Verfahren wie Brute-Force-Angriffe, Netzwerk-Exploits, Passwortdiebstahl, Drive-by-Download-Infektionsvektoren, Bots oder Trojaner Zugriff auf Endpunkte zu erlangen.

2.8. Patch-Verwaltung

Die Patch-Verwaltung ist vollständig in GravityZone integriert und sorgt dafür, dass Ihre Programme und Ihr Betriebssystem immer auf dem neuesten Stand sind und verleiht Ihnen einen Überblick über den Patch-Status der verwalteten Windows-Endpunkte.

Das GravityZone-Modul Patch-Verwaltung beinhaltet verschiedene Funktionen, darunter Patch-Scans auf Knopfdruck oder nach Plan, automatische/manuelle Aufspielung von Patches und Berichte zu fehlenden Patches.

Welche Anbieter und Produkte von der GravityZone-Patch-Verwaltung unterstützt werden, können Sie in Artikel nachlesen.

Beachten Sie
Die Patch-Verwaltung ist ein Add-on, das über einen separaten Lizenzschlüssel für alle GravityZone-Pakete erworben werden kann.

2.9. Gerätesteuerung

Mit dem Modul Gerätesteuerung kann mithilfe von in Richtlinien festgelegten Blockier-Regeln und -Ausnahmen verhindert werden, dass sensible Daten unbefugt weitergegeben werden und Infektionen über externe Datenträger ins Netzwerk gelangen. Dies ist für eine Vielzahl von Gerätearten möglich wie zum Beispiel USB-Sticks, Bluetooth-Geräte, CD/DVD-Player, Speichermedien und vieles mehr.

2.10. Full Disk Encryption

Diese Sicherheitsebene verwaltet BitLocker unter Windows sowie FileVault und diskutil unter macOS und ermöglicht so eine vollständige Festplattenverschlüsselung auf Ihren Endpunkten. Sie können bootfähige und nicht bootfähige Laufwerke mit nur einem Klick verschlüsseln und entschlüsseln. Dabei übernimmt GravityZone die meiste Arbeit. Sie selbst müssen kaum etwas tun. Außerdem werden in GravityZone die Wiederherstellungsschlüssel gespeichert, die zur Entschlüsselung der Laufwerke benötigt werden, falls der Benutzer mal das Passwort vergessen sollte.

Beachten Sie
Die Full Disk Encryption ist ein Add-on, das über einen separaten Lizenzschlüssel für alle GravityZone-Pakete erworben werden kann.

2.11. Security for Exchange

Bitdefender Security for Exchange bietet Malware-, Spam- und Phishing-Schutz sowie eine Anhang- und Inhaltsfilterung. Die Lösung lässt sich nahtlos mit Microsoft Exchange Server integrieren und schafft so eine Malware-freie E-Mail- und Kollaborationsumgebung und erhöht damit die Produktivität. Dank mehrfach ausgezeichneter Malware- und Spam-Schutz-Technologie schützt die Software Exchange-Benutzer selbst vor raffinierter, bisher unbekannter Malware sowie vor Datendiebstahl.

Wichtig
Security for Exchange wurde entwickelt, um die gesamte Exchange-Organisation zu schützen, zu der der geschützte Exchange-Server gehört. Das bedeutet, dass es alle

aktiven Postfächer schützt, einschließlich Benutzer-,Raum-,Geräte- und freigegebene Postfächer.
Zusätzlich zum Microsoft Exchange-Schutz umfasst die Lizenz die auf dem Server installierten Module für den Endpunktschutz.

2.12. Anwendungssteuerung

Das Anwendungssteuerungsmodul verhindert Malware- und Zero-Day-Angriffe und sorgt für zuverlässige Sicherheit, ohne die Mitarbeiterproduktivität zu beeinträchtigen. Mit der Anwendungssteuerung können flexible Richtlinien für das Whitelisting von Anwendungen angewandt werden, die eine Installation und Ausführung von nicht erwünschten, nicht vertrauenswürdigen oder schädlichen Anwendungen erkennen und verhindern.

2.13. Sandbox Analyzer

Der Bitdefender Sandbox Analyzer bietet hohe Sicherheit vor raffinierten Bedrohungen, indem automatische, detaillierte Analysen verdächtiger Dateien durchgeführt werden; selbst solcher Dateien, die noch keine Signatur von den Bitdefender-Malware-Schutz-Engines erhalten haben. In der Sandbox kommen verschiedene Bitdefender-Technologien zum Einsatz, mithilfe derer Schadcode in einer abgeschlossenen, von Bitdefender gehosteten virtuellen Umgebung ausgeführt, anschließend das Verhalten analysiert und jede noch so kleine Veränderung am System, die auf schädliche Aktivitäten hindeuten könnten, gemeldet wird.

Sandbox Analyzer verwendet eine Reihe von Sensoren, um Inhalte von verwalteten Endpunkten, aus Netzwerk-Datenströmen, der zentralen Quarantäne und ICAP-Servern zu detonieren.

Darüber hinaus ermöglicht Sandbox Analyzer die manuelle Übermittlung von Proben und die Übermittlung über die API.

2.14. Hypervisor Memory Introspection (HVI)

Es ist allgemein bekannt, dass durchorganisierte, profitorientierte Angriffe unerkannte Sicherheitslücken (Zero-Day-Lücken) suchen oder einmalige, zweckgerichtete Exploits (Zero-Day-Exploits) und andere Mittel nutzen. Angreifer verwenden zudem hochentwickelte Techniken, mit denen sie Angriffe verzögern oder fragmentieren, um sicherheitsgefährdende Aktivitäten zu verschleiern.

Profitorientierte Angriffe jüngeren Datums sind getarnt und umgehen traditionelle Sicherheits-Tools.

Für virtualisierte Umgebungen ist das Problem nun behoben, da HVI Datenzentren mit hoher Dichte an virtuellen Maschinen vor hochentwickelten, fortschrittlichen Bedrohungen schützt, die signatur-basierte Engines nicht bekämpfen können. Es bietet hohe Abschirmung, erkennt Angriffe in Echtzeit und wehrt sie direkt beim Auftreten ab und schaltet die Bedrohung aus.

Ob es sich um ein Windows- oder Linuxgerät, um einen Server oder einen Arbeitsplatzrechner handelt, HVI bietet Einblick in einem Umfang, der aus Sicht des Gast-Betriebssystems nicht möglich ist. So wie der Hypervisor den Hardware-Zugang für alle virtuellen Gast-Maschinen kontrolliert, verfügt HVI über Detailwissen hinsichtlich Benutzermodus und Betriebssystem (Kernel Mode) des Gastspeichers. Folglich hat HVI vollständigen Einblick in den Gastspeicher und somit ein umfassendes Gesamtbild. Gleichzeitig ist HVI vom geschützten Gast isoliert im gleichen Maße wie der Hypervisor selbst isoliert ist. Da HVI auf Hypervisor-Ebene arbeitet und die Hypervisor-Funktionalitäten unterstützt, bewältigt es die technischen Herausforderungen traditioneller Sicherheitssysteme und deckt so bösartige Aktivitäten in Datenzentren auf.

HVI erkennt nicht Angriffsmuster, sondern Angriffstechniken. So kann diese Technologie übliche Exploit-Techniken erkennen, melden und verhindern. Der Kernel ist gegen Rootkit-Hook-Techniken geschützt, die während des Angriffs als Tarnung verwendet werden. Benutzer-Modus-Vorgänge sind außerdem gegen Code-Injection, Function-Detour und Code-Ausführung aus dem Stapel- oder Heap-Speicher geschützt.

2.15. Network Traffic Security Analytics (NTSA)

Bitdefender Network Traffic Security Analytics (NTSA) ist eine Lösung für die Netzwerksicherheit, die IPFIX-Datenverkehrsströme auf bösartiges Verhalten und Malware überprüft.

Bitdefender NTSA soll neben Ihren bestehenden Sicherheitsmaßnahmen als ergänzender Schutz dienen, der in der Lage ist, auch tote Winkel abzudecken, die herkömmliche Tools nicht überwachen.

Herkömmliche Tools für die Netzwerksicherheit versuchen in der Regel, Malware-Infektionen zu verhindern, indem sie den eingehenden Datenverkehr überprüfen (über Sandbox, Firewall, Virenschutzprogramme usw.). Bitdefender

NTSA konzentriert sich ausschließlich auf die Überwachung des ausgehenden Netzwerkverkehrs auf bösartiges Verhalten.

2.16. Security for Storage

Mit GravityZone Security for Storage erhalten Sie erstklassigen Echtzeitschutz für alle führenden File-Sharing- und Netzwerkspeichersysteme. Alle Upgrades des Systems und der Algorithmen für die Bedrohungserkennung laufen automatisch ab. Dadurch entstehen Ihnen keine Aufwände und Ihre Nutzer werden nicht in ihrer Arbeit gestört.

Zwei oder mehrere GravityZone Security Server Multi-Platform übernehmen die Rolle des ICAP-Servers, über den die Dienste für den Malware-Schutz für ICAP-konforme (siehe RFC3507) Network-Attached-Storage-Geräte (NAS) und File-Sharing-Systeme bereitgestellt werden.

Sobald ein Benutzer über seinen Laptop, seinen Arbeitsplatzrechner, sein Mobilgerät oder ein anderes Gerät eine Anfrage zum Öffnen, Lesen, Schreiben oder Schließen einer Datei stellt, übermittelt der ICAP-Client (NAS- oder File-Sharing-System) ein Scan-Anfrage an den Security Server und erhält eine entsprechende Rückinformation. Davon abhängig erlaubt der Security Server den Zugriff, verweigert den Zugriff oder löscht die Datei.

Beachten Sie
Dieses Modul ist ein Add-on, das mit einem eigenen Lizenzschlüssel erhältlich ist.

2.17. Security for Mobile

Die Lösung vereint unternehmensweite Sicherheit mit der Verwaltung und Compliance-Überwachung von iPhones, iPads und Android-Geräten durch die zuverlässige Bereitstellung von Software und Updates über die Apple- und Android-Marktplätze. Durch einheitliche Durchsetzung von Sicherheitsrichtlinien auf allen Mobilgeräten können Mitarbeiter ihre eigenen Geräte sicher und kontrolliert im Unternehmensnetzwerk verwenden (BYOD). Zu den Sicherheitsfunktionen gehören Bildschirmsperre, Authentifizierungskontrolle und Geräteortung, Datenlöschung per Fernzugriff und Erkennung von Geräten mit Root oder Jailbreak sowie Sicherheitsprofile. Auf Android-Geräten wird die Sicherheit noch einmal durch Echtzeit-Scans und die Verschlüsselung von Wechselmedien erhöht. So werden die Mobilgeräte zuverlässig kontrolliert und die darauf gespeicherten sensiblen Unternehmensdaten geschützt.

2.18. Verfügbarkeit der GravityZone-Sicherheitsebenen

Die Verfügbarkeit der verschiedenen GravityZone-Sicherheitsebenen hängt vom Betriebssystem des Endpunkts ab. Weitere Informationen finden Sie in der Wissensdatenbank im Artikel Verfügbarkeit der GravityZone-Sicherheitsebenen.

3. GRAVITYZONE-ARCHITEKTUR

Dank seiner einzigartigen Architektur ist GravityZone extrem skalierbar und kann eine beliebige Anzahl von Systemen schützen. GravityZone kann mehrere virtuelle Appliances und mehrere Instanzen bestimmter Rollen (Datenbank, Kommunikationsserver, Update-Server und Web-Konsole) verwenden, um Verfügbarkeit und Skalierbarkeit auf hohem Niveau zu halten.

Jede Instanz einer Rolle kann auf einer anderen Appliance installiert werden. Eingebaute Lastenverteilungen gewährleisten, dass GravityZone selbst die umfangreichsten Unternehmensnetzwerke zuverlässig schützen kann, ohne Verzögerungen oder Ressourcenengpässe zu verursachen. Statt der eingebauten Lastenverteilungen kann auch Drittanbieter-Software zur Lastenverteilung eingesetzt werden.

GravityZone wird als virtueller Container zur Verfügung gestellt und kann so in jede virtuelle Umgebung importiert werden, egal ob sie mit VMware, Citrix, Microsoft Hyper-V, Nutanix Prism oder Microsoft Azure betrieben wird.

Die Integration mit VMware vCenter, Citrix XenServer, Microsoft Active Directory, Nutanix Prism Element und Microsoft Azure macht es leichter, physische und virtuelle Endpunkte gleichzeitig zu schützen.

GravityZone besteht aus den folgenden Komponenten:

- GravityZone-Virtual-Appliance
- Security Server
- HVI-Ergänzungspaket
- Sicherheitsagenten

3.1. GravityZone VA

In der On-Premises-Version wird GravityZone als selbst-konfigurierende virtuelle Hochsicherheits-Linux-Ubuntu-Appliance (VA) zur Verfügung gestellt, die in einem virtuellen Maschinen-Image eingebettet ist und unkompliziert über eine Befehlszeilenoberfläche installiert und konfiguriert werden kann. Die virtuelle Appliance steht in verschiedenen Formaten zur Verfügung, die mit allen gängigen Virtualisierungsplattformen kompatibel sind (OVA, XVA, VHD, OVF, RAW).

3.1.1. GravityZone-Datenbank

Die zentrale Logik der GravityZone-Architektur. Bitdefender setzt eine nicht-relationale MongoDB-Datenbank ein, um Skalierung und Replikation zu erleichtern.

3.1.2. GravityZone-Update-Server

Der Update-Server übt die wichtige Funktion aus, die GravityZone und die Endpunkt-Agenten auf dem neuesten Stand zu halten, indem er die nötigen Pakete oder Installationsdateien repliziert und veröffentlicht.

3.1.3. GravityZone-Kommunikationsserver

Der Kommunikationsserver stellt das Bindeglied zwischen den Sicherheitsagenten und der Datenbank dar. Er übermittelt Richtlinien und Aufgaben an geschützte Endpunkte sowie die von Sicherheitsagenten gemeldeten Ereignisse.

3.1.4. Web-Konsole (GravityZone Control Center)

Die Sicherheitslösungen in Bitdefender werden über die Control Center-Web-Konsole von zentraler Stelle aus verwaltet. Dies erleichtert die Verwaltung und den Zugriff auf die allgemeine Sicherheitslage sowie auf globale Sicherheitsrisiken und ermöglicht zudem die zentrale Steuerung der Sicherheitsdienste, die virtuelle und physische Arbeitsplatzrechner, Server und Mobilgeräte schützen. Dank der Gravity-Architektur ist Control Center in der Lage, die Anforderungen selbst größter Unternehmen zu erfüllen.

Das Control Center lässt sich mit den bestehenden Systemverwaltungs- und Überwachungssystemen integrieren und macht es damit einfacher, nicht verwaltete Arbeitsplatzrechner, Server und Mobilgeräte automatisch zu schützen, die in Microsoft Active Directory, VMware vCenter, Nutanix Prism Element oder Citrix XenServer aufgeführt werden oder einfach im Netzwerk gefunden werden.

3.1.5. Report-Builder-Datenbank

Die Rolle Report-Builder-Datenbank stellt die nötigen Daten für die Erstellung abfragebasierter Berichte zur Verfügung.

3.1.6. Berichterstellungs-Verarbeitungsmodule

Die Report-Builder-Prozessorenrolle ist essenziell für die Erstellung, Verwaltung und Speicherung der abfragebasierten Berichte, die Informationen aus der Report-Builder-Datenbank verwenden.

3.2. Security Server

Security Server ist eine virtuelle Maschine, die eigens für die Deduplizierung und Zentralisierung eines Großteils der Malware-Schutzfunktionen der Malware-Schutz-Agenten entwickelt wurde und als Scan-Server fungiert.

Es gibt drei Security Server-Versionen für jeden Typ von Virtualisierungsumgebung:

- **Security Server for VMware NSX.** Diese Version wird automatisch auf jedem Host im Cluster installiert, auf dem Bitdefender bereitgestellt wurde.
- **Security Server für VMware vShield-Endpoint.** Diese Version muss auf jedem Host installiert sein, der geschützt werden soll.
- **Security Server Multi-Plattform.** Diese Version ist für verschiedene andere virtualisierte Umgebungen gedacht und muss auf einem oder mehreren Hosts installiert sein, um die gewünschte Anzahl an virtuellen Maschinen gewährleisten zu können. Bei Verwendung von HVI muss ein Security Server auf jedem Host installiert sein, der zu schützende virtuelle Maschinen enthält.

3.3. HVI-Ergänzungspaket

Das HVI-Paket stellt die Verbindung zwischen Hypervisor und dem Security Server auf diesem Host sicher. So ist der Security Server in der Lage, den Speicher des Hosts, auf dem er installiert ist, unter Beachtung der GravityZone-Sicherheitsrichtlinien zu überwachen.

3.4. Sicherheitsagenten

Um Ihr Netzwerk mit Bitdefender zu schützen, müssen Sie die entsprechenden GravityZone-Sicherheitsagenten auf Endpunkten im Netzwerk installieren.

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

3.4.1. Bitdefender Endpoint Security Tools

GravityZone stellt den Schutz physischer und virtueller Maschinen unter Windows und Linux mit Bitdefender Endpoint Security Tools sicher. Dabei handelt es sich um einen intelligenten Sicherheitsagenten, der die Umgebung, in der er eingesetzt wird, erkennt, und sich entsprechend an die Ressourcen des Endpunkttyps anpasst. Bitdefender Endpoint Security Tools kann sowohl auf virtuellen und physischen Computern bereitgestellt werden und stellt ein flexibles Scan-System zur Verfügung, das es zur perfekten Wahl für heterogene Umgebungen (physisch, virtuell und Cloud) macht.

Bitdefender Endpoint Security Tools schützt nicht nur das Dateisystem, sondern auch Microsoft-Exchange-Mail-Server.

Bitdefender Endpoint Security Tools benötigt nur eine einzige Richtlinienvorlage für physische und virtuelle Maschinen und nur ein einziges Installationskit für physische und virtuelle Umgebungen mit Windows.

Schutzebenen

Die folgenden Sicherheitsebenen stehen in Bitdefender Endpoint Security Tools zur Verfügung:

- Malware-Schutz
- Advanced Threat Control
- HyperDetect
- Firewall
- Inhalts-Steuerung
- Network Attack Defense
- Patch-Verwaltung
- Gerätesteuerung
- Full Disk Encryption
- Security for Exchange
- Sandbox Analyzer
- Anwendungssteuerung

Endpunktrollen

- Power-User
- Relais
- Patch-Cache-Server
- Exchange-Schutz

Power-User

Control-Center-Administratoren können über Richtlinieneinstellungen bestimmten Endpunkt-Benutzern Power-User-Rechte gewähren. Mit dem Power-User-Modul können Benutzern Administratorrechte verliehen werden, mit denen sie über die lokale Konsole Sicherheitseinstellungen anzeigen und verändern können. Im Control Center wird eine Benachrichtigung angezeigt, wenn ein Endpunkt sich im Power-User-Modus befindet, und Control Center-Administratoren können lokale Sicherheitseinstellungen immer außer Kraft setzen.

Wichtig
Dieses Modul steht nur für unterstützte Windows-Desktop- und -Server-Betriebssysteme zur Verfügung. Weitere Informationen finden Sie im Kapitel „Unterstützte Betriebssysteme“ (S. 29).

Relais

Endpunktagenten mit der Rolle Bitdefender Endpoint Security Tools Relay fungieren als Kommunikations-Proxy- und Update-Server für andere Endpunkte im Netzwerk. Endpunkt-Agenten mit Relais-Rolle werden besonders in Unternehmen mit isolierten Netzwerken benötigt, in denen sämtlicher Datenverkehr über einen einzelnen Zugangspunkt läuft.

In Unternehmen mit großen, geographisch dezentralen Netzwerken reduzieren Relais-Agenten die benötigte Bandbreite, indem sie verhindern, dass geschützte Endpunkte und Security Server eine direkte Verbindung zur GravityZone herstellen.

Nachdem ein Bitdefender Endpoint Security Tools Relay im Netzwerk installiert wurde, können andere Endpunkte per Richtlinie so konfiguriert werden, dass sie über den Relais-Agenten mit dem Control Center kommunizieren.

Bitdefender Endpoint Security Tools Relay-Agenten dienen den folgenden Zwecken:

- Alle ungeschützten Endpunkte im Netzwerk finden.
- Den Endpunkt-Agenten im lokalen Netzwerk installieren.
- Geschützte Endpunkte im Netzwerk auf dem neuesten Stand halten.
- Die Kommunikation zwischen dem Control Center und verbundenen Endpunkten gewährleisten.
- Als Proxy-Server für geschützte Endpunkte fungieren.
- Optimierung des Netzwerkverkehrs während der Durchführung von Updates, Installationen, Scan-Vorgängen und anderen ressourcenintensive Aufgaben.

Patch-Cache-Server

Endpunkte mit einer Relais-Rolle können auch als Patch-Cache-Server fungieren. Wird diese Rolle aktiviert, speichern die Relais die von den Anbieter-Websites heruntergeladenen Software-Patches und verteilen diese auf den Zielendpunkten in Ihrem Netzwerk. Gibt es auf einem Endpunkt Software, für die ein Patch verfügbar ist, wird dieser Patch vom dem Server und nicht von der Anbieter-Website heruntergeladen. Dadurch entsteht weniger Datenverkehr und die Bandbreitenauslastung wird optimiert.

Wichtig
Diese zusätzliche Rolle ist mit einem registrierten Patch-Verwaltung-Add-on verfügbar.

Exchange-Schutz

Bitdefender Endpoint Security Tools mit Exchange-Rolle kann auf Microsoft-Exchange-Servern installiert werden, um Exchange-Benutzer vor per E-Mail übertragenen Gefahren zu schützen.

Bitdefender Endpoint Security Tools mit Exchange-Rolle schützt sowohl den Server selbst als auch die Lösung Microsoft Exchange.

3.4.2. Endpoint Security for Mac

Endpoint Security for Mac ist ein Sicherheitsagent für Intel-basierte Macintosh-Computer und -Laptops. Die verfügbare Scan-Technologie ist **Lokaler Scan**; alle Sicherheitsinhalte werden dabei lokal gespeichert.

Schutzebenen

Die folgenden Sicherheitsebenen stehen in Endpoint Security for Mac zur Verfügung:

- Malware-Schutz
- Advanced Threat Control
- Inhalts-Steuerung
- Gerätesteuerung
- Full Disk Encryption

3.4.3. GravityZone Mobile Client

Mit GravityZone Mobile Client lassen sich Sicherheitsrichtlinien leicht auf eine beliebige Anzahl von Android- und iOS-Geräten anwenden und diese Geräte so vor unbefugtem Zugriff, Riskware und Datendiebstahl schützen. Zu den

Sicherheitsfunktionen gehören Bildschirmsperre, Authentifizierungskontrolle und Geräteortung, Datenlöschung per Fernzugriff und Erkennung von Geräten mit Root oder Jailbreak sowie Sicherheitsprofile. Auf Android-Geräten wird die Sicherheit noch einmal durch Echtzeit-Scans und die Verschlüsselung von Wechselmedien erhöht.

GravityZone Mobile Client wird ausschließlich über den Apple App Store und Google Play vertrieben.

3.4.4. Bitdefender Tools (vShield)

Bitdefender Tools ist ein leichter Agent für virtualisierte, mit vShield Endpoint intergrierte VMware-Umgebungen. Der Sicherheitsagent wird auf virtuellen, durch Security Server geschützte Maschinen installiert und ermöglicht Ihnen die folgenden zusätzlichen Funktionalitäten:

- Ermöglicht Speicher- und Prozess-Scan-Aufgaben auf virtuellen Maschinen.
- Informiert den Benutzer über die gefundenen Infektionen und die daraufhin ausgeführten Aktionen.
- Fügt weitere Optionen für Anti-Malware-Scan-Ausschlüsse hinzu.

3.5. Sandbox Analyzer-Architektur

Der Bitdefender Sandbox Analyzer bietet hohe Sicherheit vor raffinierten Bedrohungen, indem automatische, detaillierte Analysen verdächtiger Dateien durchgeführt werden; selbst solcher Dateien, die noch keine Signatur von den Bitdefender-Malware-Schutz-Engines erhalten haben.

Sandbox Analyzer ist in zwei Varianten erhältlich:

- Sandbox Analyzer Cloud, von Bitdefender gehostet.
- Sandbox Analyzer On-Premises, verfügbar als virtuelle Appliance, die lokal bereitgestellt werden kann.

Sandbox Analyzer Cloud

Sandbox Analyzer Cloud umfasst die folgenden Komponenten:

- **Sandbox Analyzer-Portal** – ein gehosteter Kommunikationsserver, der Anfragen zwischen Endpunkten und dem Bitdefender-Sandbox-Cluster bearbeitet.

- **Sandbox Analyzer-Cluster** – die gehostete Sandbox-Infrastruktur, innerhalb derer die virtuelle Verhaltensanalyse abläuft. Auf dieser Ebene werden die übermittelten Dateien auf virtuellen Maschinen unter Windows 7 ausgeführt.

Das **GravityZone Control Center** dient als Verwaltungs- und Berichtskonsole, über die Sicherheitsrichtlinien konfiguriert und Analyseberichte sowie Benachrichtigungen angezeigt werden können.

Bitdefender Endpoint Security Tools ist der auf Endpunkten installierte Sicherheitsagent, der als Einspeisungssensor für den Sandbox Analyzer fungiert.

Sandbox Analyzer On-Premises

Sandbox Analyzer On-Premises wird als virtuelle Linux Ubuntu-Appliance ausgeliefert, die in ein virtuelles Maschinen-Image eingebettet, einfach zu installieren und über eine Befehlszeilenschnittstelle (CLI) zu konfigurieren ist. Sandbox Analyzer On-Premises ist im OVA-Format verfügbar und kann auf VMWare ESXi installiert werden.

Eine Sandbox Analyzer On-Premises-Instanz umfasst die folgenden Komponenten:

- **Sandbox-Manager**. Diese Komponente ist der Sandbox-Orchestrator. Der Sandbox Manager verbindet sich über eine API mit dem ESXi-Hypervisor und nutzt seine Hardware-Ressourcen für den Aufbau und Betrieb der Malware-Analyse-Umgebung.
- **Virtuelle Maschinen für die Detonation**. Diese Komponente besteht aus virtuellen Maschinen, die von Sandbox Analyzer genutzt werden, um Dateien auszuführen und ihr Verhalten zu analysieren. Die virtuellen Maschinen für die Detonation können mit Windows 7 und Windows 10 64-Bit-Betriebssystemen betrieben werden.

Das **GravityZone Control Center** dient als Verwaltungs- und Berichtskonsole, über die Sicherheitsrichtlinien konfiguriert und Analyseberichte sowie Benachrichtigungen angezeigt werden können.

Sandbox Analyzer On-Premises nutzt die folgenden Einspeisungssensoren:

- **Endpunktsensor**. Bitdefender Endpoint Security Tools for Windows fungiert als auf den Endpunkten installierter Einspeisungssensor. Der Bitdefender-Agent verwendet fortschrittliche Algorithmen des maschinellen Lernens und des neuronalen Netzwerks, um verdächtige Inhalte zu erkennen und an Sandbox Analyzer zu übermitteln, einschließlich Objekte aus der zentralen Quarantäne.

- **Netzwerksensor**. Network Security Virtual Appliance (NSVA) ist eine virtuelle Appliance, die in derselben virtualisierten ESXi-Umgebung wie die Sandbox Analyzer-Instanz bereitgestellt werden kann. Der Netzwerksensor erfasst Inhalte aus Netzwerkdatenströmen und übermittelt diese an Sandbox Analyzer.
- **ICAP-Sensor**. Auf NAS-Geräten (Network Attached Storage) mit ICAP-Protokoll bereitgestellt, unterstützt Bitdefender Security Server die Übertragung von Inhalten an Sandbox Analyzer.

Zusätzlich zu diesen Sensoren unterstützt Sandbox Analyzer On-Premises auch die manuelle Übertragung und die Übertragung über die API. Weitere Einzelheiten entnehmen Sie dem Kapitel **Verwendung von Sandbox Analyzer** im GravityZone-Administratorhandbuch.

4. ANFORDERUNGEN

Alle GravityZone-Lösungen werden über das Control Center installiert und verwaltet.

4.1. GravityZone-Virtual-Appliance

4.1.1. Unterstützte Formate und Virtualisierungsplattformen

GravityZone wird als virtuelle Appliance (VA) bereitgestellt. Diese ist in den folgenden Formaten verfügbar, die die gängigsten Virtualisierungsplattformen unterstützen:

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

*OVF- und RAW-Pakete sind im Format tar.bz2 gepackt.

Mehr Details zur Kompatibilität von Oracle VM VirtualBox finden Sie in diesem Artikel.

Bitte wenden Sie sich an Bitdefender, falls Sie Unterstützung für weitere Formate oder Virtualisierungsplattformen wünschen.

4.1.2. Hardware

Die Hardwareanforderung für die virtuelle GravityZone-Appliance richten sich nach der Größe Ihres Netzwerks und der von Ihnen gewählten Bereitstellungsarchitektur. In Netzwerken mit bis zu 3.000 Endpunkten können Sie alle GravityZone-Rollen auf einer einzigen Appliance installieren. Bei größeren Netzwerken sollten Sie in Betracht ziehen, die Rollen auf mehrere Appliances zu verteilen. Die von der Appliance benötigten Ressourcen hängen davon ab, welche Rollen Sie darauf installieren und ob Sie ein Replica Set verwenden oder nicht.

Beachten Sie
Bei einem Replica Set handelt es sich um eine MongoDB-Funktion zur Replikation der Datenbank. So werden Redundanz und Hochverfügbarkeit der gespeicherten Daten garantiert. Weitere Einzelheiten finden Sie in der MongoDB-Dokumentation sowie unter „Die GravityZone-Appliance verwalten“ (S. 111).

Bitdefender HVI hat ebenfalls einen erheblichen Ressourcenbedarf. Falls Sie diesen Dienst nutzen, sehen Sie sich bitte die Tabellen mit den spezifischen Daten an. Eine Übersicht über alle Anforderungen des Dienstes finden Sie unter „HVI“ (S. 50).

Wichtig
Die Messungen sind das Ergebnis von internen Bitdefender-Tests auf einer GravityZone-Grundkonfiguration bei normaler Nutzung. Die Ergebnisse können je nach Netzwerkkonfiguration, installierter Software, Anzahl der generierten Ereignisse usw. abweichen. Für individuelle Messwerte zur Skalierbarkeit wenden Sie sich bitte an Bitdefender.

vCPU

In der folgenden Tabelle finden Sie die Anzahl der vCPUs, die jede Rolle der virtuellen Appliance anfragt.

Jede vCPU muss mindestens 2 GHz haben.

Komponente	Anzahl der Endpunkte (bis zu)							
	250	500	1000	3000	5000	10000	25000	50000
GravityZone-Grundfunktion								
Update-Server*	8	12	14	16	4	4	6	8
Web-Konsole**					6	10	12	12
Kommunikationsserver					6	10	12	18
Datenbank***					6	6	9	12
Gesamt	**8**	**12**	**14**	**16**	**22**	**30**	**39**	**50**
GravityZone mit Bitdefender HVI								
Update-Server*	8	4	4	4	4	4	6	8
Web-Konsole**		6	8	8	10	10	12	12
Kommunikationsserver		6	8	8	10	10	16	20

Komponente	Anzahl der Endpunkte (bis zu)							
	250	500	1000	3000	5000	10000	25000	50000
Datenbank***		6	6	6	6	6	9	12
Gesamt	**8**	**22**	**26**	**26**	**30**	**30**	**43**	**52**

* Empfohlen, wenn keine Relais eingesetzt werden.
** Fügen Sie für jede aktive Integration eine vCPU auf der virtuellen Appliance mit der Rolle Web-Konsole hinzu.
*** Bei verteilter Installation von Rollen zusammen mit Replica Set: Fügen Sie für jede weitere Datenbankinstanz die angegebene Anzahl zur Gesamtanzahl hinzu.

RAM (GB)

Komponente	Anzahl der Endpunkte (bis zu)							
	250	500	1000	3000	5000	10000	25000	50000
GravityZone-Grundfunktion								
Update-Server	16	16	18	20	2	2	3	3
Web-Konsole*					8	8	12	16
Kommunikationsserver					6	12	12	16
Datenbank**					8	10	12	12
Gesamt	**16**	**16**	**18**	**20**	**24**	**32**	**39**	**47**
GravityZone mit Bitdefender HVI								
Update-Server	16	2	2	2	2	2	3	3
Web-Konsole*		8	10	10	10	10	12	16
Kommunikationsserver		8	10	10	12	12	16	20
Datenbank**		8	8	8	8	12	12	12
Gesamt	**16**	**26**	**30**	**30**	**32**	**36**	**43**	**51**

* Fügen Sie für jede aktive Integration 1 GB RAM auf der virtuellen Appliance mit der Rolle Web-Konsole hinzu.
** Bei verteilter Installation von Rollen zusammen mit Replica Set: Fügen Sie für jede weitere Datenbankinstanz die angegebene Anzahl zur Gesamtanzahl hinzu.

Freier Speicherplatz (GB)

Komponente	Anzahl der Endpunkte (bis zu)								
	250	250*	500	1000	3000	5000	10000	25000	50000
GravityZone-Grundfunktion									
Update-Server	120	**160**	160	200	200	80	80	80	80
Web-Konsole						80	80	80	80
Kommunikationsserver						80	80	80	80
Datenbank**						80	120	200	500
Gesamt	**120**	**160**	**160**	**200**	**200**	**320**	**360**	**440**	**740**
GravityZone mit Bitdefender HVI									
Update-Server	120	160	80	80	80	80	80	80	80
Web-Konsole			80	80	80	80	80	80	80
Kommunikationsserver			80	80	80	80	80	80	80
Datenbank**			80	80	100	100	160	300	700
Gesamt	**120**	**160**	**320**	**320**	**340**	**340**	**400**	**540**	**940**

Wichtig
Wir empfehlen dringend die Verwendung von Solid-State-Drives (SSD).

* Zusätzlicher SSD-Speicherplatzbedarf bei Auswahl der automatischen Installation, da hierbei auch der Security Server installiert wird. Nach Abschluss der Installation können Sie den Security Server wieder deinstallieren, um wieder mehr freien Speicherplatz zu schaffen.
** Bei verteilter Installation von Rollen zusammen mit Replica Set: Fügen Sie für jede weitere Datenbankinstanz die angegebene Anzahl zur Gesamtanzahl hinzu.

4.1.3. Internetverbindung

Die GravityZone-Appliance benötigt eine aktive Internet-Verbindung.

4.2. Control Center

Folgendes wird benötigt, um die Control Center-Web-Konsole aufzurufen:

- Internet Explorer 9+, Mozilla Firefox 14+, Google Chrome 15+, Safari 5+, Microsoft Edge 20+, Opera 16+
- Empfohlene Bildschirmauflösung: mindestens 1280 x 800
- Der Computer, von dem aus Sie eine Verbindung herstellen, muss im Netzwerk mit dem Control Center verbunden sein.

Warnung
Control Center funktioniert in der Kompatibilitätsansicht des Internet Explorer 9+ nicht bzw. wird nicht richtig angezeigt. Es ist, als würden Sie eine nicht unterstützte Browserversion benutzen.

4.3. Endpunktschutz

Um Ihr Netzwerk mit Bitdefender zu schützen, müssen die GravityZone-Sicherheitsagenten auf den Netzwerk-Endpunkten installiert werden. Für bestmöglichen Schutz können Sie auch Security Server installieren. Dazu benötigen Sie einen Control Center-Benutzer mit Administratorrechten für die Dienste, die Sie installieren möchten, und für die von Ihnen verwalteten Netzwerk-Endpunkte.

Die Anforderungen an den Sicherheitsagenten sind unterschiedlich, je nachdem, ob er zusätzliche Serverrollen wie Relais, Exchange-Schutz oder Patch-Cache-Server hat. Weitere Informationen zu den Rollen des Agenten finden Sie unter „Sicherheitsagenten“ (S. 13).

4.3.1. Hardware

Sicherheitsagent ohne Rollen

CPU-Ausl.

Zielsysteme	CPU-Typ	Unterstützte Betriebssysteme
Arbeitsplatzrechner	Mit Intel® Pentium kompatible Prozessoren, mindestens 2 GHz	Microsoft-Windows-Desktop-Betriebssystem
	Intel® Core 2 Duo, mindestens 2 GHz	macOS
Intelligente Geräte	Mit Intel® Pentium kompatible Prozessoren, mindestens 800 MHZ	Eingebettete Microsoft-Windows-Betriebssysteme
Server	Minimalanforderung: Mit Intel® Pentium kompatible Prozessoren, 2.4 GHz	Microsoft-Windows-Server- Betriebssysteme und Linux-Betriebssysteme
	Empfohlen: Intel® Xeon Multi-Core CPU, mindestens 1.86 GHz	

Warnung
ARM-Prozessoren werden derzeit nicht unterstützt.

Freier RAM

Bei Installation (MB)

BS	EINZELNE ENGINE					
	Lokales Scan -Verfahren		Hybrid-Scan -Verfahren		Zentrales Scan -Verfahren	
	Nur AV	Voller Umf.	Nur AV	Voller Umf.	Nur AV	Voller Umf.
Windows	1024	1200	512	660	256	400
Linux	1024	1024	512	512	256	256
macOS	1024	1024	k.A.	k.A.	k.A.	k.A.

Bei täglicher Nutzung (MB)*

BS	Virenschutz (Single Engine)			Schutzmodule				
	Lokal	Hybrid	Zentralisiert	Verhaltens -Scan	Firewall	Inhalts-Steuerung	Power-User	Update-Server
Windows	75	55	30	+13	+17	+41	+29	+80
Linux	200	180	90	-	-	-	-	-
macOS	650	-	-	+100	-	+50	-	-

* Angegeben ist der Bedarf für die tägliche Nutzung des Endpunkt-Clients, ohne zusätzliche Aufgaben wie Bedarf-Scans oder Produkt-Updates.

Freier Festplattenspeicher

Bei Installation (MB)

BS	EINZELNE ENGINE						ZWEI ENGINES			
	Lokales Scan -Verfahren		Hybrid-Scan -Verfahren		Zentrales Scan -Verfahren		Zentrales + lokales Scan-Verfahren		Zentrales + Hybrid-Scan -Verfahren	
	Nur AV	Voller Umf.	Nur AV	Voller Umf.	Nur AV	Voller Umf.	Nur AV	Voller Umf.	Nur AV	Voller Umf.
Windows	1024	1200	500	700	350	570	1024	1200	500	700
Linux	1600	1600	1100	1100	600	600	1600	1600	1100	1100

BS	EINZELNE ENGINE						ZWEI ENGINES			
	Lokales Scan -Verfahren		Hybrid-Scan -Verfahren		Zentrales Scan -Verfahren		Zentrales + lokales Scan-Verfahren		Zentrales + Hybrid-Scan -Verfahren	
	Nur AV	Voller Umf.	Nur AV	Voller Umf.	Nur AV	Voller Umf.	Nur AV	Voller Umf.	Nur AV	Voller Umf.
macOS	1024	1024	k.A.	k.A.	k.A.	k.A.	k.A.	k.A.	k.A.	k.A.

Bei täglicher Nutzung (MB)*

BS	Virenschutz (Single Engine)			Schutzmodule				
	Lokal	Hybrid	Zentralisiert	Verhaltens -Scan	Firewall	Inhalts-Steuerung	Power-User	Update-Server
Windows	410	190	140	+12	+5	+60	+80	+10
Linux	500	200	110	-	-	-	-	-
macOS	1700	-	-	+20	-	+0	-	-

* Angegeben ist der Bedarf für die tägliche Nutzung des Endpunkt-Clients, ohne zusätzliche Aufgaben wie Bedarf-Scans oder Produkt-Updates.

Sicherheitsagent mit Relais-Rolle

Die Relay-Rolle benötigt über die Grundkonfiguration des Sicherheitsagenten hinausgehende weitere Hardware-Ressourcen. Diese Anforderungen dienen der Unterstützung des Update-Servers und der vom Endpunkt gehosteten Installationspakete:

Anzahl der verbundenen Endpunkte	CPU zur Update-Server-Unterstützung	RAM	Freier Speicherplatz für Update-Server
1-300	Mindestens Intel® Core™ i3 oder gleichwertiger Prozessor, 2 vCPU pro Kern	1.0 GB	10 GB

Anzahl der verbundenen Endpunkte	CPU zur Update-Server-Unterstützung	RAM	Freier Speicherplatz für Update-Server
300-1000	Mindestens Intel® Core™ i5 oder gleichwertiger Prozessor, 4 vCPU pro Kern	1.0 GB	10 GB

Warnung

- ARM-Prozessoren werden derzeit nicht unterstützt.
- Relais-Agente erfordern SSD-Festplatten, um die hohe Anzahl der Lese- und Schreibvorgänge unterstützen zu können.

Wichtig

- Wenn Sie die Installationspakete und Updates auf einer anderen Partition als der, auf der der Agent installiert ist, speichern möchten, stellen Sie sicher, dass beide Partitionen über ausreichend freien Speicherplatz (10 GB) verfügen, andernfalls bricht der Agent die Installation ab. Dies ist nur bei der Installation erforderlich.
- Auf Windows-Endpunkten müssen die symbolischen Links für lokal zu lokal aktiviert sein.

Sicherheitsagent mit Exchange-Schutz-Rolle

Die Quarantäne für Exchange-Server benötigt zusätzlichen Festplattenspeicher auf der Partition, auf der der Sicherheitsagent installiert ist.

Die Größe der Quarantäne hängt davon ab, wie viele Objekte sich darin befinden und wie groß diese sind.

Standardmäßig wird der Agent auf der Systempartition installiert.

Sicherheitsagent mit Patch-Cache-Server-Rolle

Der Agent mit der Patch-Cache-Server-Rolle muss alle der folgenden Anforderungen erfüllen:

- Alle Hardware-Anforderungen des einfachen Sicherheitsagenten (ohne Rollen)
- Alle Hardware-Anforderungen der Relais-Rolle
- Zusätzlich weitere 100 GB freier Speicherplatz zur Speicherung der heruntergeladenen Patches

Wichtig
Wenn Sie die Patches auf einer anderen Partition als der, auf der der Agent installiert ist, speichern möchten, stellen Sie sicher, dass beide Partitionen über ausreichend freien Speicherplatz (100 GB) verfügen, andernfalls bricht der Agent die Installation ab. Dies ist nur bei der Installation erforderlich.

Anforderungen für VMware-vShield-Umgebungen

Dies sind die Bitdefender Tools-Anforderungen und der Ressourcenverbrauch für Systeme, die mit vShield Endpoint in VMware-Umgebungen integriert sind.

Plattform	RAM	Speicherplatz
Windows	6-16* MB (~ 10 MB für die GUI)	24 MB
Linux	9-10 MB	10-11 MB

*5 MB, wenn der Hintergrund-Modus aktiviert ist, 10 MB, wenn er deaktiviert ist. Wenn der Hintergrund-Modus aktiviert ist, wird die Benutzeroberfläche von Bitdefender Tools (GUI) nicht automatisch beim Systemstart geladen. Hierdurch werden Ressourcen freigesetzt.

4.3.2. Unterstützte Betriebssysteme

Windows Desktop

- 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-Update vom . October 2018 (Redstone 5)
- Windows 10 April 2018 Update (Redstone 4)
- Windows 10 Fall Creators Update (Redstone 3)
- Windows 10 Creators Update (Redstone 2)
- Windows 10 Anniversary Update (Redstone 1)
- Windows 10 November Update (Threshold 2)
- Windows 10

- Windows 8.1[(1)(2)]
- Windows 8[(3)]
- Windows 7

Warnung
(1) VMware vShield (agentenlose Version) unterstützt Windows 8.1 (32-/64-Bit) ab VMware vSphere 5.5 – ESXi Build 1892794.
(2) In VMware NSX wird die Betriebssystemversion ab vSphere 5.5 Patch 2 unterstützt.
(3) In VMware NSX wird die Betriebssystemversion ab vSphere 5.5 unterstützt.

Warnung
Bitdefender unterstützt keine Windows-Insider-Programm-Builds.

Windows-Tablet und Embedded

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

Windows Server

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

Warnung
(1) VMware vShield (agentenlose Version) unterstützt Windows Server 2012 R2 (64-Bit) ab VNware vSphere 5.5 – ESXi Build 1892794.
(2) In VMware NSX wird die Betriebssystemversion ab vSphere 5.5 Patch 2 unterstützt.
(3) In VMware NSX wird die Betriebssystemversion ab vSphere 5.5 unterstützt.
(4) VMware NSX unterstützt die 32-Bit-Versionen von Windows 2012 und Windows Server 2008 R2 nicht.

Linux

Wichtig
Linux-Endpunkte verwenden Lizenzplätze aus dem Pool der Lizenzen für Server-Betriebssysteme.

- Ubuntu 14.04 LTS oder höher
- Red Hat Enterprise Linux / CentOS 6.0 oder höher(2)
- SUSE Linux Enterprise Server 11 SP 4 oder neuer
- OpenSUSE Leap 42.x
- Fedora 25 oder höher(1)
- Debian 8.0 oder höher
- Oracle Linux 6.3 oder höher
- Amazon Linux AMI 2016.09 oder höher
- Amazon Linux 2

Warnung
(1) Unter Fedora 28 (und neueren Versionen) muss für Bitdefender Endpoint Security Tools das Paket `libnsl` manuell installiert werden. Führen Sie dazu den folgenden Befehl aus:

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

(2) Bei Minimalinstallationen von CentOS muss für Bitdefender Endpoint Security Tools das Paket `libnsl` manuell installiert werden. Führen Sie dazu den folgenden Befehl aus:

```
sudo yum install libnsl
```

Voraussetzungen für Active Directory

Bei der Integration von Linux-Endpunkten mit einer Active-Directory-Domäne über den System Security Services Daemon (SSSD) müssen Sie darauf achten, dass die Tools **ldbsearch, krb5-user,** und **krb5-config** installiert sind und kerberos ordnungsgemäß konfiguriert ist.

```
/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
        }
```

Beachten Sie
Es wird bei allen Eingaben zwischen Groß- und Kleinschreibung unterschieden.

Zugriff-Scan-Unterstützung

Zugriff-Scans sind auf allen unterstützten Gast-Betriebssystemen möglich. Auf Linux-Systemen werden Zugriff-Scans in den folgenden Fällen unterstützt:

Kernel-Versionen	Linux-Distributionen	Voraussetzungen für Zugriff-Scans
2.6.38 oder höher*	Red Hat Enterprise Linux / CentOS 6.0 oder höher Ubuntu 14.04 oder höher SUSE Linux Enterprise Server 11 SP 4 oder neuer OpenSUSE Leap 42.x Fedora 25 oder höher Debian 9.0 oder höher Oracle Linux 6.3 oder höher Amazon Linux AMI 2016.09 oder höher	**Fanotify** (Kernel-Option) muss aktiviert sein.
2.6.38 oder höher	Debian 8	**Fanotify** muss aktiviert und im „Enforcing"-Modus sein und anschließend das Kernel-Paket neu gebaut werden. Weitere Einzelheiten finden Sie in diesem Artikel in der Wissensdatenbank.

Kernel-Versionen	Linux-Distributionen	Voraussetzungen für Zugriff-Scans
2.6.32 - 2.6.37	CentOS 6.x Red Hat Enterprise Linux 6.x	Bitdefender bietet Support über **DazukoFS** mit vorgefertigten Kernel-Modulen an.
Alle anderen Kernel	Alle anderen unterstützten Systeme	Das **DazukoFS**-Modul muss manuell kompiliert werden. Weitere Informationen finden Sie unter „Kompilieren Sie das DazukoFS-Modul manuell“ (S. 162).

* Mit bestimmten Einschränkungen (siehe unten).

Einschränkungen bei Zugriff-Scans

Kernel-Versionen	Linux-Distributionen	Details
2.6.38 oder höher	Alle unterstützten Systeme	Zugriff-Scans können nur unter folgenden Bedingungen zur Überwachung von gemounteten Netzwerkfreigaben eingesetzt werden: • **Fanotify** ist auf Remote- und lokalen Systemen aktiviert. • Die Freigabe basiert auf dem CIFS- und NFS-Dateisystem. **Beachten Sie** Der Zugriff-Scan prüft keine Netzwerkfreigaben, die mit SSH oder FTP gemountet wurden.
Alle Kernel	Alle unterstützten Systeme	Auf Systemen mit **DazukoFS** werden Zugriff-Scans nicht für Netzwerkfreigaben unterstützt, die in Pfaden eingehängt sind, die bereits durch das Zugriff-Scan-Modul geschützt werden.

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)

Die Inhaltssteuerung wird von macOS Big Sur (11.0) nicht unterstützt.

4.3.3. Unterstützte Dateisysteme

Bitdefender kann auf den folgenden Dateisystemen installiert werden und diese schützen:

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

Beachten Sie
Bei NFS und CIFS/SMB werden Zugriff-Scans nicht unterstützt.

4.3.4. Unterstützte Web-Browser

Security for Endpoints funktioniert mit folgenden Browsern:

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

4.3.5. Unterstützte Virtualisierungsplattformen

Security for Virtualized Environments ist auf den folgenden Virtualisierungsplattformen sofort einsatzbereit:

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

  Beachten Sie
  Die Workload-Management-Funktionalität in vSphere 7.0 wird nicht unterstützt.

- 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 or 5.5 (einschließlich Xen Hypervisor)
- Citrix Virtual Apps and Desktops 7 1808, 7 1811, 7 1903, 7 1906
- Citrix XenApp and 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 oder Windows Server 2008 R2, 2012, 2012 R2 (inkl. Hyper-V Hypervisor)
- Red Hat Enterprise Virtualization 3.0 (inkl. 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

Beachten Sie
Der Support oder Virtualisierungsplattformen kann auf Anfrage bereitgestellt werden.

Anforderungen für die Integration mit VMware NSX-V

- Ab ESXi 5.5 für jeden Server
- Ab vCenter Server 5.5
- Ab NSX Manager 6.2.4
- VMware Tools 9.1.0 oder neuer mit Guest Introspection Thin Agent.

- Weitere Informationen zu Windows-VMs finden Sie in diesem Artikel.
- Weitere Informationen zu Linux-VMs finden Sie in diesem Artikel.

Beachten Sie
VMware empfiehlt die folgenden Versionen der VMware Tools:

- 10.0.8 oder neuer, um mit langsamen VMs nach einem Upgrade von VMware Tools in NSX / vCloud Networking and Security umzugehen (VMware Knowledge-Base-Artikel 2144236).
- 10.0.9 oder neuer zur Unterstützung von Windows 10.

Wichtig
Es wird empfohlen, alle VMware-Produkte stets mit dem neuesten Patch auf dem neuesten Stand zu halten.

Voraussetzungen für die Integration mit VMware NSX-T Data Center

- VMware NSX-T Manager 2.4, 2.5 oder 3.0
- ESXi, kompatibel mit der NSX-T Manager-Version
- vCenter Server & vSphere, kompatibel mit der NSX-T Manager-Version
- VMware Tools mit Guest Introspection Thin Agent, kompatibel mit der NSX-T Manager-Version

Weitere Einzelheiten zur Kompatibilität finden Sie auf den folgenden VMware-Webseiten:

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

Voraussetzungen für die Integration mit Nutanix Prism Element

- Anmeldedaten eines Nutanix Prism Element-Benutzers mit Administratorrechten (Cluster Admin oder User Admin)
- Nutanix Prism with AOS (LTS) 5.5, 5.10, 5.15
- Nutanix Prism with AOS (STS) 5.6, 5.11, 5.18
- Nutanix Prism with AHV (Community Edition) 20170830.115, 20170830.301, 20170830.395, 20190916.294

Unterstützte Cloud-Plattformen

Neben On-Premises-Virtualisierungsumgebungen lässt sich GravityZone zudem mit den folgenden Cloud-Plattformen integrieren:

- **Amazon EC2**

  Als Amazon-EC2-Kunde können Sie das Inventar der EC2-Instanzen gruppiert nach Regionen und Verfügbarkeitszonen mit dem GravityZone-Netzwerkinventar integrieren.

- **Microsoft Azure**

  Als Microsoft-Azure-Kunde können Sie das Inventar der virtuellen Maschinen in Microsoft-Azure gruppiert nach Regionen und Verfügbarkeitszonen mit dem GravityZone-Netzwerkinventar integrieren.

Kompatibilität mit Technologien zur Desktop- und Anwendungsvirtualisierung

GravityZone ist mit den folgenden Virtualisierungstechnologien kompatibel, beginnend mit Bitdefender Endpoint Security Tools Version 6.6.16.226:

- **VMware:**

  VMware V-App (gleiche Version mit vCenter Server)

  VMware ThinApp 5.2.6

  VMware AppVolumes 2.180

  Wichtig
  Es wird empfohlen, nicht im Anwendungs-Stack oder beschreibbare Volumes zu installieren.

- **Microsoft:**

  Microsoft App-V 5.0, 5.1

  Microsoft FSLogix 2.9.7237

- **Citrix:**

  Citrix App Layering 19.10

  Citrix Appdisks 7.12

Wichtig
Weisen Sie Richtlinien auf der Grundlage von Benutzerregeln zu, so dass die Gerätesteuerung die Erstellung von Betriebssystem- und Plattformebenen nicht verhindert.
Möglicherweise müssen Sie die GravityZone-Firewall-Regeln konfigurieren, um den Netzwerkverkehr für jede dieser Anwendungen zuzulassen. Weitere Informationen finden Sie unter Citrix App Layering-Produktdokumentation.

Unterstützte Virtualisierungs-Verwaltungs-Tools

Control Center lässt sich derzeit mit den folgenden Virtualisierungs-Verwaltungs-Tools integrieren:

- VMware vCenter Server
- Citrix XenServer
- Nutanix Prism Element

Um die Integration einzurichten, müssen Sie Benutzernamen und Passwort eines Administrators eingeben.

4.3.6. Security Server

Security Server ist eine vorkonfigurierte virtuelle Maschine, die auf einem Ubuntu Server mit den folgenden Versionen läuft:

- 16.04 (VMware NSX und Multi-Plattform)
- 12.04 LTS (VMware vShield)

Arbeitsspeicher und CPU

Die Zuteilung der Arbeitsspeicher- und CPU-Ressourcen für den Security Server hängt von der Anzahl und Art der VMs ab, die auf dem Host laufen. In der folgenden Tabelle sind die empfohlenen Ressourcen aufgeführt:

Anzahl geschützter VMs	RAM	CPUs
1-50 VMs	2 GB	2 CPUs
51-100 VMs	2 GB	4 CPUs
101-200 VMs	4 GB	6 CPUs

Die vordefinierte Hardware-Konfiguration von Security Server for NSX (CPU und RAM) kann im VMware vSphere Web Client angepasst werden, indem Sie die Maschine ausschalten, ihre Einstellungen bearbeiten und sie wieder einschalten. Detaillierte Informationen finden Sie unter „Installation von Security Server for VMware NSX“ (S. 130).

Speicherplatz (Festplatte)

Umgebung	Bereitstellung von Festplattenspeicherplatz
VMware NSX-V / NSX-T	40 GB
VMware mit vShield Endpoint	40 GB
Sonstige	16 GB

Security Server-Verteilung auf Hosts

Umgebung	Security Server vs. Hosts
VMware NSX-V / NSX-T	Security Server wird zum Zeitpunkt der Bereitstellung des Bitdefender-Dienstes automatisch auf jedem ESXi-Host im zu schützenden Cluster installiert.
VMware mit vShield Endpoint	Security Server muss auf jedem ESXi-Host installiert werden, der geschützt werden soll.
Sonstige	Es ist zwar nicht zwingend erforderlich, aber Bitdefender empfiehlt, zur Verbesserung der Leistung Security Server auf jedem physischen Host zu installieren.

Netzwerklatenz

Die Kommunikationslatenz zwischen Security Server und den geschützten Endpunkten muss unter 50 ms liegen.

Speicherschutzlast

Der Speicherschutz wirkt sich bei einem Scan von 20 GB wie folgt auf den Security Server aus:

Status des Speicherschutzes	Security Server-Ressourcen	Security Server-Last	Übertragungszeit (mm:ss)
Deaktiviert (Baseline)	N/A	N/A	10:10
Aktiviert	4 vCPUs 4 GB RAM	Normal	10:30
Aktiviert	2 vCPUs 2 GB RAM	Hoch	11:23

Beachten Sie
Diese Ergebnisse wurden mit verschiedenen Typen von Musterdateien (.exe, .txt, .doc, .eml, .pdf, .zip etc.) zwischen 10 KB und 200 MB erzielt. Die Übertragungszeit entspricht 20 GB Daten in insgesamt 46.500 Dateien.

4.3.7. Bandbreitennutzung

- **Benötigte Bandbreite für Produkt-Updates zwischen dem Endpunkt-Client und dem Update-Server**

  Durch jedes regelmäßige Produkt-Update für Bitdefender Endpoint Security Tools entsteht der folgende Download-Datenverkehr an jedem Endpunkt-Client:

  - Unter Windows: ~20 MB
  - Unter Linux: ~26 MB
  - Unter macOS: ~25 MB

- **Datenverkehr für heruntergeladene Sicherheitsinhalte zwischen Endpunkt-Client und Update-Server (MB/Tag)**

Update-Server-Typ	Scan-Engine-Typ		
	Lokal	Hybrid	Zentrales
Relais	65	58	55
Öffentlicher Bitdefender-Update-Server	3	3.5	3

- **Für zentralisierte Scans benötigte Bandbreite zwischen dem Endpunkt-Client und dem Security Server**

Gescannte Objekte	Art des Datenverkehrs		Download (MB)	Upload (MB)
Dateien*	Erster Scan		27	841
	Gecachter Scan		13	382
Websites**	Erster Scan	Internet-Datenverkehr	621	N/A
		Security Server	54	1050
	Gecachter Scan	Internet-Datenverkehr	654	N/A
		Security Server	0.2	0.5

* Die angegebenen Daten basieren auf einem Dateivolumen von 3,49 GB (6.658 Dateien), wovon 1,16 GB auf PE-Dateien (Portable Executable) entfallen.

** Die angegebenen Daten basieren auf den 500 bestbewerteten Websites.

- **Hybrid-Scan-Datenverkehr zwischen dem Endpunkt-Client und Bitdefender Cloud Services.**

Gescannte Objekte	Art des Datenverkehrs	Download (MB)	Upload (MB)
Dateien*	Erster Scan	1.7	0.6
	Gecachter Scan	0.6	0.3
Internet-Datenverkehr**	Internet-Datenverkehr	650	N/A
	Bitdefender Cloud Services	2.6	2.7

* Die angegebenen Daten basieren auf einem Dateivolumen von 3,49 GB (6.658 Dateien), wovon 1,16 GB auf PE-Dateien (Portable Executable) entfallen.

** Die angegebenen Daten basieren auf den 500 bestbewerteten Websites.

- **Datenverkehr zwischen Bitdefender Endpoint Security Tools Relay-Clients und Update-Server zum Herunterladen von Sicherheitsinhalten**

  Clients mit der Bitdefender Endpoint Security Tools Relay laden bei jedem unterstützten Betriebssystem ca. ~16 MB / Tag* vom Update-Server herunter.

  * Verfügbar für Bitdefender Endpoint Security Tools ab Version 6.2.3.569.

- **Datenverkehr zwischen Endpunkt-Clients und dem Control Center**

  Durchschnittlich entsteht pro Tag 618 KB an Datenverkehr zwischen Endpunkt-Clients und dem Control Center.

4.4. Exchange-Schutz

Security for Exchange wird durch Bitdefender Endpoint Security Tools bereitgestellt, das sowohl das Dateisystem als auch den Microsoft Exchange-Mail-Server schützt.

4.4.1. Unterstützte Microsoft-Exchange-Umgebungen

Security for Exchange unterstützt die folgenden Microsoft-Exchange-Versionen und -Rollen:

- Exchange Server 2019 mit Edge-Transport- oder Mailbox-Rolle
- Exchange Server 2016 mit Edge-Transport- oder Mailbox-Rolle
- Exchange Server 2013 mit Edge-Transport- oder Mailbox-Rolle
- Exchange Server 2010 mit Edge-Transport-, Hub-Transport- oder Mailbox-Rolle
- Exchange Server 2007 mit Edge-Transport-, Hub-Transport- oder Mailbox-Rolle

Security for Exchange ist mit Microsoft-Exchange-Datenbankverfügbarkeitsgruppen kompatibel.

4.4.2. Systemanforderungen

Security for Exchange ist mit jedem physischen oder virtuellen 64-Bit-Server (Intel oder AMD) kompatibel, der eine unterstützte Microsoft-Exchange-Server-Version und -Rolle hat. Weitere Informationen zu Systemvoraussetzungen für Bitdefender Endpoint Security Tools finden Sie unter „Sicherheitsagent ohne Rollen“ (S. 25).

Empfohlene verfügbare Server-Ressourcen:

- Freier RAM: 1 GB
- Freier Festplattenspeicher: 1 GB

4.4.3. Andere Software-Anforderungen

- Für Microsoft Exchange Server 2013 mit Service Pack 1: KB2938053 von Microsoft.
- Für Microsoft Exchange Server 2007: .NET Framework 3.5 Service Pack 1 oder neuer

4.5. Sandbox Analyzer On-Premises

Sandbox Analyzer On-Premises hat die folgenden spezifischen Anforderungen:

- ESXi Hypervisor (die Virtualisierungsplattform, auf der die Umgebung ausgeführt wird).
- Sandbox Analyzer Virtual Appliance (die Management-Appliance, die die virtuellen Maschinen zur Detonation steuert).
- Network Security Virtual Appliance (eine VM, die einen Netzwerksensor einschließt, der in der Lage ist, den Schadcode aus dem Netzwerkverkehr zu extrahieren).
- Konnektivität zu einem bestehenden GravityZone Control Center, die für das übergeordnete Management der Sandbox-Umgebung verwendet wird.
- Internetverbindung zum Download der Virtual Appliance des Sandbox Analyzer, Mindestbandbreite 5 MBps.

> **Wichtig**
> Stellen Sie sicher, dass keine Anwendungen oder Prozesse laufen, die die Internetverbindung stören könnten, während Sandbox Analyzer heruntergeladen und installiert wird.

4.5.1. ESXi Hypervisor

Die Sandbox Analyzer Virtual Appliance ist im OVA-Format verfügbar und kann auf einem einzelnen physischen Host bereitgestellt werden, auf dem VMware ESXi Hypervisor (Version 6.5 oder 6.7) ausgeführt wird.

Hardwareanforderungen für den physischen Host

- CPU: Die Gesamtzahl der CPU-Kerne (unter Berücksichtigung von Hyperthreading) kann mit Hilfe der im Abschnitt „Anforderungen an den physischen Host und Hardwareskalierung“ (S. 47) beschriebenen Berechnung abgeleitet werden.
- RAM: Die Gesamtmenge an RAM, die für den physikalischen Host benötigt wird, kann mit Hilfe der im Abschnitt „Anforderungen an den physischen Host und Hardwareskalierung“ (S. 47) beschriebenen Berechnung abgeleitet werden.

- Festplattenspeicher: Mindestens 1 TB SSD-Speicher (ausreichend für eine 8-VM-Detonationsumgebung, skalierbar mit mindestens 50 GB für jede zusätzliche Detonations-VM).
- Netzwerk: Eine dedizierte physische Netzwerkschnittstellenkarte (NIC).

  Diese NIC kann mit den folgenden Zuordnungen in zwei virtuelle NICs aufgeteilt werden:

  – Eine NIC für die Verwaltungsschnittstelle.

  – Eine NIC für das Detonationsnetzwerk.

  Beachten Sie
  Es wird empfohlen, dedizierte physische NICs mit denselben Mappings wie die oben genannten vNICs zu verwenden, wenn die Hardwarekonfiguration dies zulässt.

Software-Anforderungen

Unterstützte Versionen des ESXi-Servers: 6.5 oder höher, VMFS Version 5.

Zusätzliche Konfiguration auf dem ESXi-Host:

- SSH beim Start aktiviert.
- NTP-Dienst konfiguriert und aktiv.
- Die Option **Start/Stopp mit Host** ist aktiviert.

Beachten Sie
Sandbox Analyzer ist mit der Testversion von VMWare ESXi kompatibel. Für Produktivumgebungen wird jedoch empfohlen, eine lizenzierte Version von ESXi zu nutzen.

4.5.2. Virtuelle Sandbox Analyzer-Appliance

Die virtuelle Sandbox Analyzer-Appliance lässt sich nahezu unbegrenzt skalieren, solange die zugrunde liegenden Hardware-Ressourcen verfügbar sind.

Von den insgesamt verfügbaren ESXi-Ressourcen teilt Sandbox Analyzer CPU und RAM auf den Sandbox Manager und die virtuellen Maschinen auf.

Mindestsystemanforderungen für Sandbox Manager

- 6 vCPUs

- 20 GB RAM
- 600 GB Speicherplatz

Der Sandbox Manager verfügt über drei interne virtuelle NICs, die wie folgt zugeordnet sind:

- Eine NIC für die Kommunikation mit der Managementkonsole (GravityZone Control Center).
- Eine NIC für die Internetverbindung.
- Eine NIC für die Kommunikation mit den Detonations-VMs.

Beachten Sie
Um eine Kommunikation zu ermöglichen, müssen sich sowohl die ESXi-Management-NIC als auch die Sandbox Manager-Management-vNIC im selben Netzwerk befinden.

Virtuelle Maschinen für die Detonation

Systemanforderungen

- 4 vCPUs (im Verhältnis 4:1 überdimensioniert, mehr dazu unter „Anforderungen an den physischen Host und Hardwareskalierung“ (S. 47))
- 3 GB RAM
- 50 GB Speicherplatz

Sandbox Analyzer On-Premises unterstützt benutzerdefinierte virtuelle Maschinen-Images. Dies ermöglicht die Detonation von Stichproben in einer Laufzeitumgebung, die eine realistische Produktivumgebung nachahmt.

Für die Erstellung eines virtuellen Maschinen-Images müssen die folgenden Voraussetzungen erfüllt sein:

- Das Image der virtuellen Maschine liegt im VMDK-Format, Version 5.0, vor.
- Unterstützte Betriebssysteme für die Erstellung von virtuellen Maschinen zur Detonation:
  - Windows 7 64-Bit (beliebiger Patchstand)
  - Windows 10 64-Bit (beliebiger Patchstand)

Wichtig

- Das Betriebssystem muss auf der zweiten Partition in der Partitionstabelle installiert und auf Laufwerk C: (Standardinstallationskonfiguration von Windows) gemountet werden.
- Das lokale "Administrator"-Konto muss aktiviert sein und eine leere Passwortzeichenfolge haben (Passwort deaktivieren).
- Bevor Sie das VM-Image exportieren, müssen Sie das Betriebssystem und sämtliche installierte Software im Image der virtuellen Maschine ordnungsgemäß lizenzieren.

Software für das virtuelle Maschinen-Image

Sandbox Analyzer ist in der Lage, eine Vielzahl von Dateiformaten und -typen zu detonieren. Weitere Einzelheiten dazu finden Sie unter „Sandbox Analyzer-Objekte“ (S. 241).

Stellen Sie zum Erhalt von aussagekräftigen Berichten sicher, dass im benutzerdefinierten Image Software installiert ist, die den zur Detonation vorgesehenen Dateityp öffnen kann. Weitere Einzelheiten dazu finden Sie unter „Empfohlene Anwendungen für die Detonations-VMs“ (S. 242).

4.5.3. Network Security Virtual Appliance

Die Network Security Virtual Appliance steuert den Netzwerksensor, der Schadroutinen aus Netzwerkdatenströmen extrahiert und an Sandbox Analyzer übermittelt. Es müssen die folgenden Mindestanforderungen erfüllt werden:

- 4 vCPUs
- 4 GB RAM
- 1 TB Speicherplatz
- 2 vNICs

4.5.4. Anforderungen an den physischen Host und Hardwareskalierung

Der Skalierungsalgorithmus der Sandbox Analyzer-Umgebung verwendet die folgende Formel, wobei "K" gleich der Anzahl der Detonationsplätze (bzw. Detonations-VMs) ist:

- Sandbox Analyzer VA vCPU = 6 vCPUs + K x 1 vCPU

- Sandbox Analyzer VA RAM = 20 GB RAM + K x 2GB

Analog dazu lautet der Skalierungsalgorithmus für den Host wie folgt:

- ESXi Host vCPU = 6 vCPUs + K x 2 vCPUs
- ESXi Host RAM = 20 GB RAM + K x 5 GB

Der Hauptunterschied zwischen Sandbox Analyzer VA- und ESXi-Ressourcen besteht in den Ressourcen, die jeder Detonations-VM zugewiesen sind.

Demzufolge gelten für eine typische Detonationsumgebung (8 VMs) die folgenden Anforderungen:

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

> **Beachten Sie**
> Jede Detonations-VM benötigt 1 vCPU für die Sandbox Analyzer VA und 1 vCPU für die Detonations-VM. Die Detonations-VM wird mit 4 vCPUs bereitgestellt, diese werden jedoch im Verhältnis 4:1 überdimensioniert, so dass nur 1 vCPU für den ESXi-Host benötigt wird.

- ESXi Host RAM = 20 GB RAM + 8 x 5 GB = 60 GB RAM

> **Beachten Sie**
> RAM wird in einem Verhältnis von 1:1 zwischen der Sandbox Analyzer VA, Detonations-VMs und dem ESXi-Host verwendet. Demzufolge benötigt jede Detonations-VM 5 GB RAM vom ESXi-Host, von denen 2 GB der Sandbox Analyzer VA und 3 GB der Detonations-VM selbst zugewiesen werden.

Der daraus resultierende physische Host erfordert im zuvor beschriebenen Szenario mindestens 22 CPU-Kerne (einschließlich Hyperthreading) und mindestens 60 GB RAM, wobei weitere 10-20 % des RAM für den Hypervisor selbst reserviert sind.

In der Regel dauern die Detonation einer Stichprobe und die Erstellung des entsprechenden Detonationsberichts neun Minuten und es werden alle bereitgestellten Ressourcen verwendet. Es wird empfohlen, Ihre Sandboxing-Umgebung ausgehend von der Detonationskapazität (Dateien/Stunde) zu planen und diese Kennzahl dann in benötigte Ressourcen auf Host- und VM-Ebene zu übersetzen.

4.5.5. Sandbox Analyzer-Kommunikationsanforderungen

Die Komponenten von Sandbox Analyzer On-Premises verwenden bestimmte Kommunikationsports, die an bestimmte Netzwerkschnittstellen gebunden sind, um untereinander und/oder mit den öffentlichen Servern von Bitdefender zu kommunizieren.

Die Sandboxing-Umgebung erfordert drei Netzwerkschnittstellen:

- **eth0 - Schnittstelle Verwaltungsnetzwerk**. Stellt eine Verbindung zu GravityZone und zum ESXi-Host her.

  Es wird empfohlen, eth0 mit demselben Netzwerk wie die ESXi-Verwaltungsschnittstelle zu verbinden. Es wird auch empfohlen, sie einem dedizierten physischen Adapter zuzuordnen.

  In der folgenden Tabelle finden Sie die Anforderungen an die Netzwerkkommunikation für eth0:

Richtung	Kommunikations-Ports (auf TCP)	Quelle/Ziel
Ausgehend	8443	GravityZone-Kommunikationsserver
	443	GravityZone-Virtual-Appliance
	80	GravityZone-Virtual-Appliance
	22	ESXi-Host
	443	ESXi-Host-API
Eingehend	8443	Alle

- **eth1 - Detonationsnetzwerk**. Keine Konfiguration erforderlich. Der Installationsvorgang erzeugt die erforderlichen virtuellen Ressourcen.
- **eth2 – Internetzugangsnetzwerk**. Es wird eine uneingeschränkte und ungefilterte Verbindung zum Internet empfohlen.

  Es wird empfohlen, das Verwaltungsnetzwerk und das Internetzugangsnetzwerk verschiedenen Subnetzen zuzuordnen.

Die GravityZone Virtual Appliance erfordert den Zugriff auf die Sandbox Analyzer Virtual Appliance auf Port 443 (auf TCP), um Sandbox Analyzer-Berichte anzuzeigen und herunterzuladen.

Die GravityZone Virtual Appliance erfordert eine Verbindung zur Sandbox Analyzer Virtual Appliance auf Port 443 (auf TCP), um den Status der detonierten Stichproben abzufragen.

4.6. HVI

HVI arbeitet mit zwei Komponenten: Security Server und HVI Ergänzungspaket. Diese Produkte müssen auf den Hosts in der virtualisierten Umgebung installiert sein, in der Sie zu schützende virtuelle Maschinen nutzen.

Vor der Installation von HVI auf Hosts sollten die folgenden Anforderungen erfüllt sein:

Unterstützte Virtualisierungsplattformen

- Ab Citrix XenServer 7.1 Enterprise Edition, mit den neuesten Patches

  Wichtig
  Auf abgekündigten XenServer-Versionen ab Version 7.1 wird HVI durch Bitdefender zwei Monate über den EOL-Zeitpunkt hinaus unterstützt. Nach Ablauf dieser Frist empfehlen wir ein Update auf eine von Citrix unterstützte XenServer-Version. Weitere Informationen finden Sie in der Citrix Legacy Products Matrix und in der Citrix Product Matrix.

- Ab Citrix Hypervisor 8.0 Enterprise Edition, mit den neuesten Patches

  Warnung
  Für Citrix Hypervisor 8.0 müssen Sie den Patch XS80E004 installieren.

Unterstützte virtuelle Gast-Maschinen

Virtuelle Maschinen, die durch HVI geschützt werden sollen, müssen die folgenden Anforderungen erfüllen:

1. Die Maschinen befinden sich im HVM-Virtualisierungsmodus, was bedeutet, dass sie vollständig virtuell sind.
2. Auf den Maschinen läuft ein unterstütztes Betriebssystem:
   - **Windows Desktop-Betriebssysteme (32-Bit und 64-Bit)**

     Windows 10 May 2020 Update (20H1)

Windows 10 November 2019 Update (19H2)
Windows 10 May 2019 Update (19H1)
Windows-10-Update vom . October 2018 (Redstone 5)
Windows-10-Update vom . April 2018 (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
Windows 8
Windows 7

- **Windows Server-Betriebssysteme (64-Bit)**
  Windows Server 2019
  Windows Server 2016
  Windows Server 2012/ Windows Server 2012 R2
  Windows Server 2008 R2
- **Linux-Betriebssysteme (64-Bit)**

Distribution	Version	Kernel-Version
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	Ab 3.13.139
CentOS	8.2	4.18

Distribution	Version	Kernel-Version
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	Vor 7.5	4.1 (UEK/RHCK)
Oracle Linux	Ab 7.5	4.14 (UEK/RHCK)

Hardware-Anforderungen für GravityZone VA

- **Benötigte vCPU**

  In der folgenden Tabelle finden Sie die Anzahl der vCPUs, die jede Rolle der virtuellen Appliance anfragt.

  Jede vCPU muss mindestens 2 GHz haben.

Komponente	Anzahl der Endpunkte (bis zu)							
	250	500	1000	3000	5000	10000	25000	50000
Update-Server*	8	4	4	4	4	4	6	8
Web-Konsole**		6	8	8	10	10	12	12
Kommunikationsserver		6	8	8	10	10	16	20
Datenbank***		6	6	6	6	6	9	12
Gesamt	**8**	**22**	**26**	**26**	**30**	**30**	**43**	**52**

* Empfohlen, wenn keine Relais eingesetzt werden.
** Fügen Sie für jede aktive Integration eine vCPU auf der virtuellen Appliance mit der Rolle Web-Konsole hinzu.
*** Bei verteilter Installation von Rollen zusammen mit Replica Set: Fügen Sie für jede weitere Datenbankinstanz die angegebene Anzahl zur Gesamtanzahl hinzu.

- **Benötigter Arbeitsspeicher (GB)**

Komponente	Anzahl der Endpunkte (bis zu)							
	250	500	1000	3000	5000	10000	25000	50000
Update-Server	16	2	2	2	2	2	3	3
Web-Konsole*		8	10	10	10	10	12	16
Kommunikationsserver		8	10	10	12	12	16	20
Datenbank**		8	8	8	8	12	12	12
Gesamt	**16**	**26**	**30**	**30**	**32**	**36**	**43**	**51**

* Fügen Sie für jede aktive Integration 1 GB RAM auf der virtuellen Appliance mit der Rolle Web-Konsole hinzu.
** Bei verteilter Installation von Rollen zusammen mit Replica Set: Fügen Sie für jede weitere Datenbankinstanz die angegebene Anzahl zur Gesamtanzahl hinzu.

- **Erforderlicher Speicherplatz (GB)**

Update-Server	120	160	80	80	80	80	80	80	80
Web-Konsole			80	80	80	80	80	80	80
Kommunikationsserver			80	80	80	80	80	80	80
Datenbank**			80	80	100	100	160	300	700
Gesamt	**120**	**160**	**320**	**320**	**340**	**340**	**400**	**540**	**940**

* Zusätzlicher SSD-Speicherplatzbedarf bei Auswahl der automatischen Installation, da hierbei auch der Security Server installiert wird. Nach Abschluss der Installation können Sie den Security Server wieder deinstallieren, um wieder mehr freien Speicherplatz zu schaffen.

** Bei verteilter Installation von Rollen zusammen mit Replica Set: Fügen Sie für jede weitere Datenbankinstanz die angegebene Anzahl zur Gesamtanzahl hinzu.

Hardware-Anforderungen für Hosts

- **CPU-Micro-Architektur:**
  - Jeder Intel® Sandy Bridge-Prozessor oder neuere Versionen, die Intel® Virtualization-Technologie unterstützen.
  - VT-x oder VT-d-Endungen müssen in BIOS aktiviert sein.
- **Freier HDD-Speicherplatz:** Außer dem Speicherplatz, den Security Server erfordert, benötigt HVI für das Ergänzungspaket weitere 9 MB auf jedem Host.

Security Server-Anforderungen

Speicher- und CPU-Zuteilung für Security Server hängt von der Anzahl und Art der VMs ab, die auf dem Host laufen. In der folgenden Tabelle sind die empfohlenen Ressourcen aufgeführt:

Anzahl geschützter VMs	RAM	CPUs
1-50 VMs	6 GB	4 CPUs
51-100 VMs	8 GB	6 CPUs
101-200 VMs	16 GB	8 CPUs

Freier HDD-Speicherplatz: Sie müssen für den Security Server auf jedem Host 8 GB-Festplatten-Speicherplatz bereitstellen.

Skalieren Sie die Security Server-Ressourcen auf Grundlage Ihrer Konfiguration wie im Folgenden beschrieben, um eine optimale Performance in einer XenAPP-Umgebung sicherzustellen:

Anzahl der XenApp-VDAs	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

Anzahl der XenApp-VDAs	VDA		Security Server	
	CPUs	RAM (GB)	CPUs	RAM (GB)
8 VDA	4	12	4	16

Anforderungen für virtuelle Gast-Maschinen

In der üblichen Umgebung wird für optimale Leistung und eine optimale VM-Konsolidierungsquote für virtuelle Gast-Maschinen die folgenden Mindestanforderungen empfohlen:

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

4.7. Full Disk Encryption

GravityZone Full Disk Encryption ermöglicht es Ihnen, BitLocker auf Windows-Endpunkten und FileVault sowie das Befehlszeilenprogramm diskutil auf MacOS-Endpunkten über das Control Center zu betreiben.

Dieses Modul bietet durch vollständige Verschlüsselung fester bootfähiger und nicht-bootfähiger Laufwerke höchste Datensicherheit; außerdem speichert es Wiederherstellungsschlüssel für den Fall, dass ein Benutzer das Passwort vergisst.

Das Verschlüsselungsmodul nutzt die vorhandenen Hardware-Ressourcen in Ihrer GravityZone-Umgebung.

Softwareseitig sind die Anforderungen fast identisch mit denen für BitLocker, FileVault und dem Befehlszeilenprogramm diskutil, und die meisten Einschränkungen beziehen sich auf diese Tools.

Unter Windows

GravityZone-Verschlüsselung unterstützt BitLocker ab Version 1.2 auf Computern mit und ohne Trusted Platform Module (TPM)-Chip.

GravityZone unterstützt BitLocker auf Endpunkten mit den folgenden Betriebssystemen:

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

*BitLocker ist in diesen Betriebssystemen nicht enthalten und muss separat installiert werden. Weitere Informationen zur Installation von BitLocker unter Windows Server finden Sie in den folgenden KB-Artikeln von 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

Wichtig
GravityZone unterstützt Verschlüsselung nicht unter Windows 7 und Windows 2008 R2 ohne TPM.

Details zu den Anforderungen für BitLocker finden Sie in folgendem KB-Artikel von Microsoft: https://technet.microsoft.com/en-us/library/cc766200(v=ws.10).aspx

Unter macOS

GravityZone unterstützt FileVault und diskutil auf macOS-Endpunkten mit den folgenden Betriebssystemen:

- 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. Speicherschutz

Unterstützte Speicher- und Filesharing-Lösungen:

- ICAP-kompatible Network Attached Storage (NAS)- und Storage Area Network (SAN)-Systeme von Dell®, EMC®, IBM®, Hitachi®, HPE®, Oracle® und anderen Herstellern
- Nutanix® Files 3.x bis 3.6.2
- Citrix® ShareFile

4.9. Schutz für unterwegs

4.9.1. Unterstützte Plattformen

Security for Mobile unterstützt die folgenden Mobilgeräte und Betriebssysteme:

- Apple iPhones und iPads (iOS 8.1+)
- Smartphones und Tablets mit Google Android (4.2+)

4.9.2. Verbindunugngsanforderungen

Mobile Geräte müssen eine aktive und funktionierende Funk-Daten- oder WLAN-Verbindung mit dem Kommunikationsserver haben.

4.9.3. Push-Benachrichtigungen

Security for Mobile verwendet Push-Benachrichtigungen, um Mobile Clients darauf hinzuweisen, dass Richtlinien-Updates oder Aufgaben bereit stehen. Push-Benachrichtigungen werden vom Kommunikationsserver über den Dienst gesendet, der vom Hersteller des Betriebssystems dafür vorgesehen ist:

- Firebase Cloud Messaging (FCM) für Android-Geräte. Damit FCM funktioniert, müssen die folgenden Punkte gegeben sein:
  - Google Play Store muss installiert sein.
  - Android 4.2 oder neuer

  - Um Push-Benachrichtigungen zu senden, müssen eine bestimmte Anzahl an Ports offen sein.
- Apple Push Notifications (APNs) bei iOS-Geräten. Weitere Informationen finden Sie in diesem Artikel der Wissensdatenbank.

Im Bereich **Konfiguration > Verschiedenes** können Sie unter **Handy-Push-Benachrichtigungs-Check** überprüfen, ob die Push-Benachrichtigungen ordnungsgemäß funktionieren.

Mehr über die Verwaltung von mobilen Gräten mit GravityZone erfahren Sie in diesem Artikel.

4.9.4. Zertifikate für die iOS-Geräteverwaltung

Um die Infrastruktur zur Verwaltung von iOS-Mobilgeräten einzurichten, benötigen Sie bestimmte Zertifikate.

Weitere Informationen finden Sie unter „Zertifikate“ (S. 104).

4.10. Report-Builder

Die Report-Builder-Rollen müssen auf separaten Instanzen der GravityZone-Virtual-Appliance laufen: auf der einen virtuellen Appliance muss die Report-Builder-Datenbankrolle installiert sein, auf der anderen die Report-Builder-Prozessorenrolle.

4.10.1. Hardware

Für die Report-Builder-Rollen sind folgende Hardwareressourcen nötig:

Erforderliche CPU

Virtuelle Appliance	Anzahl der Endpunkte (bis zu)					
	250	1000	5000	10000	25000	50000
Datenbank	4	4	4	4	6	8
Prozessoren	6	6	6	6	6	6

RAM (GB)

Virtuelle Appliance	Anzahl der Endpunkte					
	250	1000	5000	10000	25000	50000
Datenbank	8	8	8	8	16	16
Prozessoren	8	8	8	8	8	8

Freier Speicherplatz (GB)

Virtuelle Appliance	Anzahl der Endpunkte					
	250	1000	5000	10000	25000	50000
Databank*	15	20	50	90	210	400
Verarbeitung**	50	200	1000	1950	4800	9500

* Die Festplattennutzung durch die virtuelle Appliance mit der Report-Builder-Datenbank wird für Ereignisse der letzten 12 Monate angegeben.
** Die Festplattennutzung durch die virtuelle Appliance mit der Report-Builder-Prozessorenrolle wird für durchschnittlich 10 Berichte pro Monat mit jeweils 15 Spalten angegeben. Die virtuelle Appliance mit der Report-Builder-Prozessorenrolle benötigt mehr Speicherplatz, da in ihr sämtliche Berichte auf der Grundlage der Daten aus der Report-Builder-Datenbank gespeichert sind.

4.10.2. GravityZone-Produktversionen

Ab GravityZone Version 6.5.5-1 werden die Report-Builder-Rollen mit der GravityZone Virtual Appliance ausgeliefert.

Bei älteren Versionen wurden die Report-Builder-Rollen als separate virtuelle Appliances ausgeliefert, die mit Bitdefender GravityZone ab Version 6.1.27-537 kompatibel waren.

4.11. GravityZone-Kommunikations-Ports

GravityZone ist eine dezentrale Lösung. Das bedeutet, dass die einzelnen Komponenten der Lösung über das lokale Netzwerk oder das Internet miteinander

kommunizieren. Jede Komponente verwendet bestimmte Ports zur Kommunikation mit den anderen Komponenten. Diese Ports müssen für GravityZone offen sein.

Näheres zu GravityZone-Ports erfahren Sie in diesem Artikel.

5. SCHUTZ INSTALLIEREN

GravityZone ist eine Client-Server-Lösung. Um Ihr Netzwerk mit Bitdefender zu schützen, müssen Sie die GravityZone-Serverrollen bereitstellen, Ihre Lizenz registrieren, Installationspakete konfigurieren und sie über Sicherheitsagenten auf den Endpunkten bereitstellen. Einige Sicherheitsebenen erfordern die Installation und Konfiguration weiterer Komponenten.

5.1. GravityZone: Installation und Einrichtung

Führen Sie die folgenden Schritte aus, um die Installation möglichst reibungslos zu gestalten:

1. Installation vorbereiten
2. Bereitstellung und Einrichtung von GravityZone
3. Verbindung zum Control Center herstellen und erstes Benutzerkonto einrichten
4. Control Center-Einstellungen konfigurieren

5.1.1. Installation vorbereiten

Zur Installation benötigen Sie ein Image der GravityZone-Virtual-Appliance. Nachdem Sie die GravityZone-Appliance installiert und eingerichtet haben, können Sie per Fernzugriff den Client installieren bzw. die nötigen Installationspakete für anderen Komponenten der Sicherheitsdienste über die Web-Oberfläche der Control Center herunterladen.

Das Image der GravityZone-Appliance steht in verschiedenen Formaten zur Verfügung, die mit den gängigsten Virtualisierungsplattformen kompatibel sind. Die Links zum Herunterladen erhalten Sie, wenn Sie sich auf der Bitdefender-Website für eine Testversion registrieren.

Für die Installation und Ersteinrichtungen sollten Sie die folgenden Dinge zur Hand haben:

- DNS-Namen oder festgelegte IP-Adressen (entweder durch statische Konfiguration oder über DHCP-Reservierung) für die GravityZone-Appliances
- Benutzername und Passwort eines Domain-Administrators
- Eckdaten für vCenter Server, vShield Manager, XenServer (Hostname oder IP-Adresse, Kommunikations-Port, Administrator-Benutzername und -Passwort)

- Lizenzschlüssel (siehe E-Mail zur Testversions-Registrierung oder zum Kauf)
- Server-Einstellungen für ausgehende E-Mails
- wenn nötig, Proxy-Server-Einstellungen
- Sicherheitszertifikate

5.1.2. GravityZone bereitstellen

Eine GravityZone-Bereitstellung besteht aus einer oder mehreren Appliances, die die Serverrollen ausführen. Die Anzahl der Appliances hängt von verschiedenen Faktoren ab, wie z. B.: Größe und Aufbau Ihrer Netzwerkinfrastruktur oder den von Ihnen genutzten GravityZone-Funktionen. Es gibt drei Arten von Serverrollen: Basis, Zusätzlich und Optional.

Wichtig
Zusätzliche und optionale Rollen sind nur für bestimmte GravityZone-Lösungen verfügbar.

GravityZone-Rolle	Rollentyp	Installieren
Datenbank-Server Update Server Web-Konsole Kommunikationsserver	Basis (erforderlich)	Mindestens eine Instanz jeder Rolle. Eine GravityZone-Appliance kann eine, mehrere oder alle dieser Rollen ausführen.
Report-Builder-Datenbank Berichterstellungs-Verarbeitungsmodule	Zusätzlich	Eine Appliance für jede Rolle
Security Server	Freiwillig	Empfohlen nur in kleinen Netzwerken oder bei eingeschränkten Ressourcen. Andernfalls können Sie einen eigenständigen Security Server über das Control Center bereitstellen, nachdem die

GravityZone-Rolle	Rollentyp	Installieren
		GravityZone-Bereitstellung abgeschlossen ist.

Je nachdem, wie Sie die GravityZone-Rollen verteilen, müssen eine oder mehrere GravityZone-Appliances bereitstellen (mindestens drei Appliances bei Verwendung des Report-Builders). Der Datenbank-Server wird als erstes installiert.

In einem Szenario mit mehreren GravityZone-Appliances installieren Sie zunächst die Datenbank-Server-Rolle auf der ersten Appliance und konfigurieren dann alle weiteren Appliances so, dass sie eine Verbindung mit der bestehenden Datenbankinstanz herstellen.

Sie können weitere Instanzen von Datenbank-Server-, Web-Konsole- und Kommunikationsserver-Rollen bereitstellen. In diesem Fall verwenden Sie ein Replica Set für den Datenbank-Server und Lastenverteilung für Web-Konsole und Kommunikationsserver auf den GravityZone-Appliances.

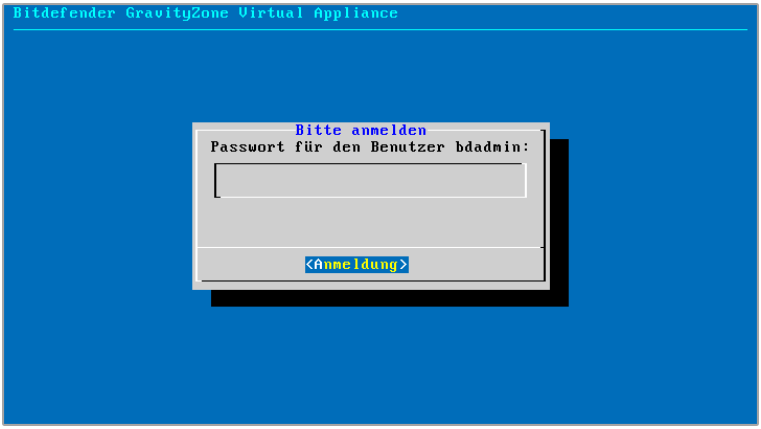
Es wird empfohlen, die Report-Builder-Rollen zu installieren, nachdem Sie GravityZone eingerichtet haben, d.h. erst nach Installation der GravityZone-Basis-Rollen, Konfiguration des Control Centers, Update von GravityZone und Bereitstellung des Schutzes auf den Endpunkten. Sie müssen zudem erst die Report-Builder-Datenbank und danach die Report-Builder-Prozessoren installieren. Weitere Einzelheiten dazu finden Sie unter „Installieren von Report-Builder“ (S. 188).

So erfolgt die Bereitstellung und Einrichtung von GravityZone:

1. Laden Sie das Image der virtuellen GravityZone-Appliance von der Bitdefender-Website herunter (Sie erhalten den Link in der E-Mail zur Registrierung oder zum Kauf).
2. Importieren Sie das Image der GravityZone-Appliance in Ihre virtualisierte Umgebung.
3. Schalten Sie die Appliance an.
4. Greifen Sie von ihrem Virtualisierungsverwaltungsprogramm auf die Konsolenoberfläche der GravityZone-Appliance zu.
5. Konfigurieren Sie das Passwort für `bdadmin`, den integrierten Systemadministrator.

Konsolenoberfläche der Appliance: neues Passwort eingeben

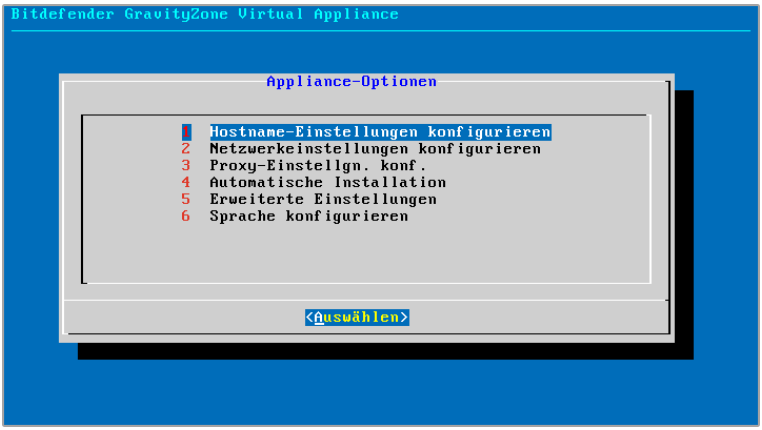
6. Melden Sie sich mit dem Passwort an, das Sie gerade eingerichtet haben.



Konsolenoberfläche der Appliance: Login

Die Konfigurationsoberfläche der Appliance wird geöffnet.

Mithilfe der Pfeiltasten und der `Tabulator`-Taste können Sie durch die Menüs und Optionen navigieren. Drücken Sie die `Eingabetaste`, um eine bestimmte Option auszuwählen.



Konsolenoberfläche der Appliance: Hauptmenü

7. Wenn Sie die Sprache der Benutzeroberfläche ändern möchten, wählen Sie die Option **Sprache konfigurieren**. Weitere Einzelheiten zur Konfiguration finden Sie unter „Sprache konfigurieren“ (S. 72).
8. Konfigurieren Sie den Appliance-Hostname.
9. Konfigurieren Sie die Netzwerkeinstellungen.
10. Konfigurieren Sie die Proxy-Einstellungen. (falls erforderlich)
11. Installieren Sie die GravityZone-Server-Rollen. Sie haben zwei Optionen:
    - Automatische Installation. Wählen Sie diese Option, wenn Sie nur eine GravityZone-Appliance in Ihrem Netzwerk bereitstellen möchten.
    - Erweiterte Einstellungen. Wählen Sie diese Option, wenn Sie GravityZone manuell oder in einer verteilten Architektur bereitstellen möchten.

Nach der Installation und Einrichtung der GravityZone-Appliance können Sie die Einstellungen der Appliance jederzeit über die Konfigurationsoberfläche bearbeiten. Weitere Informationen zur Einrichtung der GravityZone-Appliance erhalten Sie unter „Die GravityZone-Appliance verwalten“ (S. 111).

Hostname-Einstellungen konfigurieren

Die Kommunikation mit den GravityZone-Rollen funktioniert über die IP-Adresse oder den DNS-Namen derjenigen Appliance, auf denen die jeweilige Rolle installiert

ist. Standardmäßig kommunizieren die GravityZone-Komponenten über IP-Adressen. Wenn Sie die Kommunikation über DNS-Namen ermöglichen möchten, müssen Sie den GravityZone-Appliances DNS-Namen zuweisen und sicherstellen, dass diese Namen korrekt zu den konfigurierten IP-Adressen der Appliances aufgelöst werden.

Vorbereitende Maßnahmen:

- Konfigurieren Sie den DNS-Eintrag im DNS-Server.
- Der DNS-Name muss korrekt zur konfigurierten IP-Adresse der Appliance aufgelöst werden. Daher müssen Sie dafür sorgen, dass die Appliance die richtige IP-Adresse hat.

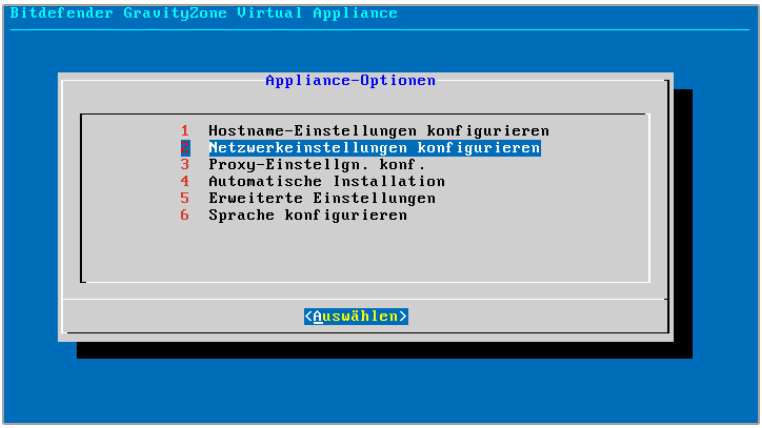
So konfigurieren Sie die Einstellungen für den Hostnamen:

1. Wählen Sie aus dem Hauptmenü **Hostname-Einstellungen konfigurieren**.
2. Geben Sie den Hostnamen der Appliance und (falls nötig) den Namen der Active-Directory-Domäne ein.
3. Wählen Sie **OK**, um die Änderungen zu speichern.

Netzwerkeinstellungen konfigurieren

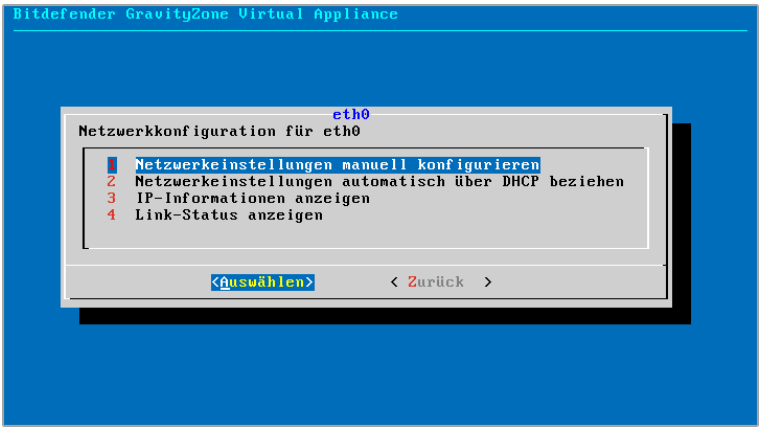
Sie können die Appliance so einrichten, dass sie die Netzwerkeinstellungen automatisch vom DHCP-Server bezieht, oder Sie können sie manuell konfigurieren. Wenn Sie die DHCP-Methode wählen, müssen Sie den DHCP-Server so konfigurieren, dass er eine bestimmte IP-Adresse für die Appliance reserviert.

1. Wählen Sie aus dem Hauptmenü **Netzwerkeinstellungen konfigurieren**.



Konsolenoberfläche der Appliance: Netzwerk Einstellungoptionen

2. Wählen Sie den Netzwerkadapter aus.
3. Wählen Sie die Konfigurationsmethode:
   - **Netzwerkeinstellungen manuell konfigurieren.** Sie müssen die IP-Adresse, die Netzwerkmaske, die Gateway-Adresse und die DNS-Server-Adressen angeben.
   - **Netzwerkeinstellungen automatisch über DHCP beziehen.** Wählen Sie diese Option nur, wenn Sie den DHCP-Server so konfiguriert haben, dass er eine bestimmte IP-Adresse für die Appliance reserviert.



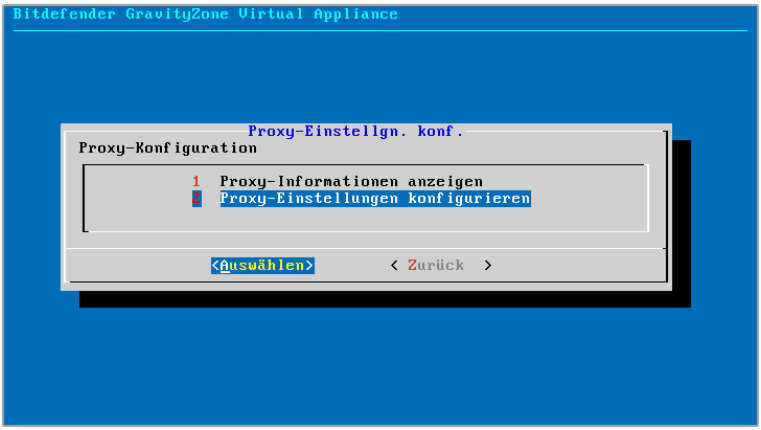
Konsolenoberfläche der Appliance: Netzwerkkonfiguration

4. Über die entsprechenden Optionen können Sie die aktuellen Details zur IP-Konfiguration bzw. den Link-Status überprüfen.

Proxy-Einstellgn. konf.

Wenn die Appliance über einen Proxy-Server mit dem Internet verbinden möchten, müssen Sie die Proxy-Einstellungen konfigurieren.

1. Wählen Sie aus dem Hauptmenü **Proxy-Einstellungen konfigurieren**.
2. Wählen Sie **Proxy-Informationen anzeigen**, um zu prüfen, ob der Proxy aktiviert ist.
3. Klicken Sie auf **OK** um zum vorherigen Bildschirm zurückzukehren.
4. Klicken Sie erneut auf **Proxy-Einstellungen konfigurieren**.



Konsolenoberfläche der Appliance: Proxy-Einstellungen konfigurieren

5. Geben Sie die Adresse des Proxy-Servers ein. Verwenden Sie die folgende Syntax:
   - Wenn der Proxy-Server keine Authentifizierung erfordert:

     `http(s)://<IP-Adresse/Hostname>:<Port>`
   - Wenn der Proxy-Server Authentifizierung erfordert:

     `http(s)://<Benutzername>:<Passwort>@<IP-Adresse/Hostname>:<Port>`
6. Wählen Sie **OK**, um die Änderungen zu speichern.

Automatische Installation

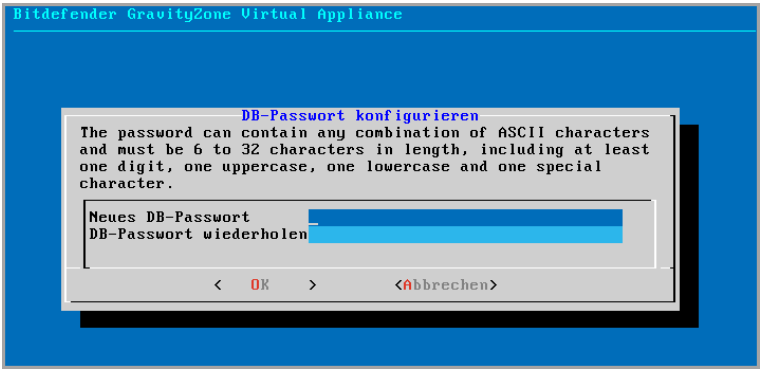
Bei einer automatischen Installation werden alle Basis-Rollen auf derselben Appliance installiert. Weitere Informationen zu einer verteilten GravityZone-Bereitstellung finden Sie unter „Erweiterte Einstellungen“ (S. 70).

Wichtig
Die automatische Bereitstellung installiert zudem den Security Server, eingebettet in die GravityZone-Appliance. Informationen zum Security Server finden Sie unter „GravityZone-Architektur“ (S. 11).
Die Option, Rollen automatisch zu installieren, ist nur bei der Ersteinrichtung von GravityZone verfügbar.

So installieren Sie die Rollen automatisch:

1. Wählen Sie im Hauptmenü den Punkt **Automatische Installation**.
2. Lesen und akzeptieren Sie die Endbenutzer-Lizenzvereinbarung, um fortzufahren.
3. Bestätigen Sie die zu installierenden Rollen.
4. Legen Sie das Passwort für den Datenbank-Server fest.

   Das Passwort kann sich aus beliebigen ASCII-Zeichen zusammensetzen,mindestens 6 und höchstens 32 Zeichen lang sein und mindestenseine Ziffer, einen Großbuchstaben, einen Kleinbuchstaben und ein Sonderzeichen enthalten.



Konsolenoberfläche der Appliance: Datenbankkennwort festlegen

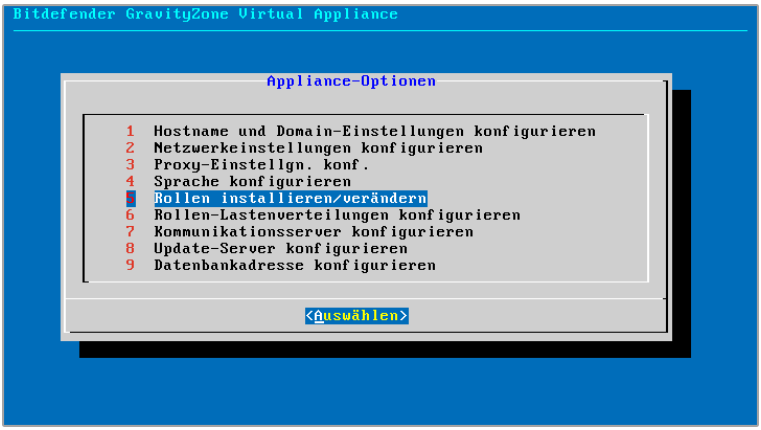
5. Warten Sie, bis der Installationsvorgang abgeschlossen ist.

Erweiterte Einstellungen

Verwenden Sie diese Option, um nur einen Teil oder alle GravityZone-Rollen einzeln zu installieren oder um Ihre GravityZone-Infrastruktur zu erweitern. Sie können die Rollen auf einer oder mehreren Appliances installieren. Diese Installationsmethode ist sowohl für das Staging von Updates als auch in verteilten GravityZone-Architekturen erforderlich, um GravityZone in großen Netzwerken zu skalieren und eine hohe Verfügbarkeit der GravityZone-Dienste zu gewährleisten.

So installieren Sie die Rollen einzeln:

1. Wählen Sie im Hauptmenü den Punkt **Erweiterte Einstellungen**.



Konsolenoberfläche der Appliance: Einstellung Rollen

2. Wählen Sie **Rollen installieren/deinstallieren**, um die Appliance in einer GravityZone-Umgebung mit nur einem Datenbankserver zu installieren.

   Beachten Sie
   Die anderen Optionen dienen der Erweiterung der GravityZone-Installation auf eine verteilte Architektur. Weitere Informationen finden Sie in den Kapiteln „Mit bestehender Datenbank verbinden“ (S. 123) und „Mit bestehender Datenbank verbinden (Secure VPN Cluster)“ (S. 124).

3. Wählen Sie **Rollen hinzufügen oder entfernen**. Eine Bestätigungsmeldung wird angezeigt.
4. Drücken Sie die `Eingabetaste`, um den Vorgang fortzusetzen.
5. Drücken Sie die `Leertaste` und dann die `Eingabetaste`, um die Datenbank-Server-Rolle zu installieren. Bestätigen Sie Ihre Auswahl, indem Sie die `Eingabetaste` erneut drücken.
6. Legen Sie das Datenbankpasswort fest.

   Das Passwort kann sich aus beliebigen ASCII-Zeichen zusammensetzen,mindestens 6 und höchstens 32 Zeichen lang sein und mindestenseine Ziffer, einen Großbuchstaben, einen Kleinbuchstaben und ein Sonderzeichen enthalten.

7. Drücken Sie die `Eingabetaste` und warten Sie, bis der Installationsvorgang beendet wurde.
8. Installieren Sie die anderen Rollen, indem Sie im Menü **Rollen installieren/deinstallieren** den Punkt **Rollen hinzufügen oder entfernen** und anschließend die zu installierenden Rollen wählen.
   a. Wählen Sie im Menü **Rollen installieren/deinstallieren** den Punkt **Rollen hinzufügen oder entfernen** aus.
   b. Lesen Sie die Endbenutzer-Lizenzvereinbarung. Drücken Sie die `Eingabetaste`, um sie zu akzeptieren und fortzufahren.

      Beachten Sie
      Dies ist nach der Installation des Datenbank-Servers nur einmal erforderlich.

   c. Wählen Sie die zu installierenden Rollen aus. Drücken Sie die `Leertaste`, um eine Rolle auszuwählen und die `Eingabetaste`, um den Vorgang fortzusetzen.
   d. Drücken Sie die `Eingabetaste` erneut, um den Vorgang zu bestätigen, und warten Sie, bis die Installation abgeschlossen ist.

Beachten Sie
Die Installation jeder Rolle dauert normalerweise ein paar Minuten. Während der Installation werden benötigte Dateien aus dem Internet heruntergeladen. Daher dauert die Installation länger, wenn die Internetverbindung langsam ist. Wenn die Installation ins Stocken gerät, installieren Sie die Appliance erneut.

Sprache konfigurieren

Zunächst erscheint die Konfigurationsoberfläche der Appliance in englischer Sprache.

Sie können die Sprache der Oberfläche wie folgt ändern:

1. Wählen Sie im Hauptmenü den Punkt **Configure Language**.
2. Wählen Sie dann eine der angezeigten Sprachen. Eine Bestätigungsmeldung wird angezeigt.

   Beachten Sie
   Um die gewünschte Sprache zu finden, müssen Sie evtl. runter scrollen.

3. Wählen Sie **OK**, um die Änderungen zu speichern.

5.1.3. Control Center: Ersteinrichtung

Nach der Installation und Einrichtung der GravityZone-Appliance müssen Sie die Web-Oberfläche des Control Center öffnen und Ihr Unternehmens-Administrator-Konto konfigurieren.

1. Geben Sie in die Adressleiste ihres Browsers IP-Adresse oder den DNS-Hostnamen der Control Center-Appliance ein (mit dem Präfix `https://`). Ein Konfigurationsassistent wird geöffnet.
2. Geben Sie die Lizenzschlüssel ein, die zur Bestätigung der erworbenen GravityZone-Sicherheitsdienste nötig sind. Sie können auch einen beliebigen anderen GravityZone-Add-on-Schlüssel eingeben, den Sie haben.

   Sie finden Ihre Lizenzschlüssel in der E-Mail zur Testversions-Registrierung oder zum Kauf.

   a. Klicken Sie auf die Schaltfläche ⊕**Hinzufügen** am oberen Ende der Tabelle. Ein Konfigurationsfenster wird sich öffnen.

   b. Wählen Sie Art der Lizenzregistrierung (online oder offline).

   c. Geben Sie im Feld **Lizenzschlüssel** den Lizenzschlüssel ein. Bei der Offline-Registrierung müssen Sie auch den Registrierungs-Code angeben.

   d. Warten Sie, bis der Lizenzschlüssel bestätigt wurde. Klicken Sie zum Abschluss auf **Hinzufügen**.

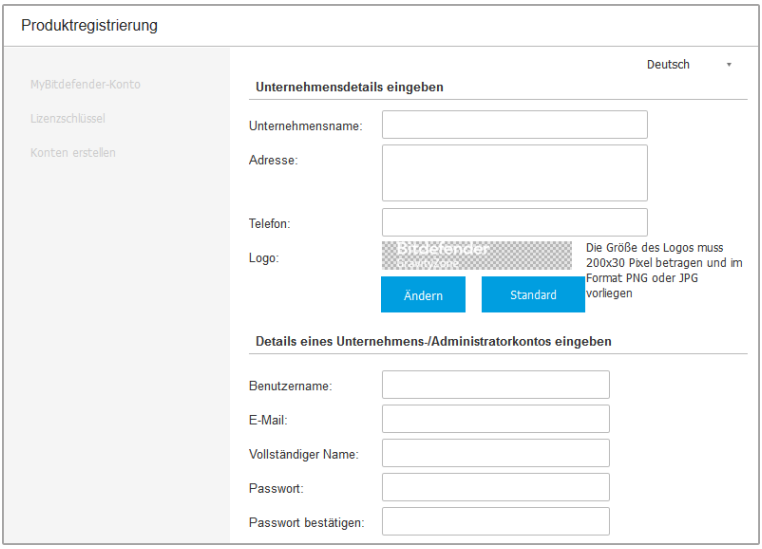
   Der Lizenzschlüssel wird in der Lizenztabelle angezeigt. In den entsprechenden Spalten sehen Sie auch den Sicherheitsdienst, den Status, das Ablaufdatum und die aktuelle Nutzung jedes Lizenzschlüssels.

Beachten Sie

- Während der Ersteinrichtung muss mindestens ein gültiger Lizenzschlüssel angegeben werden, um GravityZone zu verwenden. Später können Sie mehr Lizenz- und Add-on-Schlüssel hinzufügen oder bestehende verändern.
- Sie können die Add-ons nutzen, solange eine gültige Basislizenz besteht. Andernfalls können Sie die Funktionen nur anzeigen, aber nicht nutzen.

Ersteinrichtung - Lizenzschlüssel angeben

3. Klicken Sie auf **Weiter**.
4. Geben Sie Informationen wie den Namen, die Adresse und die Telefonnummer Ihres Unternehmens ein.
5. So können Sie das Logo, das im Control Center und in den Berichten und E-Mails Ihres Unternehmens angezeigt wird, ändern:
   - Klicken Sie auf **Ändern**, um das Logobild auf Ihrem Computer zu suchen. Das Dateiformat muss entweder PNG oder JPG sein, und das Bild muss genau 200×30 Pixel groß sein.
   - Klicken Sie auf **Standard**, um das Bild zu löschen und wieder das von Bitdefender bereitgestellte Bild zu verwenden.
6. Geben Sie die geforderten Informationen zu ihrem Unternehmens-Administrator-Konto an: Benutzername, E-Mail-Adresse und Passwort. Das Passwort muss mindestens einen Großbuchstaben, einen Kleinbuchstaben und eine Ziffer oder ein Sonderzeichen enthalten.



Ersteinrichtung - Konto konfigurieren

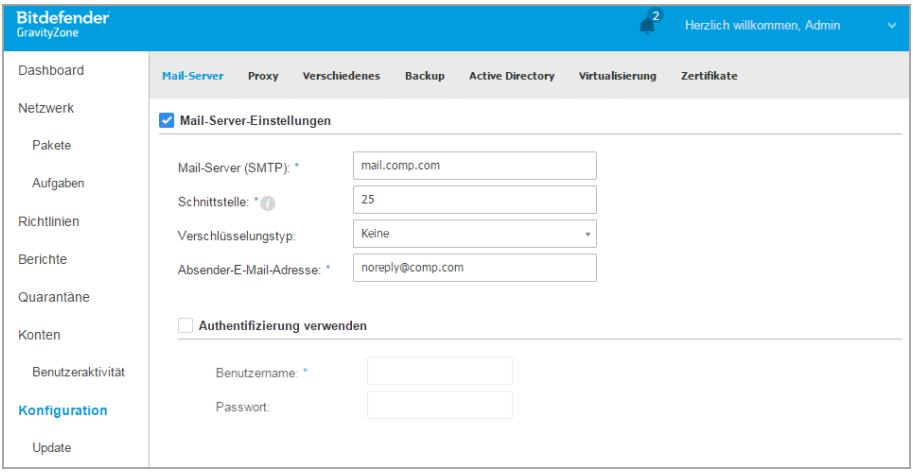
7. Klicken Sie auf **Konto erstellen**.

Das Unternehmens-Administrator-Konto wird erstellt, und Sie werden automatisch mit dem neuen Konto am Bitdefender Control Center angemeldet.

5.1.4. Control Center-Einstellungen konfig.

Nach der Ersteinrichtung müssen Sie die Einstellungen des Control Center konfigurieren. Als Unternehmensadministrator können Sie Folgendes tun:

- Mail-, Proxy- und andere allgemeine Einstellungen konfigurieren.
- Ein Control Center-Datenbank-Backup durchführen oder planen.
- Integration mit Active Directory und Virtualisierungsverwaltungstools(vCenter Server, XenServer) einrichten
- Sicherheitszertifikate installieren.



Mail-Server-Einstellungen

Mail-Server

Control Center benötigt einen externen Mail-Server, um E-Mails zu versenden.

Beachten Sie
Wir empfehlen, ein eigenes Mail-Konto für Control Center zu erstellen.

So ermöglichen sie es dem Control Center E-Mails zu versenden:

1. Gehen Sie zum Seite **Konfiguration**.
2. Wechseln Sie zum Reiter **Mail-Server**.
3. Wählen Sie **Mail-Server-Einstellungen**, und konfigurieren Sie die nötigen Einstellungen:
   - **Mail-Server (SMTP).** Geben Sie die IP-Adresse oder den Host-Namen des E-Mail-Servers ein, der die E-Mails versenden wird.
   - **Schnittstelle.** Geben Sie den Port ein, über den die Verbindung zum Mail Server hergestellt werden soll.
   - **Verschlüsselungstyp.** Wenn der Mail-Server eine verschlüsselte Verbindung erfordert, wählen Sie den passenden Typ aus dem Menü (SSL,TLS oder STRARTTLS).

- **Absender-E-Mail-Adresse.** Geben Sie die E-Mail-Adresse ein, die im Absender-Feld der E-Mail (E-Mail-Adresse des Absenders) erscheinen soll.
- **Authentifizierung verwenden.** Markieren Sie dieses Kästchen, wenn der Mail-Server eine Authentifizierung fordert. Sie müssen einen gültigen Benutzernamen/E-Mail-Adresse und ein gültiges Passwort angeben.

4. Klicken Sie auf **Speichern**.

Control Center bestätigt die Mail-Einstellungen automatisch, wenn Sie sie speichern. Wenn die angegebenen Einstellungen nicht bestätigt werden können, werden Sie durch eine Fehlermeldung auf die ungültige(n) Einstellung(en) hingewiesen. Korrigieren Sie die Einstellungen und versuchen Sie es erneut.

Proxy

Wenn Ihr Unternehmen über einen Proxy-Server mit dem Internet verbunden ist, müssen Sie die Proxy-Einstellungen konfigurieren:

1. Gehen Sie zum Seite **Konfiguration**.
2. Wechseln Sie zum Reiter **Proxy**.
3. Wählen Sie **Proxy-Einstellungen verwenden**, und konfigurieren Sie die nötigen Einstellungen:
   - **Adresse** - Geben Sie die IP-Adresse des Proxy-Servers ein.
   - **Port** - Geben Sie den Port ein, über den die Verbindung zum Proxy-Server hergestellt wird.
   - **Name** - Geben Sie einen für den Proxy-Server gültigen Benutzernamen ein.
   - **Passwort** - Geben Sie das Passwort für den zuvor angegebenen Benutzer ein.
4. Klicken Sie auf **Speichern**.

Verschiedenes

Auf der Seite **Konfiguration** können Sie im Reiter **Verschiedenes** die folgenden Grundeinstellungen konfigurieren:

- **Wenn ein Security Server-Image benötigt wird, das nicht verfügbar ist.** Standardmäßig beinhaltet die GravityZone-Appliance nicht die Images der virtuellen Maschine mit dem Security Server. Wenn ein Administrator versucht, ein Image des Security Server herunterzuladen oder eine Security

Server-Installationsaufgabe auszuführen, wird die Aktion fehlschlagen. Sie können für solche Situationen eine automatische Aktion konfigurieren, indem Sie eine der folgenden Optionen wählen:

- **Image automatisch herunterladen**
- **Den Administrator benachrichtigen und nicht herunterladen**

> **Beachten Sie**
> Um die Arbeit der Administratoren nicht zu stören, können Sie die nötigen Security Server-Pakete auf der Seite **Update** im Reiter **Produkt-Update** herunterladen. Weitere Informationen finden Sie unter „Neuste Produkt-Updates laden“ (S. 200).

- **Wenn ein nicht verfügbares Kit benötigt wird.** Sie können für solche Situationen eine automatische Aktion konfigurieren, indem Sie eine der folgenden Optionen wählen:
  - **Paket automatisch herunterladen**
  - **Den Administrator benachrichtigen und nicht herunterladen**
- **Gleichzeitige Installationen.** Über Installationsaufgaben können Administratoren aus der Ferne Sicherheitskomponenten installieren. Wählen Sie diese Option, um die Höchstzahl der Installationen festzulegen, die gleichzeitig vorgenommen werden können.

  Wenn die Höchstzahl der gleichzeitigen Installationen zum Beispiel auf 10 gesetzt wurde und eine Ferninstallationsaufgabe 100 Computern zugewiesen wird, sendet Control Center zunächst 10 Installationspakete durch das Netzwerk. In diesem Fall wird die Installation gleichzeitig auf höchstens 10 Computern durchgeführt, während alle anderen Teilaufgaben zunächst den Zustand ausstehend erhalten. Sobald eine Teilaufgabe abgeschlossen ist, wird das nächste Installationspaket gesendet, usw.
- **Zwei-Faktor-Authentifizierung für alle Konten erzwingen.** Die Zwei-Faktor-Authentifizierung (2FA) ist eine zusätzliche Sicherheitsschicht für GravityZone-Benutzerkonten, da neben den Zugangsdaten für das Control Center auch ein Authentifizierungscode abgefragt wird. Um diese Funktion nutzen zu können, muss Google Authenticator, Microsoft Authenticator oder eine beliebige andere mit dem RFC6238-Standard kompatible Anwendung zur Zwei-Faktor-Authentifizierung mit TOTP (Time-Based One-Time Password Algorithm) auf ein Mobilgerät des Benutzers heruntergeladen und installiert

werden, dann mit dem GravityZone-Benutzerkonto verknüpft werden und dann bei jeder Anmeldung am Control Center verwendet werden. Die Authenticator-App erzeugt alle 30 Sekunden einen neuen sechsstelligen Code. Um sich am Control Center anzumelden, muss der Nutzer nach der Eingabe seines Passworts zudem den sechsstelligen Authentifizierungs-Code eingeben.

Die Zwei-Faktor-Authentifizierung standardmäßig für die Anlage neuer Unternehmen aktiviert. Im Anschluss wird der Benutzer bei der Anmeldung in einem Konfigurationsfenster aufgefordert, diese Funktion zu aktivieren. Die Aktivierung der 2FA kann dabei vom Nutzer nicht mehr als dreimal übersprungen werden. Beim vierten Anmeldeversuch ist das Überspringen der 2FA-Konfiguration nicht mehr möglich und der Benutzer kann sich nicht anmelden.

Wenn Sie die 2FA-Erzwingung für alle GravityZone-Konten in Ihrem Unternehmen deaktivieren möchten, können Sie die Auswahl der Option wieder aufheben. Sie erhalten eine Bestätigungsaufforderung, bevor die Änderungen übernommen werden. So bleibt die 2FA für die Nutzer zwar weiterhin aktiviert, sie können sie aber über ihre jeweiligen Kontoeinstellungen deaktivieren.

Beachten Sie

- Den 2FA-Status für ein Benutzerkonto können Sie auf der **Konten**seite einsehen.
- Wenn ein Benutzer, bei dem die 2FA aktiviert ist, sich nicht bei GravityZone anmelden kann (wegen eines neuen Gerätes oder Verlust des geheimen Schlüssels), können Sie die Aktivierung der Zwei-Faktor-Authentifizierung im Bereich **Zwei-Faktor-Authentifizierung** über die Benutzerkontoseite zurücksetzen. Weitere Einzelheiten finden Sie in den Abschnitten **Benutzerkonten > Zwei-Faktor-Authentifizierung verwalten** im Administratorhandbuch.

- **NTP-Server-Einstellungen**. Der NTP-Server dient zur Synchronisation der Zeit zwischen allen GravityZone-Appliances. Eine Standardadresse ist voreingestellt. Im Feld **NTP-Server-Adresse** können Sie sie ändern.

Beachten Sie

Damit die GravityZone-Appliances mit dem NTP-Server kommunizieren können, muss Port 123 (UDP) offen sein.

- **Syslog aktivieren**. Wenn Sie diese Funktion aktivieren, erlauben Sie GravityZone, Benachrichtigungen an einen Protokollserver zu schicken, der das Syslog-Protokoll verwendet. Damit können Sie GravityZone-Ereignisse besser überwachen.

  Wie Sie die Liste der an den Syslog-Server gesendeten Benachrichtigungen anzeigen und konfigurieren können, erfahren Sie im Kapitel **Benachrichtigungen** des GravityZone-Administratorhandbuchs.

  So aktivieren Sie die Protokollierung auf einem entfernten Syslog-Server:

  1. Markieren Sie das Kästchen **Syslog aktivieren**.
  2. Geben Sie den Namen oder die IP-Adresse des Servers ein, das bevorzugte Protokoll und den Port, auf dem Syslog lauscht..
  3. Wählen Sie das Format, in dem die Daten an den Syslog-Server übermittelt werden sollen:
     - **JSON-Format**. JSON ist ein schlankes Datenaustauschformat, das unabhängig von der Programmiersprache einsetzbar ist. JSON stellt die Daten in einem für den Menschen lesbaren Textformat dar. Im JSON-Format sind die Details zu jedem Ereignis als Objekte gegliedert, wobei jedes Objekt aus einem Name/Wert-Paar besteht.

       Zum Beispiel:

       ```
       {
           "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"
       }
       ```

       Weitere Informationen finden Sie unter www.json.org.

       Hierbei handelt es sich um das Standardformat in GravityZone.

     - **Common Event Format (CEF)**. CEF ist ein von ArcSight entwickelter offener Standard, der das Protokollmanagement vereinfacht.

Zum Beispiel:

```
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
```

Weitere Informationen finden Sie unter ArcSight Common Event Format (CEF) Implementation Standard.

Im Kapitel **Benachrichtigungen** des Administratorhandbuchs finden Sie die verfügbaren Benachrichtigungsarten für jedes Format.

4. Klicken Sie in der Spalte **Aktion** auf die Schaltfläche ⊕ **Hinzufügen**.

Klicken Sie **Speichern**, um die Änderungen zu speichern.

Backup

Um sicherzugehen, dass all ihre Daten im Control Center gesichert sind, sollten Sie die GravityZone-Datenbank sichern. Sie können beliebig viele Datenbank-Backups durchführen oder regelmäßige Backups zu bestimmten Zeitpunkten planen.

Mit jedem Datenbank-Backup-Befehl wird eine `tgz`-Datei (gzip-komprimierte TAR-Archivdatei) am in den erstellt.

Wenn mehrere Administratoren berechtigt sind, die Control Center-Einstellungen zu verwalten, bietet es sich an, die **Benachrichtigungseinstellungen** so zu konfigurieren, dass Sie jedes Mal benachrichtigt werden, wenn ein Datenbank-Backup erstellt wurde. Weitere Informationen finen Sie im Kapitel **Benachrichtigungen** des GravityZone-Administratorhandbuchs.

Databank-Backups erstellen

So führen Sie ein Datenbank-Backup durch:

1. Öffnen Sie im Control Center die Seite **Konfiguration** und klicken Sie auf den Reiter **Backup**.
2. Klicken Sie auf die Schaltfläche **Backup jetzt durchführen** am oberen Rand der Tabelle. Ein Konfigurationsfenster wird sich öffnen.

3. Wählen Sie die Art des Speicherorts, an dem das Backup-Archiv abgelegt wird:
   - **Lokal**, hierbei wird das Archiv auf der GravityZone-Appliance gespeichert. Dabei müssen Sie den Pfad zum Verzeichnis auf der GravityZone-Appliance angeben, in dem das Archiv gespeichert werden soll.

     Die GravityZone-Appliance hat eine Linux-Verzeichnisstruktur. Sie können das Backup-Archiv z. B. im Verzeichnis `tmp` speichern. Geben Sie dazu `/tmp` in das **Pfad**-Feld ein.
   - **FTP**, hierbei wird das Backup-Archiv auf einem FTP-Server gespeichert. Geben Sie dazu die FTP-Details in die folgenden Felder ein.
   - **Netzwerk**, hierbei wird das Archiv auf einer Netzwerkfreigabe gespeichert. Geben Sie dazu den Pfad zum gewünschten Netzwerkspeicherort ein (z. B. `\\Computer\Ordner`) sowie den Domänennamen und die Zugangsdaten des Domänenbenutzers.
4. Klicken Sie auf die Schaltfläche **Einstellungen testen**. Ein Hinweis wird Ihnen mitteilen, ob die Einstellungen gültig sind oder nicht.

   Damit das Backup erstellt werden kann müssen alle Einstellungen gültig sein.
5. Klicken Sie auf **Generieren**. Die Seite **Backup** wird geöffnet. Ein neuer Backup-Eintrag wird der Liste hinzugefügt. Überprüfen Sie den **Status** des neu erstellten Backups. Nachdem das Backup erstellt wurde, finden Sie die entsprechende `tgz`-Datei am festgelegten Speicherort.

> **Beachten Sie**
> In der Liste auf der Seite **Backup** sind die Protokolle aller erstellen Backups aufgeführt. Über die Protokolle können Sie nicht auf die Backup-Archive zugreifen; sie enthalten lediglich Informationen zu den erstellten Backups.

So planen Sie ein Datenbank-Backup:

1. Öffnen Sie im Control Center die Seite **Konfiguration** und klicken Sie auf den Reiter **Backup**.
2. Klicken Sie auf die Schaltfläche **Backup-Einstellungen** am oberen Rand der Tabelle. Ein Konfigurationsfenster wird sich öffnen.
3. Wählen Sie **Geplantes Backup**.
4. Legen Sie ein Backup-Intervall (täglich, wöchentlich oder monatlich) sowie eine Startzeit fest.

So können Sie zum Beispiel Backups wöchentlich jeden Freitag um 22:00 Uhr durchführen lassen.

5. Konfigurieren Sie den Speicherort für das Backup.
6. Wählen Sie die Art des Speicherorts, an dem das Backup-Archiv abgelegt wird:
   - **Lokal**, hierbei wird das Archiv auf der GravityZone-Appliance gespeichert. Dabei müssen Sie den Pfad zum Verzeichnis auf der GravityZone-Appliance angeben, in dem das Archiv gespeichert werden soll.

     Die GravityZone-Appliance hat eine Linux-Verzeichnisstruktur. Sie können das Backup-Archiv z. B. im Verzeichnis `tmp` speichern. Geben Sie dazu `/tmp` in das **Pfad**-Feld ein.
   - **FTP**, hierbei wird das Backup-Archiv auf einem FTP-Server gespeichert. Geben Sie dazu die FTP-Details in die folgenden Felder ein.
   - **Netzwerk**, hierbei wird das Archiv auf einer Netzwerkfreigabe gespeichert. Geben Sie dazu den Pfad zum gewünschten Netzwerkspeicherort ein (z. B. `\\Computer\Ordner`) sowie den Domänennamen und die Zugangsdaten des Domänenbenutzers.
7. Klicken Sie auf die Schaltfläche **Einstellungen testen**. Ein Hinweis wird Ihnen mitteilen, ob die Einstellungen gültig sind oder nicht.

   Damit das Backup erstellt werden kann müssen alle Einstellungen gültig sein.
8. Klicken Sie auf **Speichern**, um das geplante Backup zu erstellen.

Databank-Backup wiederherstellen

Falls aus irgendeinem Grund Ihre GravityZone-Instanz nicht ordnungsgemäß funktioniert (fehlgeschlagene Updates, funktionsgestörtes Interface, fehlerhafte Datei, Störungen etc.), können Sie die GravityZone-Databank über eine Backup-Kopie folgendermaßen wiederherstellen:

- Unter Verwendung der gleichen Appliance
- Mit einem neuen GravityZone-Image
- Mithilfe der Replica-Set-Funktion

Wählen Sie die Option, die am besten zu Ihrer Situation passt, und fahren Sie mit dem Wiederherstellungsvorgang fort. Beachten Sie dabei jedoch unbedingt die im Folgenden beschriebenen Voraussetzungen.

Wiederherstellung der Datenbank auf der gleichen virtuellen GravityZone-Appliance

Vorbereitende Maßnahmen

- Eine SSH-Verbindung mit der GravityZone-Appliance unter Verwendung der **Root**-Rechte.

  Sie können die **putty**- und **bdadmin**-Zugangsdaten verwenden, um über SSH eine Verbindung mit der Appliance herzustellen, und dann den Befehl `sudo su` ausführen, um zum **Root**-Konto zu wechseln.
- Die GravityZone-Infrastruktur hat sich seit der Sicherung nicht verändert.
- Das Backup ist neuer als 30. April 2017, und die GravityZone-Version ist neuer als 6.2.1-30. Andernfalls wenden Sie sich bitte an den technischen Support.
- In verteilten Architekturen wurde GravityZone nicht für die Verwendung der Datenbankreplikation konfiguriert (Replica Set).

  So können Sie die Konfiguration überprüfen:

  1. Öffnen Sie die Datei `/etc/mongodb.conf`.
  2. Stellen Sie sicher, dass `replSet` nicht konfiguriert ist. Sehen Sie dazu folgendes Beispiel:

     ```
     # replSet = setname
     ```

  Beachten Sie
  Informationen zur Wiederherstellung der Datenbank bei aktiviertem Replica-Set finden Sie in Abschnitt „Wiederherstellung der Datenbank in einer Replica-Set-Umgebung“ (S. 89).

- Es laufen keine CLI-Prozesse.

  Führen Sie folgenden Befehl aus, um sicherzustellen, dass alle CLI-Prozesse beendet wurden:

  ```
  # killall -9 perl
  ```

- Das **mongoconsole**-Paket wurde auf der Appliance installiert.

Führen Sie folgenden Befehl aus, um zu überprüfen, ob die Bedingung erfüllt wird:

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

Der Befehl sollte keine Fehler zurückgeben, führen Sie andernfalls Folgendes aus:

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

Wiederherstellung der Datenbank

1. Rufen Sie den Speicherort des Datenbankarchivs auf:

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

Dabei steht `diretory-with-backup` für den Pfad zum Speicherort, an dem die Sicherungsdateien gespeichert sind.

Zum Beispiel:

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

2. Stellen Sie die Datenbank wieder her.

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

Wichtig

Achten Sie darauf, `GZ_db_password` durch das tatsächlich verwendete Passwort des GravityZone-Datenbank-Servers und die Zeitstempelvariablen im Archivnamen durch das eigentliche Datum zu ersetzen.
Das eigentliche Datum sollte beispielsweise wie folgt aussehen:

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

3. Starten Sie die Appliances neu.

   Die Datenbankwiederherstellung ist damit abgeschlossen.

Wiederherstellung der Datenbank von einer deaktivierten virtuellen GravityZone-Appliance

Vorbereitende Maßnahmen

- Eine neu installierte virtuelle GravityZone-Appliance:
  - mit der gleichen IP wie die alte Appliance
  - bei der NUR die Datenbank-Server-Rolle installiert wurde.

  Sie können das Image für die virtuelle GravityZone-Appliance hier herunterladen.
- Eine SSH-Verbindung mit der virtuellen GravityZone-Appliance unter Verwendung der **Root**-Rechte.
- Die GravityZone-Infrastruktur hat sich seit Erstellung der Sicherung nicht verändert.
- Das Backup ist neuer als 30. April 2017.
- In verteilten Architekturen wurde GravityZone nicht für die Verwendung der Datenbankreplikation konfiguriert (Replica Set).

  Falls in Ihrer GravityZone-Umgebung ein Replica Set zum Einsatz kommt, wurde die Datenbank-Server-Rolle auch auf anderen Appliance-Instanzen installiert.

  Informationen zur Wiederherstellung der Datenbank bei aktiviertem Replica-Set finden Sie in Abschnitt „Wiederherstellung der Datenbank in einer Replica-Set-Umgebung“ (S. 89).

Wiederherstellung der Datenbank

1. Verbinden Sie sich über SSH mit der GravityZone-Appliance und wechseln Sie zu **root**.
2. Beenden Sie VASync:

```
# stop vasync
```

3. Halten Sie die Kommandozeilenoberfläche an:

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

4. Öffnen Sie den Speicherort, an dem sich das Backup befindet:

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

Dabei steht `diretory-with-backup` für den Pfad zum Speicherort, an dem die Sicherungsdateien gespeichert sind.

Zum Beispiel:

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

5. Stellen Sie die Datenbank wieder her.

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

Wichtig

Achten Sie darauf, `GZ_db_password` durch das tatsächlich verwendete Passwort des GravityZone-Datenbank-Servers und die Zeitstempelvariablen im Archivnamen durch das eigentliche Datum zu ersetzen.
Das eigentliche Datum sollte beispielsweise wie folgt aussehen:

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

6. Stellen Sie die alte Appliance-Kennung wieder her:

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

Wichtig
Achten Sie darauf, `GZ_db_password` durch das tatsächlich verwendete Passwort des GravityZone-Datenbank-Servers zu ersetzen.

7. Entfernen Sie die Verweise auf alte Rollen.

```
# /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
```

Wichtig
Achten Sie darauf, `GZ_db_password` durch das tatsächlich verwendete Passwort des GravityZone-Datenbank-Servers zu ersetzen.

8. Starten Sie VASync:

```
# start vasync
```

9. Starten Sie die Kommandozeilenoberfläche:

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

10. Installieren Sie die anderen Rollen.

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

Bitte beachten Sie, dass ein Upgrade des Datenbankschemas zur aktuellen Version erfolgreich durchgeführt wurde:

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

```
"updateTimestamp" : 1456825625581,
"version" : "000-002-011"
}
```

11. Starten Sie die Appliance neu.

    Die Datenbankwiederherstellung ist damit abgeschlossen.

Wiederherstellung der Datenbank in einer Replica-Set-Umgebung

Wenn Sie die Datenbank in einer Replica-Set-Umgebung installiert haben, finden Sie die offizielle Anleitung zur Wiederherstellung im englischsprachigen Online-Handbuch von mongoDB.

Beachten Sie
Dieses Verfahren erfordert technische Fachkenntnisse und sollte daher nur von einem geschulten Fachmann durchgeführt werden. Sollten Sie auf Schwierigkeiten stoßen, wenden Sie sich bitte an unseren Technischen Support. Hier erhalten Sie Unterstützung bei der Wiederherstellung der Datenbank.

Active Directory

Über die Active-Directory-Integration können Sie bestehende Inventare vom unternehmensinternen Active Directory und vom in Microsoft Azure gehosteten Active Directory ins Control Center importieren. So können Sie die Verwaltung, Überwachung, Berichterstattung und nicht zuletzt die Sicherheitsverwaltung vereinfachen. Active-Directory-Benutzern können im Control Center verschiedene Benutzerrollen zugewiesen werden.

So integrieren und synchronisieren Sie GravityZone mit einer Active-Directory-Domain:

1. Klicken Sie unter **Konfiguration > Active Directory > Domains** auf ⊕ **Hinzufügen**.
2. Konfigurieren Sie die erforderlichen Einstellungen:
   - Synchronisationsintervall (in Stunden)
   - Active-Directory-Domain-Name (inkl. Domain-Endung)
   - Benutzername und Passwort eines Domain-Administrators
   - Bereich im Netzwerkinventar, an dem die AD-Endpunkte angezeigt werden sollen:
     - AD-Struktur beibehalten und leere Organisationseinheiten ignorieren

  - AD-Struktur ignorieren und in Benutzerdefinierte Gruppen importieren
  - AD-Struktur nur für ausgewählte Organisationseinheiten beibehalten
- Der Domänencontroller, mit dem sich das Control Center synchronisiert. Klappen Sie den Bereich **Domänenencontroller anfordern** aus und wählen Sie die Controller aus der Tabelle aus.

3. Klicken Sie auf **Speichern**.

Wichtig
Denken Sie daran, das Benutzerpasswort auch im Control Center zu aktualisieren, wenn es sich einmal ändert.

Zugriffsberechtigungen

Mit Zugriffsberechtigungen können Sie dem GravityZone Control Center den Zugriff auf Active Directory (AD)-Benutzer auf Grundlage von Zugriffsregeln gewähren. Informationen zur Integration und Synchronisation von AD-Domänen finden Sie im Abschnitt Active Directory. Weitere Informationen zur Verwaltung von Benutzerkonten über Zugriffsregeln finden Sie im Kapitel **Benutzerkonten** im GravityZone-Installationshandbuch.

Virtualisierungsanbieter

GravityZone kann derzeit mit VMware vCenter Server, Citrix XenServer, Nutanix Prism Element, Amazon EC2 und Microsoft Azure integriert werden.

- „Integration mit vCenter Server“ (S. 91)
- „Integration mit XenServer“ (S. 94)
- „Integration mit Nutanix Prism Element“ (S. 95)
- „Integration mit Amazon EC2“ (S. 96)
- „Integration mit Microsoft Azure“ (S. 97)
- „Verwalten von Plattformintegrationen“ (S. 99)

Wichtig
Vergessen Sie nicht, bei jeder Einrichtung einer neuen Integration mit einem anderen vCenter-Server-, XenServer-, Nutanix-Prism-Element- oder Microsoft-Azure-System, die Zugriffsrechte bestehender Benutzer zu überprüfen und gegebenenfalls anzupassen.

Integration mit vCenter Server

Sie können GravityZone mit einem oder mehreren vCenter-Server-Systemen integrieren. vCenter Server-Systems im Linked Mode müssen separat zum Control Center hinzugefügt werden.

So richten Sie die Integration mit einem vCenter-Server ein:

1. Öffnen Sie im Control Center die Seite **Konfiguration** und klicken Sie danach auf **Virtualisierungsanbieter > Management-Plattformen**.
2. Klicken Sie auf die Schaltfläche ⊕ **Hinzufügen** am oberen Rand der Tabelle, und wählen Sie **vCenter Server** aus dem Menü. Ein Konfigurationsfenster wird sich öffnen.
3. Geben Sie die Informationen des vCenter-Servers an.
   - Name des vCenter-Server-Systems im Control Center
   - Hostname oder IP-Adresse des vCenter-Server-Systems
   - vCenter-Server-Port (standardmäßig `443`)
4. Geben Sie die Zugangsdaten für die Authentifizierung am vCenter-Server an. Sie können die Zugangsdaten für die Integration mit Active Directory oder andere Zugangsdaten verwenden. Der Benutzer, dessen Zugangsdaten Sie angeben, muss auf dem vCenter-Server Root-Administratorenrechte haben.
5. Wählen Sie die in Ihrer Umgebung installierte VMware-Plattform, und konfigurieren Sie die Einstellungen folgendermaßen:
   - **Keine**. Wählen Sie diese Option für NSX-T oder wenn keine VMware-spezifische Plattform installiert ist und klicken Sie anschließendauf **Speichern**. Das selbst signierte Sicherheitszertifikat muss akzeptiert werden, damit die Integration funktioniert.

     Weitere Details zur Konfiguration der Integration mit NSX-T Manager und zum Endpunktschutz für VMs über die GravityZone Guest-Introspection-Richtlinie finden Sie in diesem Artikel.
   - **vShield**. Geben Sie die Informationen des vShield-Manager-Systems an, das mit dem vCenter-Server integriert ist.
     - Hostname oder IP-Adresse des vShield-Manager-Systems
     - vShield-Manager-Port (standardmäßig `443`)
   - **NSX-V**. Geben Sie die Informationen des NSX Managers ein, der mit dem vCenter-Server integriert ist.

Beachten Sie
Eine Anleitung zum Upgrade von VMware vShield auf NSX finden Sie in diesem Artikel in der Wissensdatenbank.

- Host-Name oder IP-Adresse des NSX-Managers
- NSX-Manager-Port (standardmäßig `443`)
- Verwendeter Benutzername und Passwort zur Authentifizierung auf NSX-Manager.

  Diese Zugangsdaten werden in dem schutzfähigen Element und nicht im Zugangsdaten-Manager gespeichert.
- Markieren Sie das Kästchen **Kennzeichnen, wenn ein Virus erkannt wird**, um die standardmäßigen NSX-Sicherheitstags zu verwenden, sobald auf Ihrer virtuellen Maschine Malware gefunden wird.

  Eine Maschine kann je nach Risikostufe der Bedrohung durch drei verschiedene Sicherheits-Tags gekennzeichnet sein.

  - `ANTI_VIRUS.VirusFound.threat=niedrig` gilt für Maschinen, auf denen Bitdefender Malware mit niedrigem Risikopotenzial gefunden hat, die gelöscht werden kann.
  - `ANTI_VIRUS.VirusFound.threat=mittel` gilt für Maschinen, auf denen Bitdefender die infizierten Dateien nicht löschen kann, sondern sie stattdessen desinfiziert.
  - `ANTI_VIRUS.VirusFound.threat=hoch` gilt für Maschinen, auf denen Bitdefender die infizierten Dateien weder löschen noch desinfizieren kann, sondern stattdessen den Zugriff darauf blockiert.

  Werden Bedrohungen mit unterschiedlichen Risikostufen auf der gleichen Maschine erkannt, werden alle entsprechenden Tags angewendet. Eine Maschine, auf der z.B. eine Malware mit hoher und niedriger Risikostufe gefunden wird, ist mit beiden Sicherheitstags markiert.

  Beachten Sie
  In VMware vSphere finden Sie die Sicherheits-Tags im Reiter **Netzwerk& Sicherheit> NSX Manager >** `NSX Manager` **> Verwalten> Sicherheits-Tags**.
  Sie können zwar beliebig viele Tags anlegen, doch nur die drei vorgenannten Tags funktionieren auch mit Bitdefender.

6. **Richtlinienzuweisung aus der Netzwerkansicht einschränken**. Mit dieser Option können Sie Netzwerkadministratoren die Berechtigung entziehen, Richtlinien für virtuelle Maschinen über die Ansicht **Computer und Virtuelle Maschinen** auf der Seite **Netzwerk** zu ändern. Wenn diese Option aktiv ist, können Administratoren Richtlinien für virtuelle Maschinen nur über die Ansicht **Virtuelle Maschinen** im Netzwerkinventar ändern.
7. Klicken Sie auf **Speichern**. Sie werden aufgefordert, die Sicherheitszertifikate für vCenter Server und NSX Manager zu akzeptieren. Diese Zertifikate stellen die sichere Kommunikation zwischen GravityZone und den VMware-Komponenten sicher und verhindern Man-in-the-Middle-Angriffe.

   Sie können überprüfen, ob die richtigen Zertifikate installiert wurden, indem Sie die Seiteninformationen für die jeweiligen VMware-Komponenten im Browser mit den Zertifikatinformationen vergleichen, die in der Control Center angezeigt werden.
8. Markieren Sie die Kästchen, um der Nutzung der Zertifikate zuzustimmen.
9. Klicken Sie auf **Speichern**. In der aktiven Integrationsliste wird der vCenter Server angezeigt.
10. Wenn Sie die NSX-V-Plattform verwenden:
    a. Öffnen Sie den Reiter **Update > Komponenten**.
    b. Laden und veröffentlichen Sie das **Security Server (VMware mit NSX)**-Paket. Weitere Informationen zur Aktualisierung der GravityZone- Komponenten finden Sie unter „Aktualisieren von GravityZone“ (S. 196).
    c. Wechseln Sie zum Reiter **Konfiguration > Virtualisierungsanbieter**
    d. Klicken Sie in der Spalte **Aktion** auf die Schaltfläche **Register**, die dem mit NSX integriertem vCenter entspricht, und registrieren Sie den Bitdefender-Service mit VMware NSX Manager.

Warnung
Sollte das Sicherheitszertifikat abgelaufen sein, wenn das vCenter einen Synchronisierungsversuch unternimmt, werden Sie per Pop-up-Fenster zur Aktualisierung aufgefordert. Rufen Sie das Konfigurationsfenster der vCenter-Server-Integration auf und klicken Sie auf **Speichern**, akzeptieren Sie die neuen Zertifikate und klicken Sie erneut auf **Speichern**.

Nach Registrierung fügt Bitdefender folgendes zur VMware vSphere-Konsole hinzu:

- Bitdefender-Service
- Bitdefender-Service-Manager
- Drei neue Standard-Service-Profile für tolerante, normale und aggressive Scan-Modi.

> **Beachten Sie**
> Diese Service-Profile werden auch auf der **Richtlinien**-Seite in Control Center angezeigt. Für weitere Informationen klicken Sie die Schaltfläche **Spalten** im oberen rechten Fensterbereich an.

Zum Schluss sehen Sie, dass das vCenter Server einen Synchronisierungsvorgang ausführt. Es dauert einige Minuten, bis die Synchronisation abgeschlossen ist.

Integration mit XenServer

Sie können GravityZone mit einem oder mehreren XenServer-Systemen integrieren.

So richten Sie die Integration mit einem XenServer ein:

1. Öffnen Sie im Control Center die Seite **Konfiguration** und wechseln Sie zum Reiter **Virtualisierungsanbieter**.
2. Klicken Sie auf die Schaltfläche ⊕ **Hinzufügen** am oberen Rand der Tabelle, und wählen Sie **XenServer** aus dem Menü. Ein Konfigurationsfenster wird sich öffnen.
3. Geben Sie die Informationen des XenServers an.
   - Name des XenServer-Systems im Control Center
   - Hostname oder IP-Adresse des XenServer-Systems
   - XenServer-Port (standardmäßig `443`)
4. Geben Sie die Zugangsdaten für die Authentifizierung am XenServer an. Sie können die Zugangsdaten für die Integration mit Active Directory oder andere Zugangsdaten verwenden.
5. **Richtlinienzuweisung aus der Netzwerkansicht einschränken**. Mit dieser Option können Sie Netzwerkadministratoren die Berechtigung entziehen, Richtlinien für virtuelle Maschinen über die Ansicht **Computer und Virtuelle Maschinen** auf der Seite **Netzwerk** zu ändern. Wenn diese Option aktiv ist, können Administratoren Richtlinien für virtuelle Maschinen nur über die Ansicht **Virtuelle Maschinen** im Netzwerkinventar ändern.

6. Klicken Sie auf **Speichern**. Das vCenter Server und der Synchronisationsvorgang werden in der aktiven Integrationsliste angezeigt. Es dauert einige Minuten, bis die Synchronisation abgeschlossen ist.

Integration mit Nutanix Prism Element

Sie können das GravityZone mit einem oder mehreren Nutanix Prism Element-Clustern integrieren, unabhängig davon, ob diese bei Nutanix Prism Central registriert sind oder nicht.

Gehen Sie folgendermaßen vor, um die Integration mit Nutanix Prism Element einzurichten:

1. Öffnen Sie im Control Center die Seite **Konfiguration** und wechseln Sie zum Reiter **Virtualisierungsanbieter**.
2. Klicken Sie auf die Schaltfläche ⊕ **Hinzufügen** am oberen Rand der Tabelle, und wählen Sie **Nutanix Prism Element** aus dem Menü. Ein Konfigurationsfenster wird sich öffnen.
3. Geben Sie die Nutanix Prism Element-Details an:
   - Name des Nutanix Prism Element im Control Center.
   - Die IP-Adresse einer Controller Virtual Machine (CVM) aus dem Nutanix Prism Element-Cluster oder die IP-Adresse der Cluster Virtual IP.
   - Nutanix Prism Element-Port (Standard `9440`).
4. Geben Sie die Zugangsdaten für die Authentifizierung bei Nutanix Prism Element an.

   Wichtig
   Der Benutzer, dessen Anmeldedaten Sie angeben, muss über Cluster-Admin- oder User-Admin-Rechte in Nutanix Prism Element verfügen.

5. **Richtlinienzuweisung aus der Netzwerkansicht einschränken**. Mit dieser Option können Sie die Berechtigung der Netzwerkadministratoren steuern, die Richtlinien für virtuelle Maschinen über die Ansicht **Computer und Virtuelle Maschinen** auf der Seite **Netzwerk** zu ändern. Wenn diese Option aktiv ist, können Administratoren Richtlinien für virtuelle Maschinen nur über die Ansicht Virtuelle Maschinen im Netzwerkinventar ändern.

6. Klicken Sie auf **Speichern**. Sie werden aufgefordert, die Sicherheitszertifikate für Nutanix Prism zu akzeptieren. Diese Zertifikate stellen die sichere Kommunikation zwischen GravityZone und Nutanix Prism Element sicher und verhindern Man-in-the-Middle-Angriffe.

   Sie können überprüfen, ob die richtigen Zertifikate installiert wurden, indem Sie die Seiteninformationen für jeden Nutanix Prism Element-Cluster oder CVM mit den im Control Center angezeigten Zertifikatinformationen abgleichen.

7. Markieren Sie die Kästchen, um der Nutzung der Zertifikate zuzustimmen.

8. Klicken Sie auf **Speichern**.

   Wenn Sie zur Konfiguration der Integration eine CVM IP eingeben haben, werden Sie in einem neuen Fenster gefragt, ob Sie die Cluster Virtual IP anstelle der CVM IP verwenden möchten:

   a. Klicken Sie auf **Ja**, um die Cluster Virtual IP für die Integration zu verwenden. Die Cluster Virtual IP ersetzt die CVM IP in den Nutanix Prism Element-Details.

   b. Klicken Sie auf **Nein**, um die CVM IP weiterhin zu nutzen.

      Beachten Sie
      Als Best Practice empfiehlt es sich, die Cluster Virtual IP anstelle der CVM IP zu verwenden. Auf diese Weise bleibt die Integration auch dann aktiv, wenn ein bestimmter Host nicht mehr verfügbar ist.

   c. Klicken Sie im Fenster **Nutanix Prism Element hinzufügen** auf **Speichern**.

In der Liste der aktiven Integrationen wird Nutanix Prism Element angezeigt. Es dauert einige Minuten, bis die Synchronisation abgeschlossen ist.

Integration mit Amazon EC2

Sie können das GravityZone in Ihr Amazon-EC2-Inventar integrieren und Ihre in der Amazon-Cloud gehosteten EC2-Instanzen schützen.

Vorbereitende Maßnahmen:

- Die Zugriffsschüssel und geheimen Schlüssel eines gültigen AWS-Benutzerkontos
- Das AWS-Benutzerkonto muss über die folgenden Berechtigungen verfügen:
  - `IAMReadOnlyAccess`

– `AmazonEC2ReadOnly` für alle AWS-Regionen

Sie können mehrere Amazon-EC2-Integrationen erstellen. Sie müssen für jede Integration ein gültiges AWS-Benutzerkonto angeben.

Beachten Sie
Es ist nicht möglich, mehrere Integrationen unter Verwendung der Anmeldedaten von IAM-Rollen hinzuzufügen, die für dasselbe AWS-Konto erstellt wurden.

So können Sie die Integration mit Amazon EC2 einrichten:

1. Öffnen Sie im Control Center die Seite **Konfiguration** und wechseln Sie zum Reiter **Virtualisierungsanbieter**.
2. Klicken Sie auf die Schaltfläche ⊕ **Hinzufügen** am oberen Rand der Tabelle, und wählen Sie **Amazon-EC2-Integration** aus dem Menü. Ein Konfigurationsfenster wird sich öffnen.
3. Geben Sie die Details für die Amazon-EC2-Integration an:
   - Name der Integration. Falls Sie mehrere Amazon-EC2-Integrationen hinzufügen, können Sie diese anhand ihres Namens identifizieren.
   - Die Zugriffsschüssel und geheimen Schlüssel des AWS-Benutzerkontos.
4. **Richtlinienzuweisung aus der Netzwerkansicht einschränken**. Mit dieser Option können Sie Netzwerkadministratoren die Berechtigung entziehen, Richtlinien für virtuelle Maschinen über die Ansicht **Computer und Virtuelle Maschinen** auf der Seite **Netzwerk** zu ändern. Wenn diese Option aktiv ist, können Administratoren Richtlinien für virtuelle Maschinen nur über die Ansicht **Virtuelle Maschinen** im Netzwerkinventar ändern.
5. Klicken Sie auf **Speichern**. Wenn die angegebenen Anmeldedaten gültig sind, wird die Integration erstellt und dem Grid hinzugefügt.

Warten Sie einige Augenblicke, während GravityZone sich mit dem Amazon-EC2-Inventar synchronisiert.

Integration mit Microsoft Azure

Sie können GravityZone mit Microsoft Azure integrieren und so Ihre in der Microsoft-Cloud gehosteten virtuellen Maschinen schützen.

Vorbereitende Maßnahmen:

- Azure-Anwendung mit der Berechtigung Leser

- Active-Directory-ID
- Anwendungs-ID
- Anwendungsgeheimnis

Mehr Details dazu, wie Sie die nötigen Zugangsdaten erhalten und die Azure-Anwendung einrichten, erfahren Sie in diesem Artikel.

Sie können mehrere Microsoft-Azure-Integrationen erstellen. Für jede Integration ist eine gültige Active-Directory-ID nötig.

So richten Sie eine Integration mit Microsoft-Azure ein:

1. Öffnen Sie im Control Center die Seite **Konfiguration** und wechseln Sie zum Reiter **Virtualisierungsanbieter**.
2. Klicken Sie auf die Schaltfläche ⊕ **Hinzufügen** am oberen Rand der Tabelle, und wählen Sie **Azure-Integration** aus dem Menü. Ein Konfigurationsfenster wird sich öffnen.
3. Legen Sie die Details der Azure-Integration fest:
   - **Der Name der Integration**. Falls Sie mehrere Azure-Integrationen hinzufügen, können Sie diese anhand ihres Namens identifizieren.
   - **Active-Directory-ID**. Zu jeder Instanz eines Azure-Active-Directory steht in den Microsoft-Azure- Kontodetails eine eigene Bezeichnung.
   - **Anwendungs-ID**. Für jede Azure-Anwendung steht eine eigene Bezeichnung in den Anwendungsdetails.
   - **Anwendungsgeheimnis**. Das Anwendungsgeheimnis ist der Wert, der angezeigt wird, wenn ein Schlüssel in den Einstellungen der Azure-Anwendung gespeichert wird.
4. Wählen Sie die Option **Richtlinienzuweisung aus der Netzwerkansicht einschränken**, wenn Sie möchten, dass Richtlinien nur aus der Ansicht **Virtuelle Maschinen** geändert werden können. Wird diese Option deaktiviert, können Richtlinien auch aus der Ansicht **Computer und Virtuelle Maschinen** geändert werden.
5. Klicken Sie auf **Speichern**. Wenn die angegebenen Anmeldedaten gültig sind, wird die Integration erstellt und dem Grid hinzugefügt.

Warten Sie einige Augenblicke, während GravityZone sich mit dem Microsoft-Azure-Inventar synchronisiert.

Verwalten von Plattformintegrationen

So können Sie eine Plattformintegration bearbeiten oder aktualisieren:

1. Wechseln Sie im Control Center zum Reiter **Konfiguration > Virtualisierung**.
2. Klicken Sie die Schaltfläche **Bearbeiten** in der Spalte **Aktion**.
3. Konfigurieren Sie die Regeleinstellungen nach Bedarf. Weitere Information entsprechend Ihren Anforderungen finden Sie in den folgenden Bereichen:
   - „Integration mit vCenter Server“ (S. 91)
   - „Integration mit XenServer“ (S. 94)
   - „Integration mit Nutanix Prism Element“ (S. 95)
   - „Integration mit Amazon EC2“ (S. 96)
   - „Integration mit Microsoft Azure“ (S. 97)
4. Klicken Sie auf **Speichern**. Warten Sie einige Minuten; der Server sychnronisiert.

Integrationen mit Nutanix Prism Element, Amazon EC2 und Microsoft Azure werden automatisch alle 15 Minuten synchronisiert. Sie können eine Integration jederzeit manuell synchronisieren. Gehen Sie dazu wie folgt vor:

1. Wechseln Sie im Control Center zum Reiter **Konfiguration > Virtualisierung**.
2. Klicken Sie in der Spalte **Aktion** auf die Schaltfläche **Inventar neu synchronisieren**.
3. Zum Bestätigen der Aktion klicken Sie **Ja**.

Die Schaltfläche **Inventar neu synchronisieren** ist besonders dann nützlich, wenn sich der Status der Integration ändert und eine Synchronisation erforderlich macht. So zum Beispiel unter folgenden Umständen:

- Für die Integration mit Nutanix Prism Element:
  - Der Benutzer verfügt im Inventar nicht mehr über Administratorrechte.
  - Der Benutzer wird ungültig (verändertes oder gelöschtes Passwort).
  - Das Sicherheitszertifikat wird ungültig.
  - Es gibt einen Verbindungsfehler.
  - Ein Host wird einem Nutanix-Prism-Element-Cluster hinzugefügt oder daraus entfernt.
- Für die Integration mit Microsoft Azure:
  - In Microsoft Azure wird ein Abonnement hinzugefügt oder entfernt.

– Virtuelle Maschinen werden im Microsoft-Azure-Inventar hinzugefügt oder daraus entfernt.

Sie können die Integration auch synchronisieren, indem Sie auf die **Bearbeiten**-Schaltfläche und danach auf **Speichern** klicken.

So entfernen Sie eine Integration mit vShield, XenServer, Nutanix Prism Element, Amazon EC2 oder Microsoft Azure:

1. Wechseln Sie im Control Center zum Reiter **Konfiguration > Virtualisierung**.
2. Klicken Sie die Schaltfläche **Löschen** in der Spalte **Aktion** an, die der zu entfernenden Integration entspricht.
3. Zum Bestätigen der Aktion klicken Sie **Ja**.

So entfernen Sie eine NSX-Integration:

1. Loggen Sie sich in die VMware vSphere-Konsole ein und löschen Sie alle Bitdefender-Richtlinien und Security Server.
2. Wechseln Sie im Control Center zum Reiter **Konfiguration > Virtualisierung**.
3. In der Spalte **Aktion**, die der zu entfernenden Integration entspricht, klicken Sie **Deregistrieren** an und dann **Löschen**.
4. Zum Bestätigen der Aktion klicken Sie **Ja**.

Um sicherzustellen, dass die neuesten Informationen angezeigt werden, klicken Sie am oberen Rand der Tabelle auf **Neu laden**.

Sicherheitsanbieter

GravityZone Security for Virtualized Environments lässt sich über den NSX-T Manager in VMware NSX-T Data Center integrieren.

Integration mit NSX-T Manager

NSX-T Manager ist die Verwaltungsebene für Ihre mit NSX-T Data Center integrierten vCenter-Server. Damit die Integration funktioniert, müssen Sie die Integration für die zum NSX-T Manager zugehörigen vCenter-Server einrichten. Weitere Informationen finden Sie im Abschnitt Integration mit vCenter Server.

Gehen Sie zur Einrichtung der Integration mit NSX-T Manager folgendermaßen vor:

1. Klicken Sie im Control Center auf **Konfiguration > Virtualisierungsanbieter > Sicherheitsanbieter**.

2. Klicken Sie auf die Schaltfläche ⊕**Hinzufügen** am oberen Ende der Tabelle. Ein Konfigurationsfenster wird sich öffnen.
3. Geben Sie die Details für die NSX-T-Integration an:
   - Name der NSX-T-Integration.
   - Hostname oder die IP-Adresse des zugehörigen vCenter Server-Systems.
   - NSX-T-Port (standardmäßig 433).
4. Geben Sie die Zugangsdaten für die Authentifizierung bei vCenter Server an. Sie können die Zugangsdaten für die Integration mit Active Directory oder andere Zugangsdaten verwenden. Der Benutzer, dessen Zugangsdaten Sie angeben, muss auf dem vCenter-Server Root-Administratorenrechte haben.
5. Klicken Sie auf **Speichern**.

   Das Control Center ist nun mit NSX-T integriert. Weitere Informationen zur Anwendung des Endpunktschutzes auf Ihre VMs über die GravityZone Guest Introspection-Richtlinie finden Sie im Artikel Configure and apply endpoint protection to VMware NSX-T guest VMs through GravityZone Guest Introspection policy in der Wissensdatenbank.

Beachten Sie
GravityZone kann nur zum Schutz des zugehörigen vCenter Servers verwendet werden.

NTSA

In diesem Abschnitt können Sie die Integration mit BitdefenderNetwork Traffic Security Analytics konfigurieren. Dabei handelt es sich um eine Lösung für die Unternehmenssicherheit, die Sicherheitsverletzungen zuverlässig erkennt und durch die Analyse des Netzwerkdatenverkehrs auch komplexe Angriffe sichtbar macht. Weitere Informationen zu dieser Lösung finden Sie in der Produktdokumentation zu Bitdefender NTSA.

Wichtig
Der Abschnitt zur NTSA-Integration ist nur verfügbar, wenn auf der Seite **Konfiguration > Lizenz** zuvor ein gültiger Lizenzschlüssel für NTSA eingegeben wurde.

Um die NTSA-Integration konfigurieren zu können, muss die NTSA-Lösung in Ihrer Umgebung installiert sein. Darüber hinaus benötigen Sie die Zugangsdaten für den Zugriff auf die NTSA-Web-Konsole.

Während der Integration müssen Sie die Adresse der NTSA-Web-Konsole (IP-Adresse oder Hostname) und einen Token (Kopplungsschlüssel) angeben, der in der NTSA-Web-Konsole wie im Folgenden erläutert generiert wurde.

Konfiguration der NTSA-Integration

1. Melden Sie sich am GravityZone Control Center an.
2. Öffnen Sie die Seite **Konfiguration** und wechseln Sie zum Reiter NTSA.
3. Aktivieren Sie die Option **Mit Network Traffic Security Analytics (NTSA)** integrieren.
4. Geben Sie die folgenden Daten ein:
   - Die Adresse der NTSA-Web-Konsole (IP / Hostname).
   - Den Port, der von GravityZone für die Kommunikation mit NTSA verwendet wird (standardmäßig 443).
   - Den Kopplungsschlüssel (Token), der von der NTSA-Web-Konsole wie folgt generiert wird:
     a. Rufen Sie Ihre NTSA-Web-Konsole auf und gehen Sie zur Seite **Lizenzierung**.
     b. Wählen Sie die Option **Integration mit GravityZone**.
     c. Klicken Sie auf **Kopplungsschlüssel erzeugen**. Der Schlüssel wird automatisch angezeigt.
     d. Kopieren Sie den Kopplungsschlüssel über die Schaltfläche **In Zwischenablage kopieren**.
     e. Klicken Sie zur Bestätigung auf **OK**.
5. Vergewissern Sie sich, dass der angezeigte Host-Fingerabdruck mit dem Hash des SSL-Zertifikats der NTSA-Appliance übereinstimmt, und aktivieren Sie dann die Option **Ich akzeptiere das Zertifikat**.
6. Klicken Sie auf **Speichern**.

Wenn die Konfiguration erfolgreich abgeschlossen wurde, wird die Integration als **Synchronisiert** angezeigt. Für die NTSA-Integration existieren die folgenden Status:

- **N/V**: Die Integration wurde noch nicht konfiguriert.
- **Synchronisiert**: Die Integration wurde konfiguriert und ist aktiv.

- **Ungültiges Token**: Der Kopplungsschlüssel der NTSA-Web-Konsole ist ungültig.
- **Verbindungsfehler**: Die Verbindung zur angegebenen NTSA-Web-Konsole konnte nicht hergestellt werden (ungültige(r) IP-Adresse / Hostname).
- **Zertifikatfehler**: Der aktuelle Fingerabdruck des SSL-Zertifikats der NTSA-Appliance stimmt nicht mit dem ursprünglich akzeptierten Fingerabdruck überein.
- **Unbekannter Fehler**: Es ist ein unbekannter Kommunikationsfehler aufgetreten.

Das Feld **Letzte Statusänderung** zeigt Datum und Uhrzeit der letzten erfolgreichen Änderung der Integrationseinstellungen bzw. wann sich der Integrationsstatus geändert hat.

Nach Konfiguration der NTSA-Integration können Sie die Integration über das Kästchen oben auf der Seite **NTSA** aktivieren oder deaktivieren.

Verknüpfen der GravityZone- und NTSA-Benutzerkonten

Nach der Konfiguration der Integration werden Ihre Benutzerkonten für GravityZone und NTSA verknüpft und Sie können die NTSA-Web-Konsole ganz bequem wie folgt aufrufen:

1. Klicken Sie unten links im GravityZone Control Center auf die **NTSA**-Schaltfläche.
2. Sie werden zur Anmeldeseite der NTSA-Web-Konsole weitergeleitet. Nach Eingabe Ihrer NTSA-Zugangsdaten können Sie mit der Navigation der NTSA-Web-Konsole beginnen.

   Sie müssen Ihre NTSA-Zugangsdaten nur für die erste Anmeldung eingeben. In der Folge erhalten Sie automatisch und ohne zur Anmeldung aufgefordert zu werden Zugriff auf die NTSA-Web-Konsole, indem Sie auf die Schaltfläche **NTSA** klicken.

Löschen der NTSA-Integration

Wenn Sie den NTSA-Lizenzschlüssel auf der Seite **Konfiguration > Lizenz** löschen, wird auch die NTSA-Integration gelöscht.

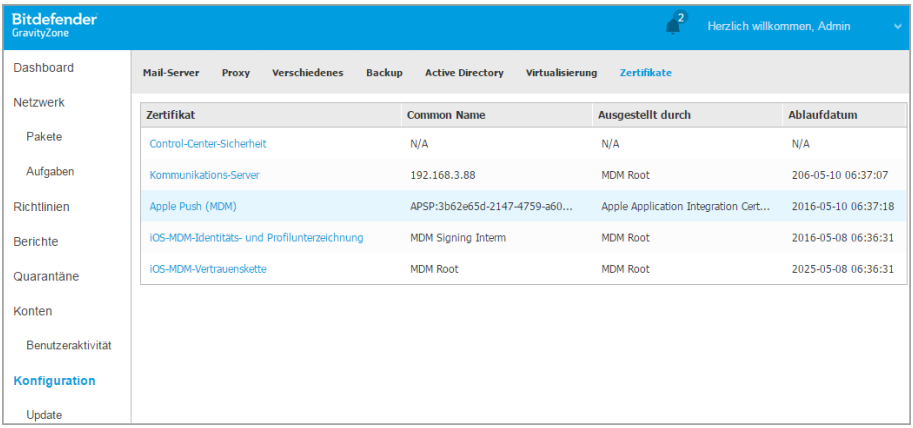
Beachten Sie
Die Verknüpfung zwischen Ihrem NTSA-Benutzerkonto und GravityZone wird unter den folgenden Umständen aufgehoben:

- Der NTSA-Lizenzschlüssel wurde entfernt.

- Ihr NTSA-Passwort wurde geändert.
- Ihr GravityZone-Passwort wurde geändert.
- Die NTSA-Integrationseinstellungen wurden geändert.

Zertifikate

Damit Ihre GravityZone-Installation ordnungsgemäß funktioniert und sicher ist, müssen Sie eine Reihe von Sicherheitszertifikaten im Control Center erstellen und hinzufügen.



Die Seite Zertifikate

Control Center unterstützt die folgenden Zertifikatsformate:

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

Beachten Sie

Die folgenden Zertifikate werden nur für die Verwaltung der Sicherheit auf Apple-Geräten benötigt:

- Kommunikationsserverzertifikat
- Apple-MDM-Push-Zertifikat

- iOS-MDM-Identifikations- und Profilunterzeichnungszertifikat
- iOS-MDM-Vertrauenskettenzertifikat

Wenn Sie nicht vorhaben, iOS-Geräte zu verwalten, brauchen Sie diese Zertifikate nicht.

Control Center-Sicherheitszertifikat

Das Sicherheitszertifikat für das Control Center wird benötigt, um die Web-Konsole des Control Center als vertrauenswürdige Website im Browser zu identifizieren. Standardmäßig verwendet Control Center ein von Bitdefender unterzeichnetes SSL-Zertifikat. Dieses eingebaute Zertifikat wird von Browsern nicht erkannt und löst Sicherheitswarnungen aus. Sicherheitswarnungen Ihres Browsers können Sie verhindern, indem Sie ein SSL-Zertifikat hinzufügen, das entweder von Ihrem Unternehmen oder von einer externen Zertifizierungsstelle (CA) unterzeichnet ist.

So fügen Sie das Control Center-Zertifikat hinzu oder ersetzen es:

1. Gehen Sie zur Seite **Konfiguration** und klicken Sie dann auf den Reiter **Zertifikate**.
2. Klicken Sie auf den Zertifikatsnamen.
3. Wählen Sie den Zertifikatstyp (mit separatem oder eingebetteten privatem Schlüssel).
4. Klicken Sie auf die Schaltfläche **Hinzufügen** neben dem Feld **Zertifikat**, und laden Sie das Zertifikat hoch.
5. Klicken Sie bei Zertifikaten mit separatem privatem Schlüssel auf die Schaltfläche **Hinzufügen** neben dem Feld **Privater Schlüssel**, und laden Sie den privaten Schlüssel hoch.
6. Wenn das Zertifikat passwortgeschützt ist, geben Sie das Passwort in das entsprechende Feld ein.
7. Klicken Sie auf **Speichern**.

Endpunkt - Security Server-Kommunikationssicherheitszertifikat

Dieses Zertifikat sorgt für eine sichere Kommunikation zwischen den Sicherheitsagenten und dem Security Server (Multi-Plattform), der ihnen zugewiesen wurde.

Während seiner Installation generiert der Security Server ein selbstunterzeichnetes Standardzertifikat. Sie können dieses eingebaute Zertifikat ersetzen, indem Sie im Control Center eines Ihrer Wahl hinzufügen.

So fügen Sie ein Endpunkt-Security Server-Kommunikationszertifikat hinzu:

1. Gehen Sie zur Seite **Konfiguration** und klicken Sie dann auf den Reiter **Zertifikate**.
2. Klicken Sie auf den Zertifikatsnamen.
3. Wählen Sie den Zertifikatstyp (mit separatem oder eingebetteten privatem Schlüssel).
4. Klicken Sie auf die Schaltfläche **Hinzufügen** neben dem Feld **Zertifikat**, und laden Sie das Zertifikat hoch.
5. Klicken Sie bei Zertifikaten mit separatem privatem Schlüssel auf die Schaltfläche **Hinzufügen** neben dem Feld **Privater Schlüssel**, und laden Sie den privaten Schlüssel hoch.
6. Wenn das Zertifikat passwortgeschützt ist, geben Sie das Passwort in das entsprechende Feld ein.
7. Klicken Sie auf **Speichern**. Wenn das Zertifikat selbstunterzeichnet oder abgelaufen ist, wird evtl. eine Warnmeldung angezeigt. Falls es abgelaufen ist, verlängern Sie bitte das Zertifikat.
8. Klicken Sie auf **Ja**, um mit dem Hochladen des Zertifikats fortzufahren. Sofort nach Beendigung des Hochladens sendet das Control Center das Sicherheitszertifikat an die Security Server.

Fall nötig können Sie das ursprüngliche eingebaute Zertifikat auf jedem Security Server wie folgt wieder einstellen:

1. Klicken Sie auf der Seite **Zertifikate** auf den Zertifikatsnamen.
2. Wählen Sie als Zertifikatstyp **Kein Zertifikat (Standard verwenden)**.
3. Klicken Sie auf **Speichern**.

Kommunikationsserverzertifikat

Das Kommunikationsserver-Zertifikat wird zur Sicherung der Kommunikation zwischen dem Kommunikationsserver und iOS-Mobilgeräten eingesetzt.

Anforderungen:

- Dieses SSL-Zertifikat kann entweder von Ihrem Unternehmen oder einer externen Zertifizierungsstelle unterzeichnet sein.

Warnung
Das Zertifikat wird unter Umständen ungültig gemacht, wenn dieses nicht von einer öffentlichen/vertrauenswürdigen Zertifizierungsstelle ausgestellt wurde (so z. B. bei selbstsignierten Zertifikaten).

- Der Common Name des Zertifikats muss extrakt mit dem Domain-Namen oder der IP-Adresse übereinstimmen, die von mobilen Clients verwendet wird, um eine Verbindung zum Kommunikationsserver herzustellen. Er ist als externe MDM-Adresse in der Konfigurationsoberfläche der GravityZone-Appliance-Konsole konfiguriert.
- Mobile Clients müssen diesem Zertifikat vertrauen. Hierfür müssen Sie auch die iOS-MDM-Vertrauenskette hinzufügen.

So fügen Sie das Kommunikationsserverzertifikat hinzu oder ersetzen es:

1. Gehen Sie zur Seite **Konfiguration** und klicken Sie dann auf den Reiter **Zertifikate**.
2. Klicken Sie auf den Zertifikatsnamen.
3. Wählen Sie den Zertifikatstyp (mit separatem oder eingebetteten privatem Schlüssel).
4. Klicken Sie auf die Schaltfläche **Hinzufügen** neben dem Feld **Zertifikat**, und laden Sie das Zertifikat hoch.
5. Klicken Sie bei Zertifikaten mit separatem privatem Schlüssel auf die Schaltfläche **Hinzufügen** neben dem Feld **Privater Schlüssel**, und laden Sie den privaten Schlüssel hoch.
6. Wenn das Zertifikat passwortgeschützt ist, geben Sie das Passwort in das entsprechende Feld ein.
7. Klicken Sie auf **Speichern**.

Apple-MDM-Push-Zertifikat

Apple benötigt ein Apple-MDM-Push-Zertifikat, um beim Versand von Push-Benachrichtigungen die Sicherheit der Kommunikation zwischen dem Kommunikationsserver und den Servern des Diensts "Apple Push Notifications" (APNs) sicherzustellen. Mit Push-Benachrichtigungen werden Geräte dazu aufgefordert, eine Verbindung zum Kommunikationsserver herzustellen, wenn dort neue Aufgaben oder Richtlinienänderungen verfügbar sind.

Apple stellt dieses Zertifikat direkt Ihrem Unternehmen zur Verfügung, fordert aber, dass die Anfrage zur Unterzeichnung eines Zertifikat (CSR) von Bitdefender unterzeichnet wird. Im Control Center gibt es einen Assistenten, der Ihnen hilft, ein Apple-MDM-Push-Zertifikat zu erwerben.

Wichtig

- Sie benötigen eine Apple-ID, um das Zertifikat zu erhalten und zu verwalten. Wenn Sie keine Apple-ID haben, können Sie auf der Website My Apple ID eine erstellen. Verwenden Sie zur Registrierung für die Apple ID eine generische E-Mail-Adresse, keine E-Mail-Adresse eines Mitarbeiters, denn Sie brauchen sie später, um das Zertifikat zu verlängern.
- Im Internet Explorer funktioniert die Apple-Website nicht ordnungsgemäß. Wir empfehlen Ihnen, die jeweils aktuelle Version von Safari oder Chrome zu verwenden.
- Das Apple-MDM-Push-Zertifikat ist nur ein Jahr lang gültig. Wenn das Zertifikat in Kürze abläuft, müssen Sie es verlängern und das verlängerte Zertifikat ins Control Center importieren. Wenn Sie das Zertifikat auslaufen lassen, müssen Sie ein neues erstellen und alle Ihre Geräte erneut aktivieren.

Ein Apple-MDM-Push-Zertifikat hinzufügen

So erhalten Sie ein Apple-MDM-Push-Zertifikat und importieren es ins Control Center:

1. Gehen Sie zur Seite **Konfiguration** und klicken Sie dann auf den Reiter **Zertifikate**.
2. Klicken Sie auf den Namen des Zertifikats und verfolgen Sie wie unten beschrieben die Anweisungen des Assistenten:

   Schritt 1 - Eine von Bitdefender unterzeichnete Anfrage zur Unterzeichnung eines Zertifikats erhalten

   Wählen Sie die passende Option:

   - **Ich brauche eine von Bitdefender unterzeichnete Anfrage zur Unterzeichnung eines Zertifikats** (empfohlen)
     a. Geben Sie den Namen Ihres Unternehmens, Ihren vollständigen Namen und Ihre E-Mail-Adresse in die entsprechenden Felder ein.
     b. Klicken Sie auf **Generieren**, um die von Bitdefender unterzeichnete CSR-Datei herunterzuladen.
   - **Ich habe bereits eine Anfrage zur Unterzeichnung eines Zertifikats, und ich benötige die Unterzeichnung von Bitdefender**

a. Laden Sie Ihre CSR-Datei und den dazugehörigen privaten Schlüssel hoch, indem Sie auf die Schaltfläche **Hinzufügen** neben den jeweiligen Feldern klicken.

   Der Kommunikationsserver benötigt den privaten Schlüssel für die Authentifizierung bei den APNs-Servern.
b. Geben Sie das Passwort ein, das den privaten Schlüssel schützt, falls es eins gibt.
c. Klicken Sie auf die Schaltfläche **Unterzeichnen**, um die von Bitdefender unterzeichnete CSR-Datei herunterzuladen.

Schritt 2 - Push-Zertifikat von Apple erhalten

a. Klicken Sie auf den Link **Apple-Push-Zertifikatsportal** und melden Sie sich mit Ihrer Apple ID und Ihrem Passwort an.
b. Klicken Sie auf die Schaltfläche **Zertifikat erstellen** und akzeptieren Sie die Nutzungsbedingungen.
c. Klicken Sie auf **Datei auswählen**, wählen Sie die CSR-Datei und klicken Sie anschließend auf **Hochladen**.

   Beachten Sie
   Je nachdem, welchen Browser Sie benutzen, heißt die Schaltfläche vielleicht nicht **Datei auswählen**, sondern **Auswählen** oder **Durchsuchen** oder so ähnlich.

d. Klicken Sie auf der Bestätigungsseite auf die Schaltfläche **Download**. Dadurch erhalten Sie Ihr MDM-Push-Zertifikat.
e. Kehren Sie zum Assistenten im Control Center zurück.

Schritt 3 - Apple-Push-Zertifikat importieren

Klicken Sie auf die Schaltfläche **Zertifikat hinzufügen**, um die Zertifikatsdatei von Ihrem Computer hochzuladen.

Im Feld unten können Sie die Details des Zertifikats überprüfen.

3. Klicken Sie auf **Speichern**.

Das Apple-MDM-Push-Zertifikat verlängern

So verlängern Sie das Apple-MDM-Push-Zertifikat und aktualisieren es im Control Center:

1. Gehen Sie zur Seite **Konfiguration** und klicken Sie dann auf den Reiter **Zertifikate**.
2. Klicken Sie auf den Namen des Zertifikats, um den Import-Assistenten zu öffnen.

3. Eine von Bitdefender unterzeichnete Anfrage zur Unterzeichnung eines Zertifikats erhalten. Das funktioniert genauso wie ein neues Zertifikat zu erhalten.
4. Klicken Sie auf den Link **Apple-Push-Zertifikatsportal** und melden Sie sich mit derselben Apple ID an, mit der Sie das Zertifikat erstellt haben.
5. Finden Sie das MDM-Push-Zertifikat für Bitdefender und klicken Sie auf die entsprechende Schaltfläche **Verlängern**.
6. Klicken Sie auf **Datei auswählen**, wählen Sie die CSR-Datei und klicken Sie anschließend auf **Hochladen**.
7. Klicken Sie auf **Download**, um das Zertifikat auf Ihrem Computer zu speichern.
8. Kehren Sie zum Control Center zurück, und importieren Sie das neue Apple-Push-Zertifikat.
9. Klicken Sie auf **Speichern**.

iOS-MDM-Identifikations- und Profilunterzeichnungszertifikat

Das iOS-MDM-Identitäts- und -Profil-Signatur-Zertifikat wird vom Kommunikationsserver dazu benutzt, Identitätszertifikate und Konfigurationsprofile, die an mobile Geräte gesendet werden, zu unterzeichnen.

Anforderungen:

- Es muss ein Zwischen- oder Endentitätszertifikat sein, das entweder von Ihrem Unternehmen oder einer externen Zertifizierungsstelle unterzeichnet ist.
- Mobile Clients müssen diesem Zertifikat vertrauen. Hierfür müssen Sie auch die iOS-MDM-Vertrauenskette hinzufügen.

So fügen Sie ein iOS-MDM-Identifikations- und Profilunterzeichnungszertifikat hinzu oder ersetzen es:

1. Gehen Sie zur Seite **Konfiguration** und klicken Sie dann auf den Reiter **Zertifikate**.
2. Klicken Sie auf den Zertifikatsnamen.
3. Wählen Sie den Zertifikatstyp (mit separatem oder eingebetteten privatem Schlüssel).
4. Klicken Sie auf die Schaltfläche **Hinzufügen** neben dem Feld **Zertifikat**, und laden Sie das Zertifikat hoch.
5. Klicken Sie bei Zertifikaten mit separatem privatem Schlüssel auf die Schaltfläche **Hinzufügen** neben dem Feld **Privater Schlüssel**, und laden Sie den privaten Schlüssel hoch.

6. Wenn das Zertifikat passwortgeschützt ist, geben Sie das Passwort in das entsprechende Feld ein.
7. Klicken Sie auf **Speichern**.

iOS-MDM-Vertrauenskettenzertifikat

Die iOS-MDM-Vertrauenskettenzertifikate sind auf mobilen Geräten nötig, um sicherzustellen, dass sie dem Kommunikationsserverzertifikat und dem iOS-MDM-Identitäts- und -Profilunterzeichnungszertifikat vertrauen. Der Kommunikationsserver sendet dieses Zertifikat während ihrer Aktivierung an mobile Geräte.

Die iOS-MDM-Vertrauenskette muss alle Zwischenzertifikate bis hin zum Root-Zertifikat Ihres Unternehmens oder bis zum von der externen Zertifizierungsstelle unterzeichneten Zwischenzertifikat enthalten.

So fügen Sie iOS-MDM-Vertrauenskettenzertifikate hinzu oder ersetzen sie:

1. Gehen Sie zur Seite **Konfiguration** und klicken Sie dann auf den Reiter **Zertifikate**.
2. Klicken Sie auf den Zertifikatsnamen.
3. Klicken Sie auf die Schaltfläche **Hinzufügen** neben dem Feld **Zertifikat**, und laden Sie das Zertifikat hoch.
4. Klicken Sie auf **Speichern**.

Repository

In diesem Reiter werden Informationen über die Updates des Sicherheitsagenten angezeigt, einschließlich der auf dem Update-Server gespeicherten Produktversionen und der im offiziellen Bitdefender-Repository verfügbaren Versionen, der Update-Ringe, des Datums und der Uhrzeit des Updates und der letzten Überprüfung auf neue Versionen.

Beachten Sie
Für Sicherheitsserver sind die Produktversionen nicht verfügbar.

5.1.5. Die GravityZone-Appliance verwalten

Die GravityZone-Appliance verfügt über eine einfache Konfigurationsoberfläche, auf die Sie von dem Verwaltungstool aus zugreifen können, mit dem Sie die virtualisierte Umgebung verwalten, in der Sie die Appliance installiert haben.

Nach der ersten Installation der GravityZone-Appliance stehen die folgenden Hauptoptionen zur Auswahl:

- Hostname-Einstellungen konfigurieren
- Netzwerkeinstellungen konfigurieren
- Proxy-Einstellgn. konf.
- MDM-Kommunikations-Server
- Erweiterte Einstellungen
- Sprache konfigurieren

Mithilfe der Pfeiltasten und der `Tabulator`-Taste können Sie durch die Menüs und Optionen navigieren. Drücken Sie die `Eingabetaste`, um eine bestimmte Option auszuwählen.

Hostname und Einstellungen konfigurieren

Die Kommunikation mit den GravityZone-Rollen funktioniert über die IP-Adresse oder den DNS-Namen derjenigen Appliance, auf denen die jeweilige Rolle installiert ist. Standardmäßig kommunizieren die GravityZone-Komponenten über IP-Adressen. Wenn Sie die Kommunikation über DNS-Namen ermöglichen möchten, müssen Sie den GravityZone-Appliances DNS-Namen zuweisen und sicherstellen, dass diese Namen korrekt zu den konfigurierten IP-Adressen der Appliances aufgelöst werden.

Vorbereitende Maßnahmen:

- Konfigurieren Sie den DNS-Eintrag im DNS-Server.
- Der DNS-Name muss korrekt zur konfigurierten IP-Adresse der Appliance aufgelöst werden. Daher müssen Sie dafür sorgen, dass die Appliance die richtige IP-Adresse hat.

So konfigurieren Sie die Einstellungen für den Hostnamen:

1. Greifen Sie über Ihre Virtualisierungsverwaltungs-Software (z. B. vSphere Client) auf die Appliance-Console zu.
2. Wählen Sie aus dem Hauptmenü **Hostname-Einstellungen konfigurieren**.
3. Geben Sie den Hostnamen der Appliance und (falls nötig) den Namen der Active-Directory-Domäne ein.
4. Wählen Sie **OK**, um die Änderungen zu speichern.

Netzwerkeinstellungen konfigurieren

Sie können die Appliance so einrichten, dass sie die Netzwerkeinstellungen automatisch vom DHCP-Server bezieht, oder Sie können sie manuell konfigurieren. Wenn Sie die DHCP-Methode wählen, müssen Sie den DHCP-Server so konfigurieren, dass er eine bestimmte IP-Adresse für die Appliance reserviert.

So konfigurieren Sie die Netzwerkeinstellungen:

1. Greifen Sie über Ihre Virtualisierungsverwaltungs-Software (z. B. vSphere Client) auf die Appliance-Console zu.
2. Wählen Sie aus dem Hauptmenü **Netzwerkeinstellungen konfigurieren**.
3. Wählen Sie den Netzwerkadapter (standardmäßig `eth0`).
4. Wählen Sie die Konfigurationsmethode:
   - **Netzwerkeinstellungen manuell konfigurieren.** Sie müssen die IP-Adresse, die Netzwerkmaske, die Gateway-Adresse und die DNS-Server-Adressen angeben.
   - **Netzwerkeinstellungen automatisch über DHCP beziehen.** Wählen Sie diese Option nur, wenn Sie den DHCP-Server so konfiguriert haben, dass er eine bestimmte IP-Adresse für die Appliance reserviert.
5. Über die entsprechenden Optionen können Sie die aktuellen Details zur IP-Konfiguration bzw. den Link-Status überprüfen.

Proxy-Einstellgn. konf.

Wenn die Appliance über einen Proxy-Server mit dem Internet verbunden ist, müssen Sie die Proxy-Einstellungen konfigurieren.

Beachten Sie
Die Proxy-Einstellungen können auch über das Control Center auf der Seite **Konfiguration > Proxy** konfiguriert werden. Werden die Proxy-Einstellungen an einer Stelle geändert, werden sie automatisch auch an der anderen Stelle aktualisiert.

So konfigurieren Sie die Proxy-Einstellungen:

1. Greifen Sie über Ihre Virtualisierungsverwaltungs-Software (z. B. vSphere Client) auf die Appliance-Console zu.
2. Wählen Sie aus dem Hauptmenü **Proxy-Einstellungen konfigurieren**.

3. Wählen Sie **Proxy-Einstellungen konfigurieren**.
4. Geben Sie die Adresse des Proxy-Servers ein. Verwenden Sie die folgende Syntax:
   - Wenn der Proxy-Server keine Authentifizierung erfordert:

     `http(s)://<IP-Adresse/Hostname>:<Port>`
   - Wenn der Proxy-Server Authentifizierung erfordert:

     `http(s)://<Benutzername>:<Passwort>@<IP-Adresse/Hostname>:<Port>`
5. Wählen Sie **OK**, um die Änderungen zu speichern.

Wählen Sie **Proxy-Informationen anzeigen**, um die Proxy-Informationen anzuzeigen.

MDM-Kommunikations-Server

Beachten Sie
Diese Konfiguration ist nur für die Verwaltung von Mobilgeräten nötig, falls Ihre Lizenz den Dienst Security for Mobile beinhaltet. Die Option wird im Menü nach der Installation der Kommunikationsserver-Rolle angezeigt.

In der Standardeinrichtung von GravityZone können mobile Geräte nur verwaltet werden, wenn sie direkt mit dem Unternehmensnetzwerk verbunden sind (über WLAN oder VPN). Der Grund dafür ist, dass mobile Geräte bei der Registrierungen so konfiguriert werden, dass sie eine Verbindung zur lokalen Adresse der Kommunikationsserver-Appliance herstellen.

Um mobile Geräte an einem beliebigen Ort über das Internet zu verwalten, müssen Sie eine öffentlich erreichbare Adresse für den Kommunikationsserver konfigurieren.

Zur Verwaltung mobiler Geräte, die nicht mit dem Unternehmensnetzwerk verbunden sind, stehen Ihnen die folgenden Möglichkeiten zur Verfügung:

- Port-Weiterleitung im Unternehmens-Gateway für die Appliance konfigurieren, auf der die Kommunikationsserver-Rolle läuft.
- Einen zusätzlichen Netzwerkadapter zur Appliance, auf der die Kommunikationsserver-Rolle läuft, hinzufügen und ihm eine öffentliche IP-Adresse zuweisen.

In beiden Fällen müssen Sie für den Kommunikationsserver die externe Adresse konfigurieren, die für die Verwaltung mobiler Geräte benutzt werden soll:

1. Greifen Sie über Ihre Virtualisierungsverwaltungs-Software (z. B. vSphere Client) auf die Appliance-Console zu.
2. Wählen Sie aus dem Hauptmenü **MDM-Kommunikationsserver**.
3. Wählen Sie **Externe Adresse des MDM-Servers konfigurieren**
4. Geben Sie die externe Adresse ein.

   Verwenden Sie die folgende Syntax: `https://<IP/Domain>:<Port>`.

   - Wenn Sie Port-Weiterleitung verwenden, müssen Sie erstens die öffentliche IP-Adresse oder den Domain-Namen und zweitens den auf dem Gateway offenen Port eingeben.
   - Wenn Sie die öffentliche Adresse des Kommunikationsservers verwenden, müssen Sie erstens die öffentliche IP-Adresse oder oder den Domain-Namen und zweitens den Kommunikationsserver-Port angeben. Der Standard-Port ist `8443`.
5. Wählen Sie **OK**, um die Änderungen zu speichern.
6. Wählen Sie **Externe Adresse des MDM-Servers anzeigen**, um die Einstellungen zu überprüfen.

Erweiterte Einstellungen

Die erweiterten Einstellungen umfassen mehrere Optionen für die manuelle Bereitstellung, die Erweiterung der Umgebung und die Verbesserung der Sicherheit:

- Rollen installieren/deinstallieren
- Security Server installieren
- Neues Datenbankpasswort festlegen
- Update-Server
- Rollen-Lastverteilungen konfigurieren
- Replikatgruppe
- Secure VPN Cluster aktivieren
- Mit bestehender Datenbank verbinden
- Mit bestehender Datenbank verbinden (Secure VPN Cluster)
- Secure VPN Cluster überprüfen

Die Verfügbarkeit der Optionen hängt von den installierten Rollen und den aktivierten Diensten ab. Wenn beispielsweise die Datenbankserver-Rolle nicht auf der Appliance installiert ist, können Sie nur Rollen installieren oder sich mit einer in Ihrem Netzwerk bereitgestellten GravityZone-Datenbank verbinden. Sobald die Datenbankserver-Rolle auf der Appliance installiert wurde, werden die Optionen für die Verbindung mit einer anderen Datenbank nicht mehr angezeigt.

Rollen installieren/deinstallieren

Auf der GravityZone-Appliance können eine, mehrere oder alle der folgenden Rollen laufen:

- **Datenbank-Server**
- **Update-Server**
- **Web-Konsole**
- **Kommunikationsserver**
- **Vorfallserver**

Für die Installation von GravityZone muss je eine Instanz jeder Rolle laufen. Das bedeutet, dass Sie, je nachdem wie Sie die GravityZone-Rollen verteilen möchten, zwischen einer und vier GravityZone-Appliances installieren werden. Die Datenbank-Server-Rolle ist die, die zuerst installiert wird. In einem Szenario mit mehreren GravityZone-Appliances installieren Sie zunächst die Datenbank-Server-Rolle auf der ersten Appliance und konfigurieren dann alle weiteren Appliances so, dass sie eine Verbindung mit der bestehenden Datenbankinstanz herstellen.

Beachten Sie

Sie können zusätzliche Instanzen bestimmter Rollen mithilfe von Rollen-Lastenverteilungen installieren. Weitere Informationen finden Sie unter „Rollen-Lastverteilungen konfigurieren“ (S. 120).

So installieren Sie GravityZone-Rollen:

1. Greifen Sie über Ihre Virtualisierungsverwaltungs-Software (z. B. vSphere Client) auf die Appliance-Console zu.
2. Wählen Sie im Hauptmenü den Punkt **Erweiterte Einstellungen**.
3. Wählen Sie **Rollen installieren/deinstallieren**.
4. Wählen Sie **Rollen hinzufügen oder entfernen**.
5. Dieser Schritt hängt von Ihrer aktuellen Situation ab:

- Wenn dies die erste Installation einer GravityZone-Appliance ist, drücken Sie die `Leertaste` und dann die `Eingabetaste`, um die Datenbank-Server-Rolle zu installieren. Bestätigen Sie Ihre Auswahl, indem Sie die `Eingabetaste` erneut drücken. Legen Sie das Datenbankkennwort fest und warten Sie, bis der Installationsvorgang abgeschlossen ist.
- Wenn Sie bereits eine andere Appliance mit der Datenbank-Server-Rolle installiert haben, wählen Sie **Abbrechen**, um zum Menü **Rollen hinzufügen oder entfernen** zurückzukehren. Sie müssen dann **Datenbankadresse konfigurieren** wählen und die Adresse des Datenbank-Servers eingeben. Stellen Sie sicher, dass ein Datenbankkennwort festgelegt wurde, bevor Sie auf diese Option zugreifen. Falls Sie das Datenbankkennwort nicht kennen, können Sie im Hauptmenü unter **Erweiterte Einstellungen > Neues Datenbankkennwort festlegen** ein neues Kennwort festlegen.

  Verwenden Sie die folgende Syntax: `http://<IP/Hostname>:<Port>`. Der Standard-Datenbank-Port ist `27017`. Geben Sie das primäre Datenbankkennwort ein.

6. Installieren Sie die anderen Rollen, indem Sie im Menü **Rollen installieren/verändern** den Punkt **Rollen installieren/deinstallieren** und anschließend die zu installierenden Rollen wählen. Drücken Sie für jede Rolle, die Sie installieren oder deinstallieren möchten, die `Leertaste`, um die Rolle zu markieren bzw. die Markierung aufzuheben, und drücken Sie anschließend `Enter`, um fortzufahren. Sie müssen Ihre Wahl noch einmal mit der `Enter`-Taste bestätigen und dann warten, bis die Installation abgeschlossen ist.

Beachten Sie

Die Installation jeder Rolle dauert normalerweise ein paar Minuten. Während der Installation werden benötigte Dateien aus dem Internet heruntergeladen. Daher dauert die Installation länger, wenn die Internetverbindung langsam ist. Wenn die Installation ins Stocken gerät, installieren Sie die Appliance erneut.

Sie können die installierten Rollen und ihre IP-Adressen anzeigen, indem Sie eine der folgenden Optionen aus dem Menü **Rollen installieren/deinstallieren** wählen:

- **Lokal installierte Rollen anzeigen**, wenn Sie nur die auf dieser Appliance installierten Rollen anzeigen möchten.
- **Alle installierten Rollen anzeigen**, wenn Sie alle in Ihrer GravityZone-Umgebung installierten Rollen anzeigen wollen.

Security Server installieren

Beachten Sie
Der Security Server steht nur zur Verfügung, wenn Ihr Lizenzschlüssel ihn abdeckt.

Sie können den Security Server von der Konfigurationsoberfläche der GravityZone-Appliance aus installieren, direkt auf der GravityZone-Appliance oder über das Control Center als eigenständige Appliance. Den Security Server von der Appliance zu installieren, hat folgende Vorteile:

- Für GravityZone-Umgebungen mit einer einzigen Appliance, auf der alle Rollen installiert sind.
- Sie können den Security Server anzeigen und verwenden, ohne GravityZone mit einer Virtualisierungsplattform zu integrieren.
- Weniger erforderliche Installationsvorgänge.

Vorbereitende Maßnahmen:

Auf der GravityZone-Appliance muss die Datenbank-Server-Rolle installiert sein, oder die Appliance muss so konfiguriert sein, dass sie eine Verbindung zu einer bestehenden Datenbank herstellt.

So installieren Sie den Security Server von der Appliance-Oberfläche aus:

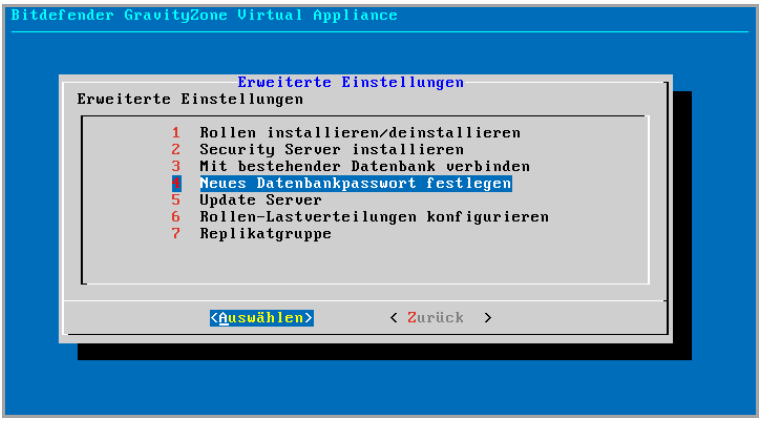
1. Greifen Sie über Ihre Virtualisierungsverwaltungs-Software (z. B. vSphere Client) auf die Appliance-Console zu.
2. Wählen Sie im Hauptmenü den Punkt **Erweiterte Einstellungen**.
3. Wählen Sie **Security Server installieren**. Eine Bestätigungsmeldung wird angezeigt.
4. Drücken Sie `Enter`, um fortzufahren, und warten Sie, bis die Installation abgeschlossen ist.

Beachten Sie
Sie können diesen Security Server nur über das Menü **Erweiterte Einstellungen** der Appliance-Oberfläche deinstallieren.

Neues Datenbankpasswort festlegen

Bei der Installation der Datenbankserver-Rolle müssen Sie zum Schutz der Datenbank ein Passwort einrichten. Falls Sie das Datenbankpasswort ändern

möchten, können Sie über das Hauptmenü unter **Erweiterte Einstellungen > Neues Datenbankkennwort festlegen** eines neues festlegen.



Konsolenoberfläche der Appliance: Option Neues Datenbankkennwort festlegen

Halten Sie sich dabei an die Vorgaben für die Festlegung sicherer Passwörter.

Update-Server konfigurieren

Die GravityZone-Appliance ist standardmäßig so eingerichtet, dass sie Updates aus dem Internet bezieht. Wenn Sie möchten, können Sie Ihre installierten Appliances so konfigurieren, dass sie Updates vom lokalen Bitdefender-Update-Server (der GravityZone-Appliance mit der installierten Update-Server-Rolle) beziehen.

So richten Sie die Update-Server-Adresse ein:

1. Greifen Sie über Ihre Virtualisierungsverwaltungs-Software (z. B. vSphere Client) auf die Appliance-Console zu.
2. Wählen Sie im Hauptmenü den Punkt **Erweiterte Einstellungen**.
3. Wählen Sie **Update-Server**.
4. Wählen Sie **Update-Adresse konfigurieren**.
5. Geben Sie die IP-Adresse oder den Hostnamen der Appliance ein, auf der die Update-Server-Rolle läuft. Der Standard-Update-Server-Port ist `7074`.

Rollen-Lastverteilungen konfigurieren

Um die Zuverlässigkeit und Skalierbarkeit aufrechtzuerhalten, können Sie mehrere Instanzen bestimmter Rollen installieren (Kommunikationsserver, Web-Konsole).

Um Ausfallsicherheit und Skalierbarkeit zu gewährleisten, können Sie mehrere Instanzen bestimmter Rollen installieren (Vorfallserver, Kommunikationsserver, Web-Konsole).

Jede Instanz einer Rolle wird auf einer anderen Appliance installiert.

Alle Instanzen einer bestimmten Rolle müssen über eine Rollen-Lastverteilung mit den anderen Rollen verbunden sein.

Die GravityZone-Appliance verfügt über eingebaute Lastverteilungen, die Sie installieren und verwenden können. Wenn Sie in Ihrem Netzwerk bereits Software oder Hardware zur Lastverteilung haben, können Sie auch diese anstatt der eingebauten Lastverteilungen verwenden.

Eingebaute Rollen-Lastenverteilungen können nicht zusammen mit Rollen auf einer GravityZone-Appliance installiert werden.

1. Greifen Sie über Ihre Virtualisierungsverwaltungs-Software (z. B. vSphere Client) auf die Appliance-Console zu.
2. Wählen Sie im Hauptmenü den Punkt **Erweiterte Einstellungen**.
3. Wählen Sie **Rollen-Lastverteilungen konfigurieren**.
4. Wählen Sie die gewünschte Option:
   - **Externe Lastverteilungen verwenden.** Wählen Sie diese Option, wenn Ihre Netzwerkinfrastruktur bereits Software oder Hardware zur Lastenverteilung besitzt. Sie müssen für jede Rolle, die sie verteilen möchten, die Adresse der Lastenverteilung eingeben. Verwenden Sie die folgende Syntax:

     `http(s)://<IP-Adresse/Hostname>:<Port>`.

   - **Eingebaute Lastverteilungen verwenden.** Wählen Sie diese Option, um die eingebaute Lastenverteilungs-Software zu installieren und zu verwenden.

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

5. Wählen Sie **OK**, um die Änderungen zu speichern.

Replikatgruppe

Mit dieser Option können Sie statt einer Einzel-Server-Datenbankinstanz eine Datenbank-Replikatgruppe aktivieren. Mit diesem Mechanismus können mehrere Datenbankinstanzen in einer geografisch dezentralen GravityZone-Umgebung erstellt werden, womit selbst bei einem Ausfall eine hohe Verfügbarkeit gewährleistet wird.

Wichtig
Datenbankreplikation steht nur in frischen Installationen der GravityZone-Appliance ab der Version 5.1.17-441 zur Verfügung.

Replikatgruppe konfigurieren

Zunächst müssen Sie Replikatgruppe auf der ersten installierten GravityZone-Appliance aktivieren. Dann können Sie Replikate hinzufügen, indem Sie die Datenbankrolle auf den anderen GravityZone-Instanzen in derselben Umgebung installieren.

Wichtig

- Replikatgruppe funktioniert nur mit mindestens drei Mitgliedern.
- Sie können bis zu 7 Instanzen mit der Datenbank Rolle als Replikate hinzufügen (Beschränkung durch MongoDB).
- Es wird empfohlen, eine ungerade Anzahl von Datenbank-Instanzen zu verwenden. Eine gerade Anzahl an Mitgliedern verbraucht für das gleiche Ergebnis mehr Resourcen.

So aktivieren Sie die Datenbankreplizierung in Ihrer GravityZone-Umgebung:

1. Installieren Sie die Datenbank-Server-Rolle auf der ersten GravityZone-Appliance. Weitere Informationen finden Sie unter „Rollen installieren/deinstallieren“ (S. 116).
2. Konfigurieren Sie die anderen Appliances so, dass sie eine Verbindung zur ersten Datenbankinstanz herstellen. Weitere Informationen finden Sie unter „Mit bestehender Datenbank verbinden“ (S. 123).
3. Wählen Sie im Hauptmenü der ersten Appliance **Erweiterte Einstellungen** und anschließend **Replikatgruppe**. Eine Bestätigungsmeldung wird angezeigt.
4. Bestätigen Sie mit einem Klick auf **Ja**.

5. Installieren Sie die Datenbank-Server-Rolle auf allen anderen GravityZone-Appliances.

Sobald Sie alle oben genannten Schritte durchgeführt haben, bilden alle Datenbankinstanzen eine Replikatgruppe:

- Eine primäre Instanz wird gewählt. Diese ist die einzige, die Schreibvorgänge annimmt.
- Die primäre Instanz nimmt sämtliche Änderungen seinem Datensatz in ein Protokoll auf.
- Die sekundären Instanzen replizieren dieses Protokoll und wenden dieselben Änderungen auf ihre Datensätze an.
- Wenn die primäre Instanz einmal nicht verfügbar ist, wird eine der sekundären Instanzen der Replikatgruppe zur primären Instanz.
- Wenn eine Instanz länger als 10 Sekunden nicht mit den anderen Replikaten der Gruppe kommuniziert, versucht die Replikatgruppe eine neue primäre Instanz zu wählen.

Replikate aus einer Gruppe entfernen

Wenn Sie ein Replikat einer Gruppe entfernen möchten, wählen Sie im Menü der Konsolenoberfläche der Appliance einfach **Rollen installieren/deinstallieren > Rollen hinzufügen oder entfernen** und entfernen die Markierung der Option **Datenbankserver**.

Beachten Sie
Sie können Replikate nur dann aus einer Gruppe entfernen, wenn mindestens vier Datenbankinstanzen im Netzwerk installiert sind.

Secure VPN Cluster aktivieren

Die GravityZone-Rollen haben mehrere interne Dienste, die ausschließlich untereinander kommunizieren. Für eine sicherere Umgebung können Sie diese Dienste isolieren, indem Sie einen VPN-Cluster für sie erstellen. Entweder sind diese Dienste auf demselben Appliance oder auf mehreren. Die Kommunikation erfolgt über einen sicheren Kanal.

Wichtig
- Diese Funktion erfordert eine Standardinstallation von GravityZone, auf der keine benutzerdefinierten Tools installiert sind.

- Nach Aktivierung des Clusters können Sie ihn nicht mehr deaktivieren.

So können Sie die internen Dienste auf den Appliances absichern:

1. Greifen Sie über Ihre Virtualisierungsverwaltungs-Software (z. B. vSphere Client) auf die Appliance-Console zu.
2. Wählen Sie im Hauptmenü den Punkt **Erweiterte Einstellungen**.
3. Wählen Sie **Secure VPN Cluster aktivieren**.

   Eine Meldung informiert Sie über die Änderungen, die vorgenommen werden.
4. Klicken Sie auf **Ja**, um die VPN-Installation zu bestätigen und fortzusetzen.

   Nach Abschluss des Vorgangs wird eine Bestätigungsmeldung angezeigt.

Ab sofort sind alle Rollen auf der Appliance im gesicherten Modus installiert und die Dienste kommunizieren über die VPN-Schnittstelle. Jede neue Appliance, die Sie der Umgebung hinzufügen, muss dem VPN-Cluster beitreten. Weitere Informationen finden Sie unter „Mit bestehender Datenbank verbinden (Secure VPN Cluster)“ (S. 124).

Mit bestehender Datenbank verbinden

In verteilten GravityZone-Architekturen müssen Sie zunächst die Datenbankserver-Rolle auf der ersten Appliance installieren. Danach konfigurieren Sie alle weiteren Appliances so, dass sie eine Verbindung mit der bestehenden Datenbankinstanz herstellen. Auf diese Weise nutzen alle Appliances die gleiche Datenbank.

Wichtig
Es wird empfohlen, Secure VPN Cluster zu aktivieren und sich mit einer Datenbank innerhalb dieses Clusters zu verbinden. Weitere Informationen finden Sie unter :

- „Secure VPN Cluster aktivieren“ (S. 122)
- „Mit bestehender Datenbank verbinden (Secure VPN Cluster)“ (S. 124)

So können Sie die Appliance mit einer GravityZone-Datenbank außerhalb eines sicheren VPN-Clusters verbinden:

1. Greifen Sie über Ihre Virtualisierungsverwaltungs-Software (z. B. vSphere Client) auf die Appliance-Console zu.
2. Wählen Sie im Hauptmenü den Punkt **Erweiterte Einstellungen**.

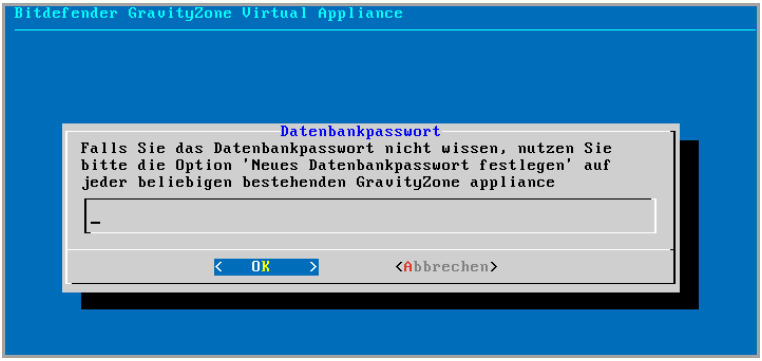
3. Wählen Sie **Mit bestehender Datenbank verbinden**.

> **Beachten Sie**
> Stellen Sie sicher, dass ein Datenbankkennwort festgelegt wurde, bevor Sie auf diese Option zugreifen. Falls Sie das Datenbankkennwort nicht kennen, können Sie im Hauptmenü unter **Erweiterte Einstellungen > Neues Datenbankkennwort festlegen** ein neues Kennwort festlegen.

4. Wählen Sie **Datenbank-Server-Adresse konfigurieren**.
5. Geben Sie die Adresse der Datenbank mit folgender Syntax ein:

   `<IP-Adresse/Hostname>:<Port>`

   Die Angabe des Ports ist optional. Der Standard-Port ist `27017`.
6. Geben Sie das primäre Datenbankkennwort ein.



Konsolenoberfläche der Appliance: Datenbankkennwort eingeben

7. Wählen Sie **OK**, um die Änderungen zu speichern.
8. Wählen Sie **Datenbank-Server-Adresse anzeigen**, um sich zu vergewissern, dass die Adresse korrekt konfiguriert wurde.

Mit bestehender Datenbank verbinden (Secure VPN Cluster)

Verwenden Sie diese Option, wenn Sie Ihre GravityZone-Bereitstellung um weitere Appliances erweitern müssen und Secure VPN Cluster aktiviert ist. Auf diese Weise

nutzt die neue Appliance die gleiche Datenbank wie die bestehende Bereitstellung im sicheren Modus.

Weitere Informationen zum Secure VPN Cluster finden Sie unter „Secure VPN Cluster aktivieren“ (S. 122).

Vorbereitende Maßnahmen

Stellen Sie vor dem Fortfahren sicher, dass Sie Folgendes zur Hand haben:

- IP-Adresse des Datenbankservers
- Passwort für den Benutzer **bdadmin** auf der Appliance mit der Datenbankserverrolle

Verbindung zur Datenbank

So können Sie die Appliance mit einer GravityZone-Datenbank innerhalb eines sicheren VPN-Clusters verbinden:

1. Greifen Sie über Ihre Virtualisierungsverwaltungs-Software (z. B. vSphere Client) auf die Appliance-Console zu.
2. Wählen Sie im Hauptmenü den Punkt **Erweiterte Einstellungen**.
3. Wählen Sie **Mit bestehender Datenbank verbinden (Secure VPN Cluster)**.

   Sie werden über die Anforderungen und mögliche Alternativen informiert, falls die Anforderungen nicht erfüllt werden.
4. Klicken Sie **OK**, um zu bestätigen und fortzufahren.
5. Geben Sie die IP-Adresse des Datenbankservers innerhalb des Secure VPN Cluster ein.
6. Geben Sie das Passwort für den Benutzer **bdadmin** auf der Appliance mit dem Datenbankserver ein.
7. Klicken Sie **OK**, um die Änderungen zu speichern und fortzufahren.

Nach Abschluss des Vorgangs erhalten Sie eine Bestätigungsmeldung. Die neue Appliance wird Mitglied des Clusters und kommuniziert sicher mit den anderen Appliances. Alle Appliances nutzen die gleiche Datenbank.

Status des Secure VPN Cluster überprüfen

Diese Option ist nur verfügbar, wenn Sie den sicheren VPN-Cluster zuvor aktiviert haben. Wählen Sie diese Option, um zu überprüfen, welche Appliances in Ihrer

GravityZone-Bereitstellung ihre Dienste noch nicht gesichert haben. Möglicherweise müssen Sie weiter nachforschen und prüfen, ob die Appliances online sind und auf sie zugegriffen werden kann.

Sprache konfigurieren

So ändern Sie die Sprache der Appliance-Konfigurationsoberfläche:

1. Wählen Sie im Hauptmenü den Punkt **Configure Language**.
2. Wählen Sie dann eine der angezeigten Sprachen. Eine Bestätigungsmeldung wird angezeigt.

   Beachten Sie
   Um die gewünschte Sprache zu finden, müssen Sie evtl. runter scrollen.

3. Wählen Sie **OK**, um die Änderungen zu speichern.

5.2. Lizenzmanagement

Die GravityZone-Sicherheitsdienste werden getrennt lizenziert und verkauft. Jeder GravityZone-Sicherheitsdienst benötigt einen gültigen Basislizenzschlüssel. Zur Verwendung von GravityZone muss mindestens ein gültiger Lizenzschlüssel eingegeben werden.

Über die grundlegenden Sicherheitsdienste hinaus bietet GravityZone weitere starke Sicherheitsfunktionen in der Form von Add-ons. Jedes Add-on hat seinen eigenen Lizenzschlüssel und kann nur in Kombination mit einer gültigen Basislizenz genutzt werden. Wenn die Basislizenz ungültig ist, können Sie die Add-on-Funktionen nur anzeigen, aber nicht nutzen.

Sie können GravityZone testen, um zu entscheiden, ob es für Ihr Unternehmen die richtige Lösung ist. Um Ihren Testzeitraum zu aktivieren, müssen Sie Ihren Testlizenzschlüssel aus der Registrierungs-E-Mail in Control Center eingeben.

Beachten Sie
Control Center wird kostenlos mit jedem GravityZone-Sicherheitsdienst mitgeliefert.

Um einen Sicherheitsdienst nach Ablauf des Testzeitraums weiterhin zu nutzen, müssen Sie einen Lizenzschlüssel erwerben und damit den Dienst registrieren.

Wenn Sie eine Lizenz erwerben möchten, kontaktieren Sie einen Bitdefender-Händler, oder schreiben Sie uns eine E-Mail an enterprisesales@bitdefender.com.

GravityZone-Lizenzschlüssel können auf der Seite **Konfiguration > Lizenz** im Control Center verwaltet werden. Wenn ihr aktueller Lizenzschlüssel bald abläuft, wird in der Konsole eine Nachricht angezeigt, die Sie darauf hinweist. Gehen Sie zur Eingabe eines neuen Lizenzschlüssels oder zum Anzeigen der aktuellen Lizenzinformationen zur Seite **Konfiguration > Lizenz**.

5.2.1. Einen Händler finden

Unsere Händler stellen Ihnen alle benötigten Informationen zur Verfügung und unterstützen Sie bei der Auswahl einer Lizenz-Option, die Ihren Anforderungen gerecht wird.

So finden Sie einen Bitdefender-Wiederverkäufer in Ihrem Land:

1. Gehen Sie zur Partnersuche auf der Bitdefender-Website.
2. Wählen Sie Ihr Land, um Informationen zu Bitdefender-Partnern in Ihrer Nähe anzuzeigen.
3. Falls Sie in Ihrem Land keinen Bitdefender-Händler finden, können Sie uns gerne unter enterprisesales@bitdefender.com kontaktieren.

5.2.2. Ihren Lizenzschlüssel eingeben

Die GravityZone-Lizenz Registrierung kann online oder offline durchgeführt werden. In beiden Fällen müssen Sie einen gültigen Lizenzschlüssel für jeden Sicherheitsdienst, den Sie nutzen möchten, angeben.

Zur Offline-Registrierung benötigen Sie auch den Offline-Registrierungs-Code, der zum Lizenzschlüssel passt.

Sie können mehrere Lizenzschlüssel für denselben Dienst eingeben, aber immer nur der zuletzt eingegebene wird aktiv sein.

Wenn Sie Lizenzen für Ihre GravityZone-Sicherheitsdienste erwerben, bestehende Lizenzschlüssel ändern oder einen separaten Schlüssel für ein Add-on eingeben möchten, gehen Sie wie folgt vor:

1. Melden Sie sich mit einem Unternehmensadministratorkonto an der Control Center an.
2. Gehen Sie zur Seite **Konfiguration > Lizenz**
3. Klicken Sie auf die Schaltfläche ⊕**Hinzufügen** am oberen Ende der Tabelle.
4. Wählen Sie den Registrierungstyp:
   - **Online**. Geben Sie in diesem Fall einen gültigen Lizenzschlüssel in das Feld **Lizenzschlüssel** ein. Der Lizenzschlüssel wird online überprüft.

- **Offline**, wenn keine Internetverbindung besteht. Hierbei müssen Sie den Lizenzschlüssel und den Registrierungscode angeben.

Wenn der Lizenzschlüssel nicht gültig ist, wird eine Fehlermeldung als Quickinfo über dem **Lizenzschlüssel**-Feld angezeigt.

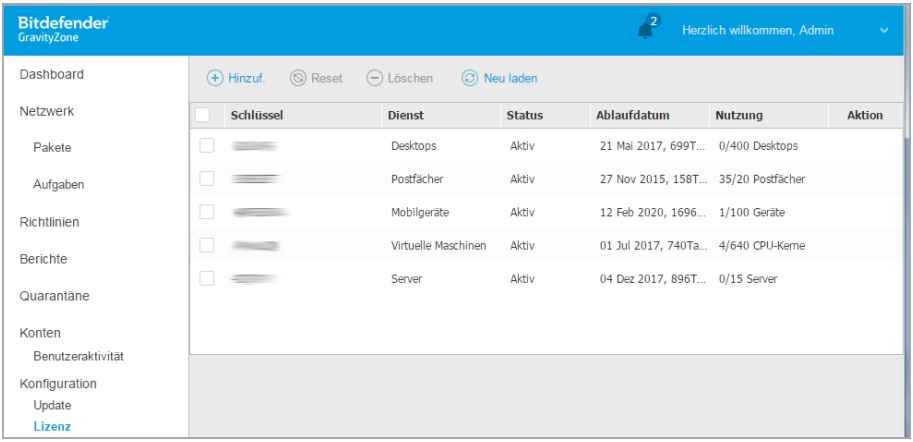
5. Klicken Sie auf **Hinzufügen**. Der Lizenzschlüssel wird auf der Seite **Lizenz** hinzugefügt. Dort werden weitere Details angezeigt.
6. Klicken Sie **Speichern**, um die Änderungen zu speichern. Das Control Center wird neu gestartet, und Sie müssen sich erneut anmelden.

Beachten Sie
Sie können die Add-ons nutzen, solange Sie über eine kompatible Basislizenz verfügen. Andernfalls können Sie die Funktionen nur anzeigen, aber nicht nutzen.

5.2.3. Aktuelle Lizenzinformationen anzeigen

So zeigen Sie ihre Lizenzinformationen an:

1. Melden Sie sich mit einem Unternehmensadministratorkonto an der Control Center an.
2. Gehen Sie zur Seite **Konfiguration > Lizenz**



Die Lizenzübersicht

3. In der Tabelle können Sie Details zu bestehenden Lizenzschlüsseln einsehen.
   - Lizenzschlüssel

- Sicherheitsdienst, zu dem der Lizenzschlüssel gehört
- Status des Lizenzschlüssels

  Wichtig
  Für jeden Dienst kann immer nur ein Lizenzschlüssel gleichzeitig aktiv sein.

- Ablaufdatum und verbleibender Lizenzzeitraum

  Wichtig
  Wenn die Lizenz abläuft, werden die Sicherheitsmodule der installierten Agenten deaktiviert. Endpunkte sind dann nicht mehr geschützt, und Scan-Aufgaben können nicht mehr ausgeführt werden. Danach neu installierte Agenten werden nur einen Testzeitraum lang funktionieren.

- Benutzeranzahl der Lizenz

5.2.4. Benutzeranzahl der Lizenz zurücksetzen

Informationen zur Benutzeranzahl Ihrer Lizenzschlüssel finden Sie auf der Seite **Lizenz** in der Spalte **Nutzung**.

Wenn Sie die Informationen zur Lizenznutzung aktualisieren möchten, können Sie den entsprechenden Lizenzschlüssel markieren und auf die Schaltfläche **Zurücksetzen** am oberen Rand der Tabelle klicken.

5.2.5. Lizenzschlüssel löschen

Auf der Seite **Lizenz** können Sie ungültige oder ausgelaufene Lizenzschlüssel löschen.

Warnung
Wenn Sie einen Lizenzschlüssel löschen, wird der entsprechende Sicherheitsdienst aus dem Control Center entfernt. Sie werden diesen Dienst nicht auf den Endpunkten Ihres Netzwerks installieren oder verwalten können. Die Endpunkte bleiben jedoch geschützt, solange der Lizenzschlüssel noch gültig ist.
Wenn Sie einen neuen gültigen Lizenzschlüssel eingeben, der den zuvor gelöschten Dienst abdeckt, werden alle Funktionen dieses Diensts im Control Center wieder aktiviert.

So löschen Sie einen Lizenzschlüssel:

1. Melden Sie sich mit einem Unternehmensadministratorkonto an der Control Center an.

2. Gehen Sie zur Seite **Konfiguration > Lizenz**
3. Wählen Sie den Lizenzschlüssel, den Sie entfernen möchten, und klicken Sie auf die Schaltfläche ⊖ **Löschen** am oberen Rand der Tabelle.

5.3. Schutz für Endpunkte installieren

Je nach Konfiguration der Maschine und der Netzwerksumgebung können Sie entweder nur die Sicherheitsagenten installieren oder zusätzlich einen Security Server verwenden. Im letzeren Fall müssen Sie zuerst den Security Server installieren und dann erst die Sicherheitsagenten.

Es wird empfohlen, in virtualisierten Umgebungen, so z. B. in Nutanix, VMware oder Citrix Xen oder bei Maschinen mit geringen Hardware-Resourcen, den Security Server zu verwenden.

Wichtig
Nur Bitdefender Endpoint Security Tools und Bitdefender Tools unterstützen die Verbindungen zum Security Server. Weitere Informationen finden Sie unter „GravityZone-Architektur“ (S. 11).

5.3.1. Security Server installieren

Security Server ist eine virtuelle Maschine, die eigens für die Deduplizierung und Zentralisierung eines Großteils der Malware-Schutzfunktionen der Malware-Schutz-Clients da ist und als Scan-Server fungiert.

Die Security Server-Bereitstellung ist von der Art der installierten Umgebung abhängig. Die Installationsvorgänge werden hier beschrieben:

- Security Server für VMware NSX
- Security Server Multi-Platform oder für VMware vShield
- Security Server für Amazon EC2
- Security Server for Microsoft Azure

Installation von Security Server for VMware NSX

In VMware-NSX-Umgebungen müssen Sie den Bitdefender-Dienst in jedem zu schützenden Cluster installieren. Die spezielle Appliance wird automatisch auf allen Hosts im Cluster bereitgestellt. Alle virtuellen Maschinen auf einem Host werden automatisch über die Guest Introspection mit der auf diesem Host installierten Security Server-Instanz verbunden.

Die Security Server-Bereitstellung hat ausschließlich über den vSphere Web Client zu erfolgen.

So können Sie den Bitdefender-Dienst installieren:

1. Melden Sie sich beim vSphere Web Client an.
2. Öffnen Sie **Netzwerk & Sicherheit > Installation** und wechseln Sie zum Reiter **Dienstbereitstellungen**.
3. Klicken Sie auf die Schaltfläche für eine **Neue Dienstbereitstellung** (das Pluszeichen-Symbol). Das Konfigurationsfenster wird angezeigt.
4. Wählen Sie **Guest Introspection** und klicken Sie auf **Weiter**.
5. Wählen Sie das Rechenzentrum und die Cluster aus, auf denen der Dienst bereitgestellt werden soll und klicken Sie auf **Weiter**.
6. Wählen Sie den Speicher und das Verwaltungsnetzwerk aus, klicken Sie auf **Weiter** und danach auf **Fertig stellen**.
7. Wiederholen Sie Schritt 3 bis 6, aber wählen Sie dieses Mal **Bitdefender**-Dienst aus.

   Bevor Sie mit der Installation fortfahren, müssen Sie sicherstellen, dass eine Netzwerkverbindung zwischen dem ausgewählten Netzwerk und der GravityZone Control Center besteht.

   Nach Installation des Bitdefender-Dienstes stellt dieser automatisch den Security Server auf allen ESXi-Hosts in dem ausgewählten Clustern bereit.

Warnung
Damit die Dienste ordnungsgemäß funktionieren können, ist es äußerst wichtig, dass Sie zunächst die Guest Introspection und danach Bitdefender installieren und nicht beide gleichzeitig.

Beachten Sie
Weitere Informationen zum Hinzufügen von Partnerdiensten zu NSX finden Sie im VMware NSX Documentation Center.
Wenn Sie für Speicher und Netzwerkverwaltung **Auf Host angegeben** auswählen, müssen Sie sicherstellen, dass Agent VM auf den Hosts sowohl für die Guest Introspection als auch für die Bitdefender-Dienste eingerichtet wurde.

Die spezifischen Anforderungen für Security Server richten sich nach der Anzahl der virtuellen Maschinen, die geschützt werden sollen. So können Sie die Standardkonfiguration der Security Server-Hardware anpassen:

1. Melden Sie sich beim VMware vSphere Web Client an.
2. Rufen Sie **Host und Cluster** auf.
3. Wählen Sie den Cluster aus, in dem Security Server bereitgestellt wurde, und wechseln Sie danach zum Reiter **Verwandte Objekte > Virtuelle Maschinen**.
4. Schalten Sie die **Bitdefender**-Appliance aus.
5. Klicken Sie mit der rechten Maustaste auf den Namen der Appliance und wählen Sie im Kontextmenü **Einstellungen bearbeiten...** aus.
6. Passen Sie im Reiter **Virtuelle Hardware** die Werte für CPU und RAM entsprechend Ihren Erfordernissen an und klicken Sie auf **OK**, um die Änderungen zu speichern.
7. Schalten Sie die Appliance wieder an.

Beachten Sie
Eine Anleitung zum Upgrade von VMware vShield auf NSX finden Sie in diesem Artikel in der Wissensdatenbank.

Installation von Security Server Multi-Platform oder for VMware vShield

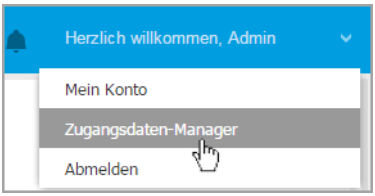
1. Mit der Virtualisierungsplattform verbinden
2. Security Server auf Hosts installieren

Mit der Virtualisierungsplattform verbinden

Um auf die mit dem Control Center integrierte virtuelle Infrastruktur zugreifen zu können, müssen Sie Ihre Benutzerzugangsdaten für jedes verfügbare virtualisierte Server-System angeben. Control Center stellt mithilfe Ihrer Zugangsdaten eine Verbindung zur virtualisierten Infrastruktur her und zeigt nur diejenigen Ressourcen an, auf die Sie Zugriff haben (wie in vCenter Server definiert).

So geben Sie die Zugangsdaten an, die zur Verbindung mit den Virtualisierungs-Server-Systemen nötig sind:

1. Klicken Sie auf Ihren Benutzernamen in der rechten oberen Ecke der Seite, und wählen Sie **Zugangsdaten-Manager**.



Das Netzwerk- und Pakete-Menü

2. Gehen Sie zum Reiter **Virtuelle Umgebung**.
3. Geben Sie die nötigen Authentifizierungszugangsdaten an.
   a. Wählen Sie einen Server aus dem entsprechenden Menü.

      Beachten Sie
      Wenn das Menü nicht verfügbar ist, wurde entweder noch keine Integration konfiguriert oder alle nötigen Zugangsdaten wurden bereits konfiguriert.

   b. Geben Sie Ihren Benutzernamen und Ihr Passwort und eine aussagekräftige Beschreibung ein.
   c. Klicken Sie auf den Button ⊕**Hinzufügen**. Die neuen Zugangsdaten werden in der Tabelle angezeigt.

Beachten Sie
Wenn Sie Ihre Zugangsdaten zur Authentifizierung nicht angegeben haben, müssen Sie sie angeben, sobald Sie das Inventar irgendeines vCenter-Server-Systems durchsuchen. Wenn Sie Ihre Zugangsdaten einmal eingegeben haben, werden sie im Zugangsdaten-Manager gespeichert, sodass Sie sie beim nächsten Mal nicht mehr eingeben müssen.

Security Server auf Hosts installieren

So installieren Sie Security Server auf Hosts:

- In VMware-Umgebungen mit vShield Endpoint müssen Sie diese spezielle Appliance auf jedem Host installieren. Alle virtuellen Maschinen auf einem Host werden automatisch über vShield Endpoint mit der Instanz von Security Server, die auf diesem Host installiert ist, verbunden.
- In Citrix-Umgebungen müssen Sie den Security Server über Remote-Installation auf jedem Host installieren, der durch HVI geschützt werden soll.

- In Nutanix Prism Element-Umgebungen muss der Sicherheitsserver auf jedem Host mit einer per Fernzugriff durchgeführten Installationsaufgabe installiert werden.
- In allen anderen Umgebungen müssen Sie Security Server auf einem oder mehreren Hosts installieren, um die entsprechende Anzahl an virtuellen Maschinen zu schützen. Dazu müssen Sie die Anzahl der geschützten virtuellen Maschinen sowie die für Security Server auf den Hosts zur Verfügung stehenden Ressourcen und die Netzwerkverbindung zwischen Security Server und den geschützten virtuellen Maschinen bedenken. Auf virtuellen Maschinen installierte Sicherheitsagenten stellen über TCP/IP eine Verbindung zum Security Server her. Dazu verwenden sie die Informationen, die bei der Installation oder über eine Richtlinie vorgegeben werden.

Wenn Control Center mit vCenter Server, XenServer oder Nutanix Prism Element integriert ist, können Sie den Security Server automatisch vom Control Center aus auf Hosts installieren. Security Server-Pakete zur Einzelinstallation können Sie auch vom Control Center herunterladen.

Beachten Sie
In VMware-Umgebungen mit vShield Endpoint können Sie Security Server nur über Installationsaufgaben auf Hosts installieren.

Lokale Installation

In allen virtualisierten Umgebungen, die nicht mit Control Center integriert sind, müssen Sie Security Server manuell mithilfe eines Installationspakets auf Hosts installieren. Das Security Server-Paket kann vom Control Center in mehreren verschiedenen Formaten heruntergeladen werden, die mit den gängigsten Virtualisierungsplattformen kompatibel sind.

Download der Installationspakete für Security Server

So laden Sie Installationspakete für Security Server herunter:

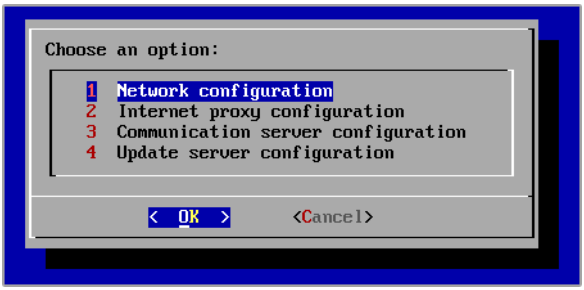
1. Gehen Sie zur Seite **Netzwerk > Pakete**.
2. Wählen Sie das Security Server-Standardpaket.
3. Klicken Sie auf die Schaltfläche **Herunterladen** am oberen Rand der Tabelle und wählen Sie den Pakettyp aus dem Menü.
4. Speichern Sie das gewählte Paket am gewünschten Speicherort.

Einsatz von Security Server Installationspaketen

Sobald sie das Installationspaket haben, können Sie es auf dem Host mithilfe eines beliebigen Installationstools für virtuelle Maschinen installieren.

Richten Sie nach der Installation den Security Server wie folgt ein:

1. Greifen Sie über Ihre Virtualisierungsverwaltungs-Software (z. B. vSphere Client) auf die Appliance-Console zu. Alternativ können Sie auch über SSH eine Verbindung zur Appliance herstellen.
2. Melden Sie sich mit den Standardzugangsdaten an.
   - Benutzername: `root`
   - Passwort: `sve`
3. Führen Sie den Befehl `sva-setup` aus. Die Konfigurationsoberfläche der Appliance wird geöffnet.



Security Server-Konfigurationsoberfläche (Hauptmenü)

Verwenden Sie zur Navigation durch die Menüs und Optionen die `Tabulator`- und Pfeiltasten. Um eine bestimmte Option auszuwählen, drücken Sie `Enter`.

4. Konfigurieren Sie die Netzwerkeinstellungen.

   Der Security Server kommuniziert mit den anderen GravityZone-Komponenten über das TCP/IP-Protokoll. Sie können die Appliance so einrichten, dass sie die Netzwerkeinstellungen automatisch vom DHCP-Server bezieht, oder Sie können sie manuell konfigurieren. Gehen Sie dazu wie folgt vor:

   a. Wählen Sie im Hauptmenü den Punkt **Netzwerkkonfiguration**.

   b. Wählen Sie den Netzwerkadapter aus.

c. Wählen Sie den IP-Adressen-Konfigurationsmodus:

- **DHCP**, wenn Sie möchten, dass der Security Server die Netzwerkeinstellungen automatisch vom DHCP-Server bezieht.
- **Statisch**, wenn kein DHCP-Server vorhanden ist oder wenn im DHCP-Server eine IP-Adresse für die Appliance reserviert wurde. In diesem Fall müssen Sie die Netzwerkeinstellungen manuell konfigurieren.

  i. Geben Sie Hostnamen, IP-Adresse, Netzwerkmaske, Gateway und DNS-Server in die entsprechenden Felder ein.

  ii. Wählen Sie **OK**, um die Änderungen zu speichern.

Beachten Sie
Wenn Sie über einen SSH-Client mit der Appliance verbunden sind, wird Ihre Sitzung sofort beendet, wenn Sie die Netzwerkeinstellungen ändern.

5. Konfigurieren Sie die Proxy-Einstellungen.

   Wenn im Netzwerk ein Proxy-Server verwendet wird, müssen Sie seine Details eingeben, damit der Security Server mit dem GravityZone Control Center kommunizieren kann.

   Beachten Sie
   Nur Proxy-Server mit Basic Authentication werden unterstützt.

   a. Wählen Sie im Hauptmenü den Punkt **Internet proxy configuration**.

   b. Geben Sie Hostnamen, Benutzernamen, Passwort und Domaine in die entsprechenden Felder ein.

   c. Wählen Sie **OK**, um die Änderungen zu speichern.

6. Konfigurieren Sie die Adresse des Kommunikationsservers.

   a. Wählen Sie im Hauptmenü den Punkt **Communication server configuration**.

   b. Geben Sie die Adresse des Kommunikationsservers einschließlich der Portnummer 8443 im folgenden Format ein:

   ```
   https://Kommunikationsserver-IP-Adresse:8443
   ```

   Statt der IP-Adresse des Kommunikationsservers können Sie auch den entsprechenden Hostnamen verwenden.

   c. Wählen Sie **OK**, um die Änderungen zu speichern.

Remote-Installation

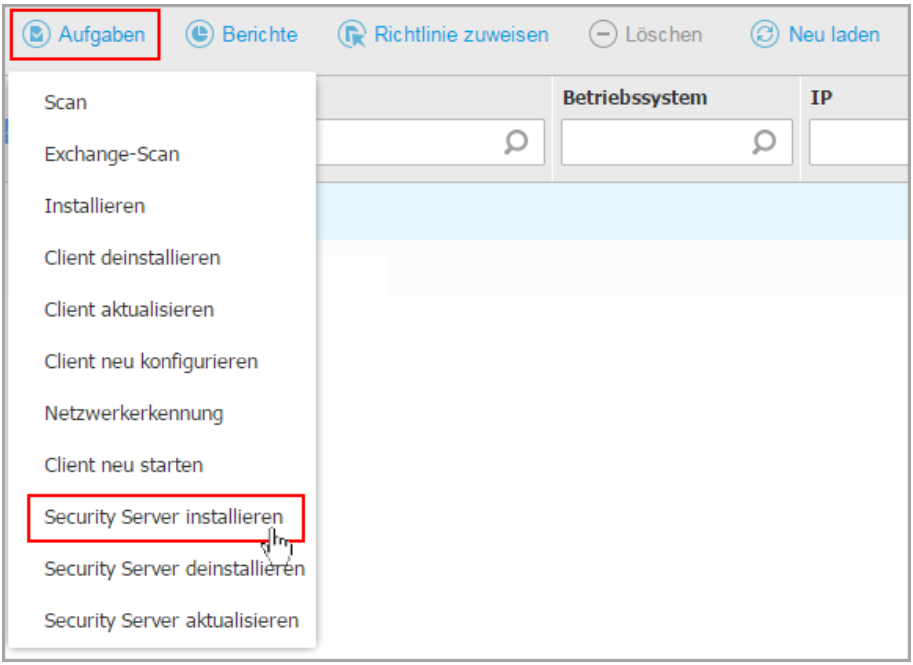
Mit Control Center können Sie über Installationsaufgaben Security Server aus der Ferne auf sichtbaren Hosts installieren.

So installieren Sie Security Server aus der Ferne auf einem oder mehreren Hosts:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Virtuelle Maschinen** aus der Ansichtsauswahl.
3. Durchsuchen Sie das VMware-, Citrix- oder Nutanix-Inventar und markieren Sie die Kästchen der gewünschten Hosts oder Container (Nutanix Prism, vCenter Server, XenServer oder Rechenzentrum). Um Zeit zu sparen, können Sie auch direkt den Root-Container auswählen wählen (Nutanix-Inventar, VMware-Inventar oder Citrix-Inventar). Im Installationsassistenten können Sie Hosts einzeln auswählen.

   Beachten Sie
   Sie können nicht Hosts von verschiedenen Ordnern gleichzeitig auswählen.

4. Klicken Sie auf die Schaltfläche **Aufgaben** am oberen Rand der Tabelle und wählen Sie **Security Server installieren** aus dem Menü. Das Fenster **Security Server-Installation** wird angezeigt.



Installieren von Security Server über das Aufgabenmenü

5. Wählen Sie den Host, auf dem Sie die Security Server-Instanzen installieren möchten.
6. Wählen Sie die gewünschten Konfigurationseinstellungen.

   Wichtig
   Wenn Sie bei der gleichzeitigen Installation mehrerer Instanzen von Security Server gemeinsame Einstellungen verwenden möchten, müssen die Hosts denselben Speicher benutzen, per DHCP-Server zugewiesene IP-Adressen haben und Teil desselben Netzwerks sein.

   Wenn Sie jeden Security Server anders konfigurieren möchten, können Sie im nächsten Schritt des Assistenten die gewünschten Einstellungen für jeden Host einzeln vornehmen. Die folgend genannten Schritte gelten, wenn die Option **Jeden Security Server einzeln konfigurieren** verwendet wird.
7. Klicken Sie auf **Weiter**.

8. Geben Sie einen aussagekräftigen Namen für den Security Server ein.
9. Wählen Sie in VMware-Umgebugen aus dem Menü **Container installieren** den Container, in dem Sie den Security Server installieren möchten.
10. Wählen Sie den Ziel-Speicherort.
11. Wählen Sie die Art der Speicherzuweisung. Für die Installation der Appliance wird die klassische Speicherzuweisung empfohlen.

    Wichtig
    Wenn bei Verwendung der schlanken Speicherzuweisung der Speicherplatz knapp wird, hängt sich die Security Server auf, wodurch der Host nicht mehr geschützt ist.

12. Konfigurieren Sie die Speicher- und CPU-Ressourcenzuteilung je nach VM-Konsolidierungsrate auf dem Host. Wählen Sie **Gering**, **Mittel** oder **Hoch**, um die empfohlenen Einstellungen für die Ressourcenzuteilung zu laden, oder **Manuell**, um die Ressourcenzuteilung manuell zu konfigurieren.
13. Vergeben Sie ein Administrator-Password für die Security Server -Konsole. Wenn Sie ein Administratorpasswort festlegen, setzt dieses das Standard-Root-Passwort ("sve") außer Kraft.
14. Legen Sie die Zeitzone der Appliance fest.
15. Wählen Sie die Netzwerkkonfigurationsart für das Bitdefender-Netzwerk. Die IP-Adresse des Security Server darf im Laufe der Zeit nicht geändert werden, da sie von Linux-Agenten zur Kommunikation verwendet wird.

    Wenn Sie DHCP wählen, konfigurieren Sie den DHCP-Server so, dass er eine IP-Adresse für die Appliance reserviert.

    Wenn Sie die Option "statisch" wählen, müssen Sie IP-Adresse, Subnetz-Maske, Gateway und DNS eingeben.
16. Wählen Sie das vShield-Netzwerk und geben Sie die vShield-Zugangsdaten ein. Die Standardbezeichnung für das vShield-Netzwerk `vmservice-vshield-pg`.
17. Klicken Sie auf **Speichern**.

Auf der Seite **Netzwerk > Aufgaben** können Sie Aufgaben anzeigen und verwalten.

Beachten Sie
Eine Anleitung zum Upgrade von VMware vShield auf NSX finden Sie in diesem Artikel in der Wissensdatenbank.

Wichtig
In Nutanix-Umgebungen kann die Installation des Security Servers per Fernzugriff aus verschiedenen Gründen fehlschlagen, so z. B. wenn der Prism Element-Cluster in Prism Central registriert ist. In solchen Fällen empfiehlt es sich, die Installation des Security Servers manuell durchzuführen. Weitere Einzelheiten finden Sie in diesem Artikel in der Wissensdatenbank.

Installieren von Security Server für Amazon EC2

Sie können Security Server wie folgt zum Schutz Ihrer Amazon-EC2-Instanzen einsetzen:

- Konfigurieren Sie den in Ihrem lokalen Netzwerk installierten Security Server zur Kommunikation mit den Amazon-EC2-Instanzen. So können Sie Ihre lokalen Ressourcen, sowie physisch und virtuell, auch zum Schutz des Amazon-EC2-Inventars einsetzen.
- Installieren Sie abhängig von Ihren Anforderungen einen oder mehrere Security Server-Instanzen in Ihrer Amazon-EC2-Umgebung. Befolgen Sie in diesem Fall die Anleitung in diesem Artikel in der Wissensdatenbank.

  Wichtig
  - Damit die Kommunikation zwischen Ihren EC2-Maschinen und den in Ihrem Amazon-EC2-Inventar installierten Sicherheitsserver-Instanzen funktioniert, müssen Sie Ihre Amazon-VPC- (Virtual Private Cloud) und Amazon-VPN-Verbindungen ordnungsgemäß konfigurieren. Weitere Informationen finden Sie in der Amazon-VPC-Dokumentation.
  - Wir empfehlen, den Security Server in der gleichen Amazon-EC2-Region zu installieren, in der auch die zu schützenden Instanzen laufen.

Der Standard-Scan-Modus für EC2-Instanzen ist Lokaler Scan (Sicherheitsinhalte werden im installierten Sicherheitsagenten gespeichert, und der Scan wird lokal auf der Maschine ausgeführt). Wenn Sie Ihre EC2-Instanzen mit einem Security Server scannen möchten, müssen Sie das Installationspaket des Sicherheitsagenten und die angewandte Richtlinie entsprechend konfigurieren.

Security Server for Microsoft Azure installieren

Mit Security Server können Sie Ihre virtuellen Maschinen in Microsoft Azure wie folgt schützen:

- Konfigurieren Sie den in Ihrem lokalen Netzwerk installierten Security Server so, dass der mit den virtuellen Maschinen in Microsoft Azure kommuniziert. So können Sie Ihre lokalen Ressourcen, physische und virtuelle, auch zum Schutz des Microsoft-Azure-Inventars nutzen.
- Installieren Sie abhängig von Ihren Anforderungen einen oder mehrere Security Server-Instanzen in Ihrer Microsoft-Azure-Umgebung. Befolgen Sie in diesem Fall die Anleitung in diesem Artikel in der Wissensdatenbank.

Wichtig

- Damit die Kommunikation zwischen Ihren virtuellen Maschinen in Microsoft Azure und den in Ihrem Microsoft-Azure-Inventar installierten Security-Server-Instanzen reibungslos funktioniert, muss Ihr virtuelles Netzwerk/Subnetz ordnungsgemäß konfiguriert sein. Weitere Details entnehmen Sie bitte der Dokumentation Virtuellen Netzwerk mit Microsoft Azure.
- Wir empfehlen, den Security Server in derselben Microsoft-Azure-Region zu installieren, in der auch die zu schützenden virtuellen Maschinen laufen.

Der Standard-Scan-Modus für virtuelle Microsoft-Azure-Maschinen ist Lokaler Scan (Sicherheitsinhalte werden im installierten Sicherheitsagenten gespeichert, und der Scan wird lokal auf der Maschine ausgeführt). Wenn Sie Ihre virtuellen Microsoft-Azure-Maschinen mit einem Security Server scannen möchten, müssen Sie das Installationspaket des Sicherheitsagenten und die angewandte Richtlinie entsprechend konfigurieren.

5.3.2. Sicherheitsagent installieren

Um Ihre physischen und virtuellen Endpunkte zu schützen, müssen Sie auf jedem von ihnen einen Sicherheitsagenten installieren. Der Sicherheitsagent verwaltet den Schutz des lokalen Endpunkts. Zudem kommuniziert er mit dem Control Center, um Befehle des Administrators entgegenzunehmen und die Ergebnisse seiner Aktionen zu übermitteln.

Weitere Informationen zu verfügbaren Sicherheitsagenten finden Sie unter „Sicherheitsagenten“ (S. 13).

Auf Windows- und Linux-Maschinen kann der Sicherheitsagent zwei Rollen haben, und Sie können ihn wie folgt installieren:

1. Als einfachen Sicherheitsagenten für Ihre Endpunkte.
2. Als Relais, und somit als Sicherheitsagent und Kommunikations-, Proxy- und Update-Server für andere Endpunkte im Netzwerk.

Sie können den Sicherheitsagenten auf physischen und virtuellen Endpunkten installieren, indem Sie Installationspakete lokal ausführen oder über Control Center Installationsaufgaben aus der Ferne ausführen.

Es ist wichtig, dass Sie die Anleitung sorgfältig lesen und befolgen, um die Installation richtig vorzubereiten.

Im Normalmodus haben die Sicherheitsagenten eine minimale Benutzeroberfläche. Über sie können Anwender den Sicherheitsstatus einsehen und grundlegende Sicherheitsaufgaben (Updates und Scans) ausführen, haben jedoch keinen Zugriff auf die Einstellungen.

Wenn der Netzwerkadministrator es per Installationspaket und Sicherheitsrichtlinie aktiviert hat, kann der Sicherheitsagent auf Windows-Endpunkten auch im Power-User-Modus ausgeführt werden. In diesem Modus kann der Endpunktbenutzer Sicherheitseinstellungen anzeigen und verändern. Der Control Center-Administrator kann jedoch in jedem Fall festlegen, welche Richtlinieneinstellungen angewendet werden und gegebenenfalls Einstellungen des Power-Users außer Kraft setzen.

Die Sprache der Benutzeroberfläche auf geschützten Windows-Endpunkten wird bei der Installation standardmäßig entsprechend der für Ihr GravityZone-Konto eingestellten Sprache festgelegt.

Auf Macs wird die Anzeigesprache der Benutzeroberfläche bei der Installation auf die Sprache festgelegt, auf die das Endpunktbetriebssystem eingestellt ist. Für Linux steht der Sicherheitsagent nicht in unterschiedlichen Sprachversionen zur Verfügung.

Um die Benutzeroberfläche auf bestimmten Windows-Endpunkten in einer anderen Sprache zu installieren, können Sie ein Installationspaket erstellen und die bevorzugte Sprache in den Konfigurationsoptionen dieses Pakets festlegen. Für Mac- und Linux-Endpunkte steht diese Option nicht zur Verfügung. Weitere Informationen zur Erstellung von Installationspaketen finden Sie unter „Installationspakete erstellen“ (S. 146).

Vor der Installation

Bevor Sie mit der Installation beginnen, sollten Sie die folgenden Hinweise beachten, um einen reibungslosen Ablauf zu garantieren:

1. Stellen Sie sicher, dass die Endpunkte die Mindestsystemanforderungen erfüllen. Bei manchen Endpunkte kann es notwendig werden, das neueste Service Pack für das Betriebssystem zu installieren oder Speicherplatz zu schaffen. Legen Sie eine Liste der Endpunkte an, die die notwendigen Anforderungen nicht erfüllen, damit Sie diese von der Verwaltung ausschließen können.
2. Entfernen Sie alle bereits installierten Malware-Schutz- oder Internet-Sicherheits-Lösungen von den Endpunkten (eine Deaktivierung ist nicht ausreichend). Wenn der Sicherheitsagent gleichzeitig mit anderen Sicherheitslösungen auf einem Endpunkt betrieben wird, kann dies deren Funktion stören und massive Probleme auf dem System verursachen.

   Viele inkompatible Sicherheitsprogramme werden automatisch gefunden und bei der Installation des Sicherheitsagenten entfernt.

   Mehr zu diesem Thema und eine Liste von Sicherheitssoftware-Produkten, die Bitdefender Endpoint Security Tools auf aktuellen Windows-Betriebssystemen erkennt, finden Sie in diesem Artikel.

   Wichtig
   Falls Sie den Sicherheitsagenten auf einem Computer mit Bitdefender Antivirus for Mac 5.X installieren möchten, müssen Sie letzteren zunächst deinstallieren. Sie finden eine Anleitung in diesem Artikel in der Wissensdatenbank.

3. Für die Installation benötigen Sie Administratorrechte und Zugriff auf das Internet. Wenn sich die entsprechenden Endpunkte in einer Active-Directory-Domain befinden, müssen Sie zur Ferninstallation über Domainadministrator-Zugangsdaten verfügen. Befinden Sie sich nicht in einer Active-Directory-Domain, müssen Sie die Zugangsdaten für jeden einzelnen Endpunkt zur Hand haben.
4. Die Endpunkte müssen eine funktionierende Netzwerkverbindung zur GravityZone-Appliance haben.
5. Für den Relais-Server wird die Nutzung einer statischen IP-Adresse empfohlen. Verwenden Sie den Host-Namen des Computers, falls Sie keine statische IP festlegen.
6. Wenn Sie den Agenten über ein Linux-Relais installieren, müssen zusätzlich die folgenden Voraussetzungen erfüllt sein:

- Auf dem Relais-Endpunkt muss das Samba-Paket (`smbclient`)mindestens in der Version 4.1.0 sowie der `net`-Binary/Befehl installiert sein, um Windows-Agenten installieren zu können.

  Beachten Sie
  Der `net`-Binary/Befehl wird üblicherweise mit den Paketen samba-client und / oder samba-common ausgeliefert. Bei einigen Linux-Distributionen (z. B. CentOS 7.4) wird der `net`-Befehl nur bei der Installation der kompletten Samba-Suite (Common + Client + Server) installiert. Stellen Sie sicher, dass auf Ihrem Relais-Endpunkt der `net`-Befehl verfügbar ist.

- Auf den gewünschten Windows-Endpunkten müssen Administratorfreigabe und Netzwerkfreigabe aktiviert sein.
- Für beteiligte Linux- und Mac-Endpunkte muss SSH aktiviert sein.

7. Nach der Installation von Endpoint Security for Mac (manuell oder aus der Ferne) unter macOS High Sierra (10.13) und neueren Betriebssystemversionen werden Benutzer aufgefordert, Bitdefender-Kernelerweiterungen auf ihren Computern zu genehmigen. Solange die Benutzer die Bitdefender-Kernelerweiterung noch nicht genehmigt haben, funktionieren einige Funktionen von Endpoint Security for Mac nicht. Um den Benutzern Aufwand zu ersparen, können die Bitdefender-Kernelerweiterungen auch im Voraus genehmigt werden, indem sie mithilfe eines Mobilgerät-Verwaltungstools auf die Whitelist gesetzt werden.
8. Wenn Sie den Agenten in einem Amazon-EC2-Inventar einsetzen, konfigurieren Sie die Sicherheitsgruppen, die den zu schützenden Instanzen zugeordnet sind im Amazon EC2 **Dashboard > Network & Security** wie folgt:

   - Erlauben Sie für die Remote-Installation den SSH*-Zugriff über die EC2-Instanz.
   - Gestatten Sie für die lokale Installation den SSH*- und RDP-Zugriff (Remote Desktop Protocol) über den Computer, über den Sie die Verbindung herstellen.

   * Sie müssen für die Remote-Installation auf Linux-Instanzen SSH-Anmeldung mit Benutzername und Passwort erlauben.
9. Achten Sie bei der Installation des Agenten in einem Microsoft-Azure-Inventar auf die folgenden Punkte:

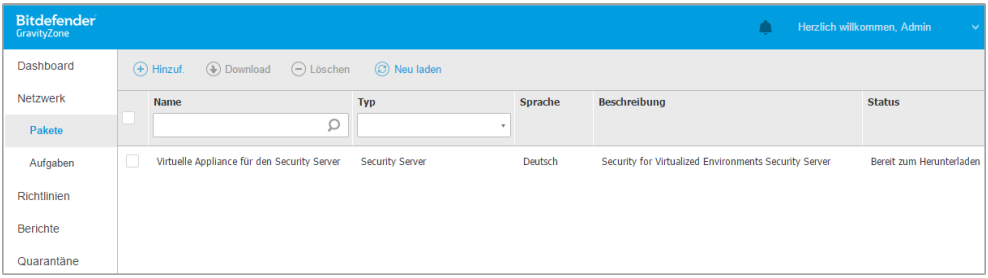
   - Die gewünschte virtuelle Maschine muss sich im selben virtuellen Netzwerk wie die GravityZone-Appliance befinden.

- Wenn sich die GravityZone-Appliance in einem anderen Netzwerk befindet, muss sich die gewünschte virtuelle Maschine im selben virtuellen Netzwerk wie ein Relais befinden, das mit der GravityZone-Appliance kommuniziert.

Lokale Installation

Eine Möglichkeit, den Sicherheitsagenten auf einem Endpunkt zu installieren ist es, ein Installationspaket lokal auszuführen.

Sie können die Installationspakete auf der Seite **Netzwerk > Pakete** erstellen und verwalten.



Die Paketübersicht

Nach der Installation des ersten Clients wird dieser dazu verwendet, um andere Endpunkte über den Netzwerkerkennungsmechanismus im gleichen Netzwerk zu finden. Weitere Informationen zur Netzwerkerkennung finden Sie unter „Wie die Netzwerkerkennung funktioniert“ (S. 164).

Gehen Sie zur lokalen Installation des Sicherheitsagenten auf einem Computer folgendermaßen vor:

1. Sie können ein Installationspaket erstellen, das Ihren Anforderungen entspricht.

   Beachten Sie
   Dieser Schritt muss nicht durchgeführt werden, falls unter Ihrem Benutzerkonto bereits ein Installationspaket für das Netzwerk erstellt worden ist.

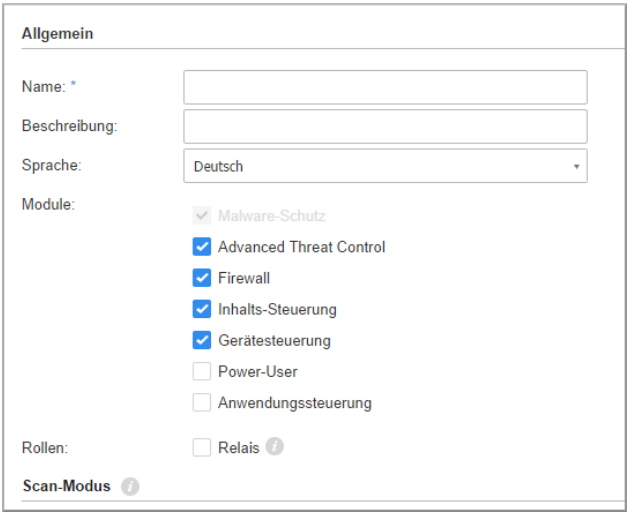
2. Auf diesem Endpunkt müssen Sie zunächst das Installationspaket herunterladen.

   Alternativ können Sie an mehrere Benutzer in Ihrem Netzwerk Download-Links zu den Installationspaketen per E-Mail senden.
3. Im nächsten Schritt Führen Sie das Installationspaket aus.

Installationspakete erstellen

So erstellen Sie ein Installationspaket:

1. Stellen Sie eine Verbindung zur Control Center her und melden Sie sich an.
2. Gehen Sie zur Seite **Netzwerk > Pakete**.
3. Klicken Sie auf die Schaltfläche ⊕**Hinzufügen** am oberen Ende der Tabelle. Ein Konfigurationsfenster wird sich öffnen.



Pakete erstellen - Optionen

4. Geben Sie einen aussagekräftigen Namen und eine Beschreibung für das zu erstellende Installationspaket ein.
5. Wählen Sie aus dem Feld **Sprache** die gewünschte Sprache für die Client-Oberfläche.

   Beachten Sie
   Diese Option steht nur für Windows-Systeme zur Verfügung.

6. Wählen Sie die Schutzmodule aus, die Sie installieren möchten.

Beachten Sie
Es werden nur die Module installiert, die vom jeweiligen Betriebssystem unterstützt werden. Weitere Informationen finden Sie unter „Sicherheitsagenten“ (S. 13).

7. Wählen Sie die Rolle des gewünschten Endpunkts:
   - **Relais**, um das Paket für einen Endpunkt mit der Relais-Rolle zu erstellen. Weitere Informationen finden Sie unter „Relais“ (S. 15)
   - **Patch-Management-Cache-Server**, um das Relais zu einem internen Server für die Verteilung von Software-Patches zu machen. Diese Rolle wird angezeigt, wenn die Relais-Rolle ausgewählt wird. Weitere Informationen finden Sie unter „Patch-Cache-Server“ (S. 16)
   - **Exchange-Schutz**, um die Sicherheitsmodule für Microsoft-Exchange-Server zu installieren (Malware-Schutz, Spam-Schutz, Inhalts- und Anhangsfilter für den Exchange-E-Mail-Verkehr sowie Bedarf-Malware-Scans in Exchange-Datenbanken). Weitere Informationen finden Sie unter „Schutz für Exchange installieren“ (S. 176).
8. **Konkurrenzprodukte entfernen**. Es wird empfohlen, dieses Kästchen aktiviert zu lassen, um inkompatible Sicherheitssoftware automatisch zu entfernen, während der Bitdefender-Agent auf dem Endpunkt installiert wird. Wenn Sie diese Option deaktivieren, wird der Bitdefender-Agent zusätzlich zur bestehenden Sicherheitslösung installiert. Sie können die bereits installierte Sicherheitslösung zu einem späteren Zeitpunkt auf eigene Gefahr manuell entfernen.

   Wichtig
   Wenn der Bitdefender-Agent gleichzeitig mit anderen Sicherheitslösungen auf einem Endpunkt betrieben wird, kann dies deren Funktion stören und massive Probleme auf dem System verursachen.

9. **Scan-Modus**. Wählen Sie die Scan-Technologie, die am besten zu Ihrer Netzwerkumgebung und den Ressourcen Ihrer Endpunkte passt. Den Scan-Modus können Sie festlegen, indem Sie eine der folgenden Optionen wählen:
   - **Automatisch**. In diesem Fall erkennt der Sicherheitsagent automatisch die Konfiguration der entsprechenden Endpunkte und passt die Scan-Technologie daran an:

- Zentralisierter Scan in der Public oder Private Cloud (mit Security Server) mit Ausweichmöglichkeit auf Hybrid-Scan (mit leichten Engines) für physische Computer mit geringer Hardware-Leistung und für virtuelle Maschinen. In diesem Fall muss mindestens ein Security Server im Netzwerk installiert sein.
- Lokaler Scan (mit vollen Engines) für physische Computer mit hoher Hardware-Leistung.
- Lokaler Scan für Amazon-EC2-Instanzen und virtuelle Microsoft-Azure-Maschinen.

Beachten Sie
Als Computer mit geringer Hardware-Leistung gelten Computer mit einer CPU-Frequenz von unter 1,5 GHz oder mit weniger als 1 GB RAM.

- **Benutzerdef**. In diesem Fall können Sie für physische und virtuelle Maschinen verschiedene Scan-Technologien festlegen:
  - Zentralisierter Scan in der Public oder Private Cloud (mit Security Server) mit Ausweichmöglichkeit* auf lokalen Scan (Full Engines) oder auf Hybrid-Scan (Light Engines)
  - Hybrid-Scan (mit leichten Engines)
  - Lokaler Scan (mit vollen Engines)

  Der Standard-Scan-Modus für EC2-Instanzen ist Lokaler Scan (Sicherheitsinhalte werden im installierten Sicherheitsagenten gespeichert, und der Scan wird lokal auf der Maschine ausgeführt). Wenn Sie Ihre EC2-Instanzen mit einem Security Server scannen möchten, müssen Sie das Installationspaket des Sicherheitsagenten und die angewandte Richtlinie entsprechend konfigurieren.

  Der Standard-Scan-Modus für virtuelle Microsoft-Azure-Maschinen ist Lokaler Scan (Sicherheitsinhalte werden im installierten Sicherheitsagenten gespeichert, und der Scan wird lokal auf der Maschine ausgeführt). Wenn Sie Ihre virtuellen Microsoft-Azure-Maschinen mit einem Security Server scannen möchten, müssen Sie das Installationspaket des Sicherheitsagenten und die angewandte Richtlinie entsprechend konfigurieren.

* Bei Scans mit zwei Engines wird die Ausweich-Engine verwendet, wenn die erste Engine nicht verfügbar ist. Der Ressourcenverbrauch und die Netzwerknutzung hängen von der verwendeten Engine ab.

Weitere Informationen zu verfügbaren Scan-Technologien finden Sie hier:„Scan-Engines“ (S. 3)

10. **Endpunkt mit vShield installieren, wenn eine mit vShield integrierte VMware-Umgebung gefunden wird**. Diese Option kann gewählt werden, wenn das Installationspaket auf einer virtuellen Maschine in einer VMware-Umgebung mit vShield installiert wird. In diesem Fall wird VMware vShield Endpoint statt dem Bitdefender-Sicherheitsagenten auf der Maschine installiert.

   Wichtig
   Diese Option steht nur für Ferninstallationen und nicht für lokale Installationen zur Verfügung. Bei lokalen Installationen in VMware-Umgebungen mit vShield können Sie wahlweise das Paket für mit vShield integrierte Umgebungen herunterladen.

11. Wenn Sie die Scan-Engines auf Public oder Private Cloud (Security Server) stellen, müssen Sie die lokal installierten Security Server, die Sie verwenden möchten, auswählen und ihre Priorität im Bereich **Security Server-Zuweisung** konfigurieren:

    a. Klicken Sie auf die Liste der Security Server in der Tabellenüberschrift. Die Liste der gefundenen Security Server wird angezeigt.

    b. Wählen Sie eine Entität.

    c. Klicken Sie in der Spaltenüberschrift **Aktionen** auf die Schaltfläche ⊕ **Hinzufügen**.

    Der Security Server wird der Liste hinzugefügt.

    d. Wiederholen Sie diese Schritte, wenn Sie mehrere Security-Server hinzufügen möchten, falls es mehrere gibt. In diesem Fall können Sie ihre Priorität konfigurieren, indem Sie auf die rechts von jeder Entität angezeigten Pfeile (⌃ und ⌄) klicken. Wenn der erste Security Server nicht verfügbar ist, wird der nächste verwendet, und dann der nächste, usw.

    e. Um eine Entität aus der Liste zu entfernen, klicken Sie auf die entsprechende Schaltfläche ⊗ **Löschen** am oberen Rand der Tabelle.

Sie können die Verbindung zum Security Server mit der Option **SSL verwenden** verschlüsseln.

12. **Verschiedenes**. Sie können die folgenden Optionen für verschiedene Dateitypen von den Zielendpunkten festlegen:
    - **Absturzabbilder übermitteln**. Wählen Sie diese Option, damit Speicherabbilddateien zur Analyse an die Bitdefender Labs geschickt werden, wenn der Sicherheitsagent abstürzt. Die Abbilddateien helfen unseren Mitarbeitern dabei, die Ursache des Problems zu finden und ein Wiederauftreten zu verhindern. Es werden keine persönlichen Informationen mitgesendet.
    - **Dateien in der Quarantäne jede Stunde an die Bitdefender-Labs senden.**. Die Dateien in Quarantäne werden standardmäßig einmal pro Stunde automatisch an die Bitdefender-Labors geschickt. Sie können das Intervall zum Versand der in die Quarantäne verschobenen Dateien festlegen. Die Beispieldateien werden dann von den Bitdefender-Malware-Forschern analysiert. Sollten das Vorhandensein von Malware bestätigt werden, wird eine Signatur veröffentlicht, um das Entfernen der Malware zu ermöglichen.
    - **Verdächtige ausführbare Dateien an Bitdefender weiterleiten**. Wählen Sie diese Option aus, damit nicht vertrauenswürdige oder verdächtige Dateien zur Analyse an die Bitdefender Labs übermittelt werden.
13. Wählen Sie **Vor der Installation scannen**, wenn Sie sichergehen möchten, dass die Maschinen sauber sind, bevor Sie den Client auf ihnen installieren. Es wird dann ein Cloud-Schnell-Scan auf den Maschinen ausgeführt, bevor die Installation gestartet wird.
14. Bitdefender Endpoint Security Tools wird im Standard-Installationsverzeichnis installiert. Wählen Sie **Benutzerdefinierten Installationspfad verwenden**, wenn Sie den Bitdefender-Agenten in einem anderen Ordner installieren möchten. Wenn der angegebene Ordner nicht existiert, wird er während der Installation erstellt.
    - Unter Windows lautet der Standardpfad `C:\Program Files\`. Wenn Sie Bitdefender Endpoint Security Tools in einem anderen Ordner installieren möchten, müssen Sie sich bei der Pfadbezeichnung an die Windows-Konventionen halten. Zum Beispiel `D:\Ordnername`.
    - Unter Linux wird Bitdefender Endpoint Security Tools standardmäßig im Ordner `/opt` installiert. Wenn Sie den Bitdefender-Agenten in einem anderen

Ordner installieren möchten, müssen Sie sich bei der Pfadbezeichnung an die Linux-Konventionen halten. Zum Beispiel `/Ordnername`.

Bei der Installation von Bitdefender Endpoint Security Tools sind folgende Pfade ausgeschlossen:

- an einem Pfad, der nicht mit einem Schrägstrich (/) beginnt; Die einzige Ausnahme hierzu ist der Windows-Pfad `%PROGRAMFILES%`, der vom Sicherheitsagenten als der Linux-Standardordner `/opt` interpretiert wird.
- Jeder Pfad, der sich unter `/tmp` oder `/proc` befindet.
- Jeder Pfad, der die folgenden Sonderzeichen enthält: `$, !, *, ?, ?, ", ', `, \, (,), [,], {, }`.
- Der `systemd`-Bezeichner (%).

Unter Linux wird für die Installationen an einem benutzerdefinierten Pfad mindestens glibc 2.21 benötigt.

Wichtig
Wenn Sie einen benutzerdefinierten Pfad verwenden, stellen Sie sicher, dass Sie für jedes Betriebssystem das richtige Installationspaket verwenden.

15. Bei Bedarf können Sie ein Passwort einrichten, um zu verhindern, dass Benutzer Ihren Schutz entfernen. Wählen Sie **Deinstallationspasswort festlegen** und geben Sie das gewünschte Passwort in die entsprechenden Felder ein.
16. Wenn sich die entsprechenden Endpunkte im Netzwerkinventar unter **Benutzerdefinierte Gruppen** befinden, können Sie sie direkt nach Abschluss der Installation des Sicherheitsagenten in einen anderen Ordner verschieben.

    Wählen Sie **Benutzerdefinierten Ordner verwenden**, und wählen Sie aus der entsprechenden Tabelle einen Ordner.
17. Wählen Sie im Bereich **Installer** die Entität, zu der die Endpunkte einer Verbindung herstellen sollen, um den Client zu installieren und zu aktualisieren.

    - **GravityZone-Appliance**, wenn die Endpunkte eine direkte Verbindung zur GravityZone-Appliance herstellen.

      Für diesen Fall können Sie auch Folgendes definieren:

      - Einen benutzerdefinierten Kommunikationsserver; geben Sie dazu, falls erforderlich, die entsprechende IP-Adresse oder den Hostnamen ein.

- Proxy-Einstellungen, wenn die Endpunkte über einen Proxy-Server mit der GravityZone-Appliance kommunizieren. Wählen Sie in diesem Fall **Proxy für die Kommunikation verwenden** und geben Sie die nötigen Proxy-Einstellungen in de entsprechenden Felder ein.

- **Endpoint-Security-Relais** - wenn Sie die Endpunkte mit einem in Ihrem Netzwerk installierten Relais-Client verbinden möchten. Alle Maschinen mit der Relais-Rolle, die in Ihrem Netzwerk gefunden wurden, werden in der unten angezeigten Tabelle aufgeführt. Wählen Sie die gewünschte Relais-Maschine. Verbundene Endpunkte kommunizieren mit dem Control Center ausschließlich über das angegebene Relais.

  Wichtig
  Port 7074 muss offen sein, damit die Installation über einen Bitdefender Endpoint Security Tools Relay funktioniert.

18. Klicken Sie auf **Speichern**.

Das neu erstellte Paket wird zur Liste der Pakete hinzugefügt.

Beachten Sie
Die in einem Installationspaket konfigurierten Einstellungen werden sofort nach der Installation auf den jeweiligen Endpunkt angewendet. Sobald eine Richtlinie auf den Client angewendet wird, werden die Einstellungen dieser Richtlinie durchgesetzt und ersetzen gegebenenfalls die Einstellungen des Installationspakets (z. B. Kommunikationsserver oder Proxy-Einstellungen).

Installationspakete herunterladen

So laden Sie die Installationspakete der Sicherheitsagenten herunter:

1. Melden Sie sich über den Endpunkt, auf dem Sie die Software installieren möchten, am Control Center an.
2. Gehen Sie zur Seite **Netzwerk > Pakete**.
3. Wählen Sie das Installationspaket aus, das Sie herunterladen möchten.
4. Klicken Sie auf die Schaltfläche **Herunterladen** am oberen Rand der Tabelle und wählen Sie den Installer-Typ aus, den Sie verwenden möchten. Es gibt zwei Arten von Installationsdateien:

   - **Downloader**. Der Downloader lädt zunächst das vollständige Installationspaket von den Bitdefender-Cloud-Servern herunter und beginnt

dann mit der Installation. Der Installer ist ein kleines Programm und kann sowohl auf 32-Bit- als auch auf 64-Bit-Systemen ausgeführt werden (und vereinfacht so die Verteilung). Er erfordert jedoch eine aktive Internet-Verbindung.

- **Installationspaket**. Die vollständigen Installationskits sind größer und sie müssen auf einem bestimmten Betriebssystem ausgeführt werden.

  Das vollständige Kit ist dafür da, um den Schutz auf Endpunkten mit einer langsamen bzw. keiner Internet-Verbindung zu installieren. Laden Sie diese Datei auf einen mit dem Internet verbundenen Endpunkt herunter und nutzen Sie externe Speichermedien oder eine Netzwerkfreigabe, um die Datei an andere Endpunkte weiterzugeben.

  Beachten Sie
  Verfügbare Installationspaket-Versionen:
  - **Windows OS:** 32-Bit- und 64-Bit-Systeme
  - **Linux OS:** 32-Bit- und 64-Bit-Systeme
  - **macOS:** nur 64-Bit-Systeme

  Vergewissern Sie sich, dass Sie die zum jeweiligen System passende Version wählen.

5. Speichern Sie die Datei auf dem Endpunkt.

   Warnung
   - Die Downloader-Datei darf nicht umbenannt werden, da sonst die Installationsdateien nicht vom Bitdefender-Server heruntergeladen werden können.

6. Zusätzlich können Sie, wenn Sie den Downloader gewählt haben, ein MSI-Paket für Windows-Endpunkte erstellen. Weitere Informationen finden Sie in diesem Artikel der Wissensdatenbank.

Download-Links zu den Installationspaketen per E-Mail senden

Vielleicht möchten Sie andere Benutzer schnell darüber informieren, dass ein Installationspaket zum Download bereitsteht. Gehen Sie dazu wie folgt vor:

1. Gehen Sie zur Seite **Netzwerk > Pakete**.
2. Wählen Sie das gewünschte Installationspaket.

3. Klicken Sie auf die Schaltfläche **Download-Links senden** am oberen Rand der Tabelle. Ein Konfigurationsfenster wird sich öffnen.
4. Geben Sie die E-Mail-Adressen aller Benutzer ein, die den Download-Link zum Installationspaket erhalten sollen. Drücken Sie nach jeder E-Mail-Adresse die `Eingabetaste`.

   Vergewissern Sie sich, dass alle eingegebenen E-Mail-Adressen gültig sind.
5. Wenn Sie die Download-Links anzeigen möchten, bevor Sie sie per E-Mail versenden, klicken Sie auf die Schaltfläche **Installationslinks**.
6. Klicken Sie auf **Senden**. An jede eingegebene E-Mail-Adresse wird eine E-Mail mit dem Download-Link gesendet.

Installationspakete ausführen

Damit die Installation erfolgreich durchgeführt werden kann, muss das Installationspaket mit Administratorrechten ausgeführt werden.

Je nach Betriebssystem gestaltet sich die Installation des Pakets etwas unterschiedlich:

- Unter Windows und macOS:
  1. Laden Sie die Installationsdatei vom Control Center auf den gewünschten Endpunkt herunter oder kopieren Sie sie von einer Netzwerkfreigabe.
  2. Wenn Sie das vollständige Kit heruntergeladen haben, extrahieren Sie die Dateien aus dem Archiv.
  3. Führen Sie die ausführbare Datei aus.
  4. Folgen Sie den Instruktionen auf dem Bildschirm.

  Beachten Sie
  Nach der Installation von Endpoint Security for Mac unter macOS werden die Benutzer aufgefordert, Bitdefender-Kernelerweiterungen auf ihren Computern zu genehmigen. Einige Funktionen des Sicherheitsagenten funktionieren erst, wenn die Bitdefender-Kernelerweiterungen genehmigt wurden. Weitere Einzelheiten finden Sie in diesem Artikel in der Wissensdatenbank.

- Unter Linux:
  1. Stellen Sie eine Verbindung zur Control Center her und melden Sie sich an.

2. Laden Sie die Installationsdatei auf den gewünschten Endpunkt herunter oder kopieren Sie sie dorthin.
3. Wenn Sie das vollständige Kit heruntergeladen haben, extrahieren Sie die Dateien aus dem Archiv.
4. Verschaffen Sie sich Root-Rechte, indem Sie den Befehl `sudo su` ausführen.
5. Verändern Sie die Rechte für die Installationsdatei, damit Sie sie ausführen können:

   ```
   # chmod +x installer
   ```

6. Führen Sie die Installationsdatei aus:

   ```
   # ./installer
   ```

7. Um zu überprüfen, ob der Agent auf dem Endpunkt installiert wurde, können Sie diesen Befehl ausführen:

   ```
   $ service bd status
   ```

Einige Minuten nachdem der Sicherheitsagent installiert wurde, wird der Endpunkt im Control Center (**Netzwerk**-Seite) als verwaltet angezeigt.

Wichtig
Wenn Sie VMware Horizon View Persona Management verwenden, wird empfohlen, die Active Directory-Gruppenrichtlinien so zu konfigurieren, dass die folgenden Bitdefender-Prozesse ausgeschlossen werden (ohne den vollständigen Pfad):

- `bdredline.exe`
- `epag.exe`
- `epconsole.exe`
- `epintegrationservice.exe`
- `epprotectedservice.exe`
- `epsecurityservice.exe`
- `epupdateservice.exe`
- `epupdateserver.exe`

Diese Ausschlüsse müssen angewendet werden, solange der Sicherheitsagent auf dem Endpunkt läuft. Weitere Einzelheiten finden Sie auf dieser Seite der VMware-Horizon-Dokumentation.

Remote-Installation

Mit Control Center können Sie den Sicherheitsagenten über Installationsaufgaben aus der Ferne auf Endpunkten installieren, die sich in Netzwerken befinden, die mit Control Center integriert sind, sowie auf anderen im Netzwerk gefundenen Endpunkten. In VMware-Umgebungen wird zur Ferninstallation VMware Tools benötigt, während in Citrix XenServer- und Nutanix Prism Element-Umgebungen administrative Windows-Freigaben und SSH benötigt werden.

Nachdem der Sicherheitsagent auf einem Endpunkt installiert wurde, kann es einige Minuten dauern, bis die anderen Netzwerkendpunkte im Control Center angezeigt werden.

Bitdefender Endpoint Security Tools verfügt über einen automatischen Netzwerkerkennungsmechanismus, mit dem Endpunkte gefunden werden können, die nicht im Active Directory sind. Die gefundenen Endpunkte werden als **nicht verwaltet** auf der **Netzwerk**-Seite angezeigt (in der Ansicht **Computer** unter **Benutzerdefinierte Gruppen**). Control Center entfernt Active-Directory-Endpunkte automatisch von der Liste der gefundenen Endpunkte.

Damit die Netzwerkerkennung funktioniert, müssen Sie Bitdefender Endpoint Security Tools bereits auf mindestens einem Endpunkt im Netzwerk installiert haben. Dieser Endpunkt wird dann verwendet, um das Netzwerk zu scannen und Bitdefender Endpoint Security Tools auf den noch nicht geschützten Endpunkten zu installieren.

Weitere Informationen zur Netzwerkerkennung finden Sie unter „Wie die Netzwerkerkennung funktioniert“ (S. 164).

Anforderungen für die Ferninstallation

Damit die Ferninstallation funktioniert, müssen die folgenden Punkte gegeben sein:

- Unter Windows:
  - Die administrative Freigabe `admin$` muss aktiviert sein. Konfigurieren Sie jeden Zielarbeitsplatzrechner so, dass die erweiterte Freigabe von Dateien nicht verwendet wird.

- Konfigurieren Sie die Benutzerkontensteuerung abhängig vom Betriebssystem, das auf den Endpunkten läuft. Wenn die Endpunkte in einer Active-Directory-Domain sind, können Sie die Benutzerkontensteuerung über eine Gruppenrichtlinie konfigurieren. Weitere Einzelheiten finden Sie in diesem Artikel in der Wissensdatenbank.
- Deaktivieren Sie die Windows-Firewall oder konfigurieren Sie sie so, dass Datenverkehr über das Datei- und Druckerfreigabeprotokoll zugelassen wird.

Beachten Sie
Die Ferninstallation funktioniert nur auf neueren Betriebssystemen ab Windows 7 / Windows Server 2008 R2, die Bitdefender vollständig unterstützt. Weitere Informationen finden Sie unter „Unterstützte Betriebssysteme“ (S. 29).

- Unter Linux: SSH muss aktiviert sein.
- Unter macOS: Remote-Anmeldung und Dateifreigaben müssen aktiviert sein.

Ausführen von Ferninstallationsaufgaben

So führen Sie eine Ferninstallationsaufgabe aus:

1. Stellen Sie eine Verbindung zur Control Center her und melden Sie sich an.
2. Gehen Sie zur Seite **Netzwerk**.
3. Wählen Sie **Computer und virtuelle Maschinen** aus der Ansichtsauswahl.
4. Wählen Sie die gewünschte Gruppe aus dem linken Fenster. Die Entitäten der ausgewählten Gruppe werden in der Tabelle im rechten Fenster angezeigt.

   Beachten Sie
   Sie können optional auch Filter anwenden, um ausschließlich die nicht verwalteten Endpunkte anzuzeigen. Klicken Sie auf das **Filter**-Menü und wählen Sie die folgenden Optionen: **Nicht verwaltet** aus dem Reiter **Sicherheit** und **Alle Objekte rekursiv** aus dem Reiter **Tiefe**.

5. Wählen Sie die Entitäten (Endpunkte oder Gruppen von Endpunkten) aus, auf denen Sie den Schutz installieren möchten.
6. Klicken Sie auf die Schaltfläche **Aufgaben** am oberen Rand der der Tabelle, und wählen Sie **Installieren**.

   Der Assistent **Client installieren** wird angezeigt.

Installation von Bitdefender Endpoint Security Tools über das Aufgabenmenü

7. Konfigurieren Sie im Bereich **Optionen** den Installationszeitpunkt:
   - **Jetzt** - hiermit startet die Installation sofort.
   - **Geplant** - hiermit legen Sie ein Intervall für die Wiederholung der Installation fest. Wählen Sie einfach das Intervall (stündlich, täglich oder wöchentlich), das Ihnen am besten passt.

     Beachten Sie
     Wenn zum Beispiel bestimmte Operationen auf einer bestimmten Maschine nötig sind, bevor der Client installiert wird (z. B. Deinstallation anderer Software oder Neustart des Betriebssystems), können Sie die Installationsaufgabe für alle 2 Stunden planen. Die Aufgabe wird dann auf jeder entsprechenden Maschine alle 2 Stunden ausgeführt, bis die gesamte Installation abgeschlossen ist.

8. Wenn Sie möchten, dass die Endpunkte nach Abschluss der Installation automatisch neu gestartet werden, wählen Sie **Autom. Neustart (falls erforderlich)**.
9. Geben Sie im Bereich **Zugangsdaten-Manager** die Administratorzugangsdaten an, die für die Fernauthentifizierung auf den entsprechenden Endpunkten benötigt werden. Sie können die Zugangsdaten hinzufügen, indem Sie den Benutzer und das Passwort der Zielbetriebssysteme eingeben.

Wichtig
Bei Windows-8.1-Systemen müssen Sie die Zugangsdaten des eingebauten Administratorkontos oder die eines Domänenadministratorkontos eingeben. Weiteres zu diesem Thema erfahren Sie in diesem Artikel.

So fügen Sie erforderlichen OS-Zugangsdaten hinzu:

a. Geben Sie im entsprechenden Feld in der Spaltenüberschrift den Benutzernamen und das Passwort eines Administratorkontos ein.

   Wenn Computer in einer Domäne sind, reicht es aus, die Anmeldeinformationen des Domänenadministrators einzugeben.

   Bei der Eingabe des Namens eines Nutzerkontos Windows-Konvention verwenden:

   - Für Active Directory-Maschinen wird folgende Syntax verwendet: `username@domain.com` und `Domäne\Benutzername`. Um sicherzugehen, dass die eingegebenen Zugangsdaten funktionieren, geben Sie sie in beiden Ausdrucksweisen ein (`Benutzername@domain.com` und `Domain\Benutzername`).
   - Bei Arbeitsgruppen-Maschinen genügt die Eingabe des Benutzernamens ohne Angabe des Namens der Arbeitsgruppe.

   Sie können jedem Konto eine Beschreibung hinzufügen, um es später leichter identifizieren zu können.

b. Klicken Sie auf den Button ⊕**Hinzufügen**. Das Konto wird zu der Liste der Zugangsdaten hinzugefügt.

Beachten Sie
Die angegebenen Zugangsdaten werden automatisch im Zugangsdaten-Manager gespeichert, sodass Sie sie beim nächsten Mal nicht mehr eingeben werden müssen. Den Zugangsdaten-Manager können Sie einfach öffnen, indem Sie mit dem Mauszeiger auf Ihren Benutzernamen in der rechten oberen Ecke der Konsole fahren.

Wichtig
Sind die für einen Endpunkt eingegebenen Zugangsdaten ungültig, schlägt die Installation des Clients auf diesem Endpunkt fehl. Denken Sie daran, die eingegebenen Zugangsdaten im Zugangsdaten-Manager zu aktualisieren, wenn sie auf den Endpunkten geändert werden.

10. Markieren Sie die Kästchen für die Konten, die Sie verwenden möchten.

> **Beachten Sie**
> Wenn Sie noch keine Zugangsdaten ausgewählt haben, wird eine Warnmeldung angezeigt. Dieser Schritt kann bei der Ferninstallation des Sicherheitsagenten auf Endpunkten nicht ausgelassen werden.

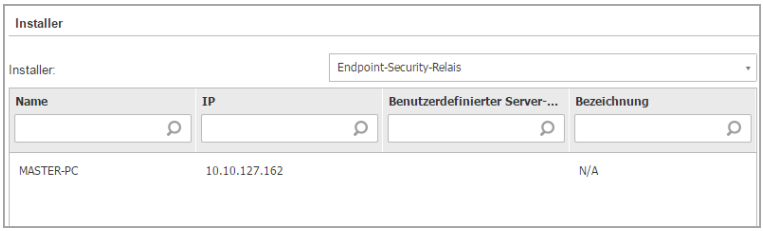
11. Wählen Sie im Bereich **Installer** die Entität, zu der die Endpunkte einer Verbindung herstellen sollen, um den Client zu installieren und zu aktualisieren.
    - **GravityZone-Appliance**, wenn die Endpunkte eine direkte Verbindung zur GravityZone-Appliance herstellen.

      In diesem Fall können Sie auch Folgendes definieren:

      – Einen benutzerdefinierten Kommunikationsserver; geben Sie dazu, falls erforderlich, die entsprechende IP-Adresse oder den Hostnamen ein.

      – Proxy-Einstellungen, wenn die Endpunkte über einen Proxy-Server mit der GravityZone-Appliance kommunizieren. Wählen Sie in diesem Fall **Proxy für die Kommunikation verwenden** und geben Sie die nötigen Proxy-Einstellungen in de entsprechenden Felder ein.
    - **Endpoint-Security-Relais** - wenn Sie die Endpunkte mit einem in Ihrem Netzwerk installierten Relais-Client verbinden möchten. Alle Maschinen mit der Relais-Rolle, die in Ihrem Netzwerk gefunden wurden, werden in der unten angezeigten Tabelle aufgeführt. Wählen Sie die gewünschte Relais-Maschine. Verbundene Endpunkte kommunizieren mit dem Control Center ausschließlich über das angegebene Relais.

> **Wichtig**
> Port 7074 muss offen sein, damit die Installation über einen Relais-Agenten funktioniert.



12. Im Bereich **Zusätzliche Ziele** können Sie den Client auf bestimmten Maschinen in Ihrem Netzwerk installieren, die nicht im Netzwerkinventar angezeigt werden. Vergrößern Sie den Bereich und geben Sie die IP-Adressen oder die Hostnamen dieser Maschinen, durch Kommas getrennt, in das entsprechende Feld ein. Sie können so viele IP-Adressen wie nötig hinzufügen.
13. Sie müssen ein Installationspaket für die aktuelle Installation auswählen. Klicken Sie auf die Liste **Paket verwenden** und wählen Sie das gewünschte Paket. Hier finden Sie alle bisher für Ihr Konto erstellten Installationspakete ebenso wie das Standard-Installationspaket, das im Control Center enthalten ist.
14. Wenn nötig, können Sie die Einstellungen des ausgewählten Installationspakets abändern, indem Sie neben dem Feld **Paket verwenden** auf die Schaltfläche **Anpassen** klicken.

    Die Einstellung des Installationspakets werden unten angezeigt, und Sie können die nötigen Änderungen vornehmen. Weitere Informationen zur Änderung von Installationspaketen finden Sie unter „Installationspakete erstellen“ (S. 146).

    Wenn Sie die Änderungen als neues Paket speichern möchten, wählen Sie die Option **Als Paket speichern** unter der Paketeinstellungsliste und vergeben Sie einen neuen Namen für das neue Paket.
15. Klicken Sie auf **Speichern**. Eine Bestätigungsmeldung wird angezeigt.

Auf der Seite **Netzwerk > Aufgaben** können Sie Aufgaben anzeigen und verwalten.

Wichtig
Wenn Sie VMware Horizon View Persona Management verwenden, wird empfohlen, die Active Directory-Gruppenrichtlinien so zu konfigurieren, dass die folgenden Bitdefender-Prozesse ausgeschlossen werden (ohne den vollständigen Pfad):

- `bdredline.exe`
- `epag.exe`
- `epconsole.exe`
- `epintegrationservice.exe`
- `epprotectedservice.exe`
- `epsecurityservice.exe`
- `epupdateservice.exe`
- `epupdateserver.exe`

Diese Ausschlüsse müssen angewendet werden, solange der Sicherheitsagent auf dem Endpunkt läuft. Weitere Einzelheiten finden Sie auf dieser Seite der VMware-Horizon-Dokumentation.

Linux-System für Zugriff-Scans vorbereiten

In Bitdefender Endpoint Security Tools für Linux können Zugriff-Scans durchgeführt werden. Dies funktioniert allerdings nur bei bestimmten Linux-Distributionen und Kernel-Versionen. Weitere Details erfahren Sie unter Systemvoraussetzungen.

Im nächsten Schritt lernen Sie, wie man das DazukoFS-Modul manuell kompiliert.

Kompilieren Sie das DazukoFS-Modul manuell

Gehen Sie wie unten beschrieben vor, um DazukoFS für die Kernel-Version des Systems zu kompilieren und laden Sie danach das Modul:

1. Laden Sie die geeigneten Kernel-Header herunter.
   - Führen Sie auf **Ubuntu**-Systemen den folgenden Befehl aus:

     ```
     $ sudo apt-get install linux-headers-`uname -r`
     ```

   - Führen Sie auf **RHEL/CentOS**-Systemen den folgenden Befehl aus:

     ```
     $ sudo yum install kernel-devel kernel-headers-`uname -r`
     ```

2. Auf **Ubuntu**-Systemen benötigen Sie das Paket `build-essential`:

   ```
   $ sudo apt-get install build-essential
   ```

3. Kopieren und extrahieren Sie den DazukoFS-Quellcode in einem Verzeichnis Ihrer Wahl:

   ```
   # 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. Kompilieren Sie das Modul:

   ```
   # make
   ```

5. Installieren und laden Sie das Modul:

```
# make dazukofs_install
```

Voraussetzungen für Zugriff-Scans mit DazukoFS

Damit DazukoFS und Zugriff-Scans zusammen funktionieren, müssen die folgenden Voraussetzungen erfüllt sein. Vergewissern Sie sich das die folgenden Punkte auf Ihr Linux-System zutreffen und befolgen Sie die Anweisungen, um Probleme zu vermeiden.

- Die SELinux-Richtlinie muss deaktiviert oder auf **tolerant** gestellt sein. Sie können die Einstellungen der SELinux-Richtlinie einsehen und anpassen, indem Sie die Datei `/etc/selinux/config` bearbeiten.
- Bitdefender Endpoint Security Tools ist ausschließlich mit der Version von DazukoFS kompatibel, die im Installationspaket enthalten ist. Wenn DazukoFS auf Ihrem System bereits installiert ist, muss es vor der Installation von Bitdefender Endpoint Security Tools entfernt werden.
- DazukoFS unterstützt bestimmte Kernel-Versionen. Wenn das in Bitdefender Endpoint Security Tools enthaltene DazukoFS-Paket nicht mit der Kernel-Version des Systems kompatibel ist, kann das Modul nicht geladen werden. Ist das der Fall, können Sie den Kernel auf die unterstützte Version aktualisieren oder das DazukoFS-Modul für Ihre Kernel-Version rekompilieren. Das DazukoFS-Paket befindet sich im Installationsverzeichnis von Bitdefender Endpoint Security Tools:

  `/opt/BitDefender/share/modules/dazukofs/dazukofs-modules.tar.gz`
- Wenn Sie für Dateifreigaben dedizierte Server wie NFS, UNFSv3 oder Samba verwenden, müssen Sie die Dienste in der folgenden Reihenfolge starten:

  1. Aktivieren Sie im Control Center Zugriff-Scans per Richtlinie.

     Weitere Informationen hierzu finden Sie im GravityZone-Administratorhandbuch.

  2. Starten Sie den Dienst für die Netzwerkfreigabe.

     Für NFS:

     ```
     # service nfs start
     ```

Für UNFSv3:

```
# service unfs3 start
```

Für Samba:

```
# service smbd start
```

Wichtig
Beim NFS-Dienst ist DazukoFS nur mit dem NFS-User-Server kompatibel.

Wie die Netzwerkerkennung funktioniert

Neben der Integration mit Active Directory verfügt GravityZone über automatische Netzwerkerkennungsmechanismen zur Erkennung von Arbeitsgruppen-Computern.

GravityZone nutzt den **Microsoft-Computersuchdienst** und das Tool **NBTscan** für die Netzwerkerkennung.

Der Computersuchdienst ist eine Netzwerktechnologie, die auf Windows-basierten Computern zum Einsatz kommt, um immer aktuelle Listen von Domänen, Arbeitsgruppen und den Computern darin zu verwalten und diese Listen bei Bedarf an Client-Computer weiterzugeben. Computer, die über den Computersuchdienst im Netzwerk erkannt wurden, können durch Eingabe des **Net View**-Befehls im Eingabeaufforderungsfenster angezeigt werden.

Der Net-View-Befehl

Das Tool NBTscan scannt Computernetzwerke mit NetBIOS. Es fragt jeden Endpunkt im Netzwerk ab und sammelt Informationen wie IP-Adresse, NetBIOS-Computername und MAC-Adresse.

Damit die automatische Netzwerkerkennung funktioniert, müssen Sie Bitdefender Endpoint Security Tools Relay bereits auf mindestens einem Computer im Netzwerk installiert haben. Von diesem Computer aus wird das Netzwerk gescannt.

Wichtig

Das Control Center verwendet keine Netzwerkinformationen von Active Directory oder aus der Netzwerkübersicht. Die Netzwerkübersicht nutzt eine andere Technologie zur Netzwerkerkennung: das Link-Layer-Topology-Discovery-Protokoll (LLTD).

Control Center übernimmt keine aktive Rolle bei der Ausführung des Computersuchdienstes. Bitdefender Endpoint Security Tools fragt beim Computersuchdienst lediglich die Liste der aktuell im Netzwerk sichtbaren Arbeitsplatzrechner und Server ab (die Suchliste) und leitet diese dann an das Control Center weiter. Das Control Center verarbeitet die Suchliste und fügt neu erkannte Computer zur der Liste der **nicht verwalteten Computer** hinzu. Bereits erkannte Computer werden nach einer Netzwerkerkennungsabfrage nicht gelöscht, daher müssen Computer, die sich nicht mehr länger im Netzwerk befinden, manuell ausgeschlossen und gelöscht werden.

Die erste Abfrage der Suchliste wird vom ersten im Netzwerk installierten Bitdefender Endpoint Security Tools durchgeführt.

- Falls das Relais auf einem Arbeitsgruppen-Computer installiert wurde, werden im Control Center nur die Computer dieser Arbeitsgruppe angezeigt.
- Falls das Relais auf einem Domänen-Computer installiert wurde, werden im Control Center nur die Computer dieser Domäne angezeigt. Computer aus anderen Domänen können erkannt werden, wenn eine Vertrauensstellung mit der Domäne besteht, in der das Relais installiert ist.

Nachfolgende Netzwerkerkennungsabfragen werden danach stündlich wiederholt. Bei jeder neuen Abfrage teilt das Control Center die verwalteten Computer in Sichtbarkeitsbereiche auf und bestimmt in jedem Bereich ein Relais zur Durchführung der Aufgabe. Ein Sichtbarkeitsbereich ist eine Gruppe von Computern, die sich gegenseitig erkennen. Normalerweise wird ein Sichtbarkeitsbereich anhand einer Arbeitsgruppe oder Domäne definiert, im Einzelfall hängt dies jedoch von der Netzwerktopologie und Konfiguration ab. Unter Umständen besteht ein Sichtbarkeitsbereich auch aus mehreren Domänen oder Arbeitsgruppen.

Falls ein ausgewähltes Relais die Abfrage nicht durchführt, wartet das Control Center auf die nächste geplante Abfrage, ohne ein anderes Relais für einen weiteren Versuch auszuwählen.

Um das gesamte Netzwerk sichtbar zu machen, muss das Relais auf mindestens einem Computer in jeder Arbeitsgruppe oder Domäne in Ihrem Netzwerk installiert sein. Im Idealfall sollte Bitdefender Endpoint Security Tools auf mindestens einem Computer in jedem Subnetzwerk installiert sein.

Weitere Informationen zum Microsoft-Computersuchdienst

Der Computersuchdienst auf einen Blick:

- Funktioniert unabhängig von Active Directory.
- Läuft ausschließlich über IPv4-Netzwerken und funktioniert unabhängig innerhalb der Grenzen einer LAN-Gruppe (Arbeitsgruppe oder Domäne). Eine Suchliste wird für jede LAN-Gruppe erstellt und verwaltet.
- Nutzt für die Kommunikation zwischen den Knoten üblicherweise verbindungslose Server-Übertragungen.
- Nutzt NetBIOS über TCP/IP (NetBT).
- Benötigt NetBIOS-Namensauflösung. Es wird empfohlen im Netzwerk eine Windows-Internet-Name-Service-Infrastruktur (WINS) zu unterhalten.
- Ist standardmäßig nicht in Windows Server 2008 und 2008 R2 aktiviert.

Weitere Informationen zum Computersuchdienst finden Sie in der Computer Browser Service Technical Reference im Microsoft Technet.

Anforderungen für Netzwerkerkennung

Um alle Computer (Server und Arbeitsplatzrechner) erfolgreich zu erkennen, die über das Control Center verwaltet werden sollen, ist Folgendes erforderlich:

- Die Computer müssen in einer Arbeitsgruppe oder Domäne zusammengefasst und über ein lokales IPv4-Netzwerk verbunden sein. Der Computersuchdienst funktioniert nicht über IPv6-Netzwerke.
- In jeder LAN-Gruppe (Arbeitsgruppe oder Domäne) müssen mehrere Computer den Computersuchdienst ausführen. Auch die primären Domänencontroller müssen den Dienst ausführen.
- NetBIOS über TCP/IP (NetBT) muss auf den Computern aktiviert sein. Die lokale Firewall muss NetBT-Verkehr zulassen.
- Wenn Sie mit einem Linux-Relais andere Linux- oder Mac-Endpunkte erkennen möchten, müssen Sie entweder auf den Zielendpunkten Samba installieren oder

sie in einem Active Directory zusammenfassen und DHCP verwenden. Damit wird NetBIOS automatisch auf ihnen konfiguriert.

- Die Freigabe von Dateien muss auf den Computern aktiviert sein. Die lokale Firewall muss die Freigabe von Dateien zulassen.
- Eine Windows-Internet-Name-Service-Infrastruktur (WINS) muss eingerichtet und funktionsfähig sein.
- Die Netzwerkerkennung muss aktiviert sein (**Systemsteuerung (> Netzwerk und Internet) > Netzwerk- und Freigabecenter > Erweiterte Freigabeeinstellungen ändern**).

  Um diese Funktionen nutzen zu können, müssen die folgenden Dienste gestartet werden:
  - DNS-Client
  - Funktionssuche-Ressourcenveröffentlichung
  - SSDP-Suche
  - UPnP-Gerätehost
- In Umgebungen mit mehreren Domänen empfiehlt es sich, Vertrauensstellungen zwischen den Domänen einzurichten, damit die Computer auch auf Suchlisten aus anderen Domänen zugreifen können.

Computer, über die Bitdefender Endpoint Security Tools den Computersuchdienst abfragt, müssen in der Lage sein, NetBIOS-Namen aufzulösen.

Beachten Sie
Der Mechanismus zur Netzwerkerkennung funktioniert auf allen unterstützten Betriebssystemen, einschließlich der Windows-Embedded-Versionen, vorausgesetzt, dass alle Anforderungen erfüllt werden.

5.4. Installation des Sandbox Analyzer On-Premises

Führen Sie die folgenden Schritte aus, um die Installation möglichst reibungslos zu gestalten:

1. Installation vorbereiten
2. Virtuelle Sandbox Analyzer-Appliance bereitstellen
3. Network Security Virtual Appliance bereitstellen

5.4.1. Installation vorbereiten

Stellen Sie vor der Installation von Sandbox Analyzer On-Premises sicher, dass:

- Der VMWare ESXi-Hypervisor installiert und konfiguriert ist. Weitere Einzelheiten finden Sie in der Dokumentation vSphere Installation and Setup, Abschnitt 2: "Installing and Setting Up ESXi".
- Die virtuelle Bitdefender GravityZone-Appliance bereitgestellt und konfiguriert ist.

Beachten Sie
Stellen Sie in Bezug auf den VMWare ESXi-Hypervisor sicher, dass:

- ESXi liegt in Version 6.5 oder höher vor.
- VMFS-Datenspeicher liegt in Version 5 vor.
- SSH ist in der **Startup Policy** mit der Konfiguration **Start and stop with host** aktiviert.
- NTP-Dienst ist aktiv und konfiguriert.

Der Lizenzschlüssel für Sandbox Analyzer On-Premises gibt vor, wie viele Detonationen maximal gleichzeitig durchgeführt werden können. Da für jede Detonation eine laufende Instanz einer virtuellen Maschine benötigt wird, gibt die Anzahl der gleichzeitigen Detonationen die Anzahl der erstellten virtuellen Maschinen wider. Weitere Informationen zum Hinzufügen von Lizenzschlüsseln im GravityZone Control Center finden Sie unter „Ihren Lizenzschlüssel eingeben“ (S. 127).

5.4.2. Virtuelle Sandbox Analyzer-Appliance bereitstellen

So können Sie die virtuelle Sandbox Analyzer-Appliance bereitstellen:

1. Melden Sie sich beim GravityZone Control Center an.
2. Gehen Sie zur Seite **Netzwerk > Pakete**.
3. Aktivieren Sie in der Tabelle das Kontrollkästchen **Sandbox Analyzer**.
4. Klicken Sie oben links auf der Seite auf **Download**. Wählen Sie die Option **Security Appliance (eigenständige ESXi-Version)**.

5. Verwenden Sie Ihr Tool für das Virtualisierungsmanagement (z. B. vSphere Client), um die heruntergeladene OVA-Datei in Ihre virtuelle Umgebung zu importieren.

   Beachten Sie
   Konfigurieren Sie die Netzwerke wie folgt, wenn Sie die OVA-Datei bereitstellen:

   - **Bitdefender-Netzwerk** - Das ist das Netzwerk, in dem sich weitere Bitdefender-Komponenten befinden (`eth0`-Schnittstelle). Sandbox Analyzer und die GravityZone-Appliance müssen sich im selben Netzwerk befinden und über `eth0` kommunizieren.
   - **Privates Detonationsnetzwerk** - Sandbox Analyzer verwendet dieses Netzwerk für die interne Kommunikation (`eth1`-Schnittstelle). Dieses Netzwerk muss von allen anderen Netzwerksegmenten isoliert werden.
   - **Internetzugangsnetzwerk** - Sandbox Analyzer verwendet dieses Netzwerk, um die neuesten Updates abzurufen (`eth2`-Schnittstelle). Die Schnittstelle `eth2` sollte nicht dieselbe IP oder dasselbe Netzwerk haben wie `eth0`.

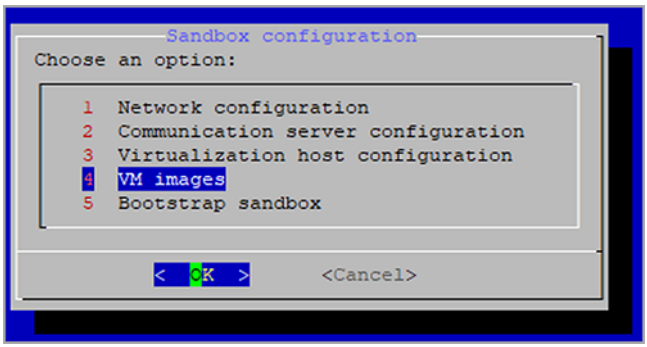
6. Schalten Sie die Appliance an.
7. Greifen Sie von Ihrem Tool für die Virtualisierungsverwaltung auf die Konsolenoberfläche der virtuellen Sandbox Analyzer Appliance zu.
8. Geben Sie als Anmeldeinformationen `root` als Benutzernamen und `sve` als Passwort ein.
9. Rufen Sie durch Ausführung des folgenden Befehls das Konfigurationsmenü auf:

   ```
   /opt/bitdefender/bin/sandbox-setup
   ```

10. Nehmen Sie im Menü **Sandbox configuration** die folgenden Einstellungen vor:
    a. **Netzwerkkonfiguration**. Wählen Sie diese Option, um die Management-NIC zu konfigurieren. Sandbox Analyzer verwendet diese Netzwerkschnittstelle zur Kommunikation mit GravityZone.

       Die IP-Adresse kann manuell oder automatisch über DHCP angegeben werden.

Beachten Sie
Wenn sich die GravityZone-Appliance in einem anderen Netzwerk als `eth0` befindet, müssen Sie unter **Netzwerkkonfiguration > BitDefender-Netzwerk > Routen** eine statische Route hinzufügen, damit Sandbox Analyzer ordnungsgemäß funktionieren kann.



Sandbox Analyzer-Appliance-Konsole

b. **Internet proxy configuration**. Für eine erfolgreiche Installation benötigt Sandbox Analyzer eine Internetverbindung. In diesem Fall können Sie Sandbox Analyzer so konfigurieren, dass er einen Proxy-Server verwendet. Dafür müssen folgende Details angegeben werden:

- **Host** - IP oder FQDN des Proxy-Servers. Verwenden Sie die folgende Syntax: `http://<IP/Hostname>:<Port>`.
- **User and password** - Sie müssen das Passwort zweimal eingeben.
- **Domain** - die Active Directory-Domain, falls zutreffend.

c. **Communication server configuration**. Geben Sie die IP-Adresse oder den Hostnamen der Appliance ein, auf der die Kommunikationsserver-Rolle läuft.

Verwenden Sie die folgende Syntax: `http://<IP/Hostname>:<Port>`. Der Standard-Port ist `8443`.

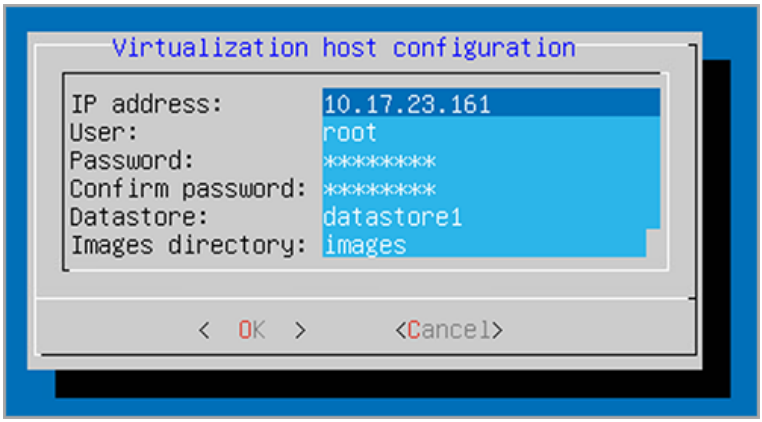
Beachten Sie
Sobald die IP-Adresse oder der Hostname angegeben und die Konfiguration gespeichert wurde, wird die Sandbox Analyzer-Instanz im GravityZone Control Center auf der Seite **Sandbox Analyzer > Infrastruktur** angezeigt.

d. **Konfiguration des virtuellen Hosts** Sandbox Analyzer verwendet ESXi-Server zur Bereitstellung der Infrastruktur für die Malware-Analyse. Über **Virtualized host configuration** verbinden Sie die Sandbox Analyzer-Appliance mit dem ESXi-Host, indem Sie die folgenden Informationen angeben:

- IP-Adresse des ESXi-Servers.
- root-Zugangsdaten für den Zugriff auf den ESXi-Host.
- Datenspeicher für Sandbox Analyzer.

  Geben Sie den Namen des Datenspeichers wie von ESXi angezeigt ein.
- Name des Ordners, der im Datenspeicher zum Speichern von virtuellen Maschinen-Images verwendet wird.

  Wenn dieser Ordner nicht vorhanden ist, müssen Sie ihn im Datenspeicher anlegen, bevor Sie die Sandbox Analyzer-Konfiguration speichern.



Sandbox Analyzer-Appliance-Konsole

e. **VM Images**. Zur Erstellung von virtuellen Maschinen für die Detonation für Sandbox Analyzer müssen Sie die VMDK-Dateien mit den gewünschten Images in den **Images**-Ordner kopieren, der im Menü **Virtualized host configuration** angegeben ist. Im Menü **VM Images** können Sie für jedes Image die folgenden Einstellungen vornehmen:

i. Geben Sie im Menü **Image Configuration** den Namen des Images (wie im GravityZone Control Center angezeigt) und das Betriebssystem an.

Beachten Sie
Der Ordner mit den VM-Images wird regelmäßig überprüft und neue Einträge werden an GravityZone gemeldet. Diese Einträge können im Control Center auf der Seite **Sandbox Analyzer > Infrastruktur > Image-Verwaltung** eingesehen werden.

In bestimmten Situationen kann es bei der Verwendung von Sandbox Analyzer zu Problemen mit den virtuellen Maschinen für die Detonation kommen. Zur Behebung dieser Probleme müssen Sie die Anti-Fingerprinting-Option deaktivieren. Weitere Einzelheiten dazu finden Sie unter „Anti-Fingerprinting-Techniken“ (S. 172).

ii. Über das Menü **DMZ Hosts** können Sie Hostnamen in die Whitelist aufnehmen, die in die virtuellen Maschinen eingebettete Dienste und Komponenten von Drittanbietern für die Kommunikation mit dem Sandbox Manager benötigen. Weitere Einzelheiten dazu finden Sie unter „DMZ Hosts“ (S. 173).

iii. Im Menü **Cleanup** können Sie VM-Images entfernen, die Sie nicht mehr benötigen.

f. **Bootstrap Sandbox**. Nachdem Sie die Konfigurationsdetails von Sandbox Analyzer eingegeben haben, fahren Sie mit der Installation fort, indem Sie diese Option auswählen. Der Status der Installation wird im GravityZone Control Center auf der Seite **Sandbox Analyzer > Infrastruktur** angezeigt.

Anti-Fingerprinting-Techniken

Sandbox Analyzer aktiviert während der Image-Erstellung standardmäßig verschiedene Anti-Fingerprinting-Techniken. Einige Arten von Malware sind in der Lage, zu erkennen, ob sie in einer Sandbox-Umgebung ausgeführt werden. Ist dies der Fall werden ihre Schadroutinen nicht aktiviert.

Der Zweck der Anti-Fingerprinting-Techniken ist es, verschiedene Bedingungen zu simulieren und so eine reale Umgebung nachzubilden. Angesichts der praktisch unbegrenzten Kombinationen aus bereitgestellter Software und Umgebungskonfiguration, Kombinationen, die nicht vorhergesehen oder gesteuert werden können, ist es möglich, dass bestimmte Techniken nicht mit der im Golden Image installierten Software kompatibel sind. Diese Situationen kommen nur selten vor und lassen sich durch die folgenden Anzeichen erkennen:

- Fehler während der Image-Erstellung.
- Fehler beim Versuch, die Software innerhalb des Images auszuführen.

- Fehlermeldungen, die beim Detonieren von Stichroben zurückgegeben werden.
- Lizenzierte Software, die aufgrund ungültiger Lizenzschlüssel nicht mehr funktioniert.

Um in diesen seltenen Situationen schnell Abhilfe zu schaffen, können Sie das Image mit deaktivierten Anti-Fingerprinting-Techniken neu erstellen. Gehen Sie dazu wie folgt vor:

1. Melden Sie sich beim GravityZone Control Center an und löschen Sie das Image.
2. Melden Sie sich bei der Sandbox Analyzer-Appliance an und starten Sie die Sandbox Analyzer-Appliance-Konsole durch Ausführung des folgenden Befehls:

   ```
   /opt/bitdefender/bin/sandbox-setup
   ```

3. Öffnen Sie **VM Images > Image Configuration**.
4. Wählen Sie das Image aus, das Probleme verursacht.
5. Rufen Sie die **Anti-Fingerprinting**-Option auf.
6. Deaktivieren Sie das entsprechende Kontrollkästchen, um die Anti-Fingerprinting-Techniken zu deaktivieren.

DMZ Hosts

Während der Image-Erstellung wird eine virtuelle Infrastruktur erstellt, um die Kommunikation zwischen dem Sandbox Manager und den virtuellen Maschinen zu vereinfachen. Aus der Sicht des Netzwerks bedeutet dies eine isolierte Netzwerkumgebung, die die gesamte potenzielle Kommunikation enthält, die eine detonierte Stichprobe erzeugen könnte.

Über DMZ-Servermenü können Sie Hostnamen in die Whitelist aufnehmen, mit denen in die virtuellen Maschinen eingebettete Dienste und Komponenten von Drittanbietern kommunizieren müssen, um ordnungsgemäß zu funktionieren.

Ein Beispiel hierfür sind die von der Windows-Lizenzierung verwendeten KMS-Lizenzierungsserver, wenn eine Volumenlizenz auf die bereitgestellten virtuellen Maschinen angewendet wird.

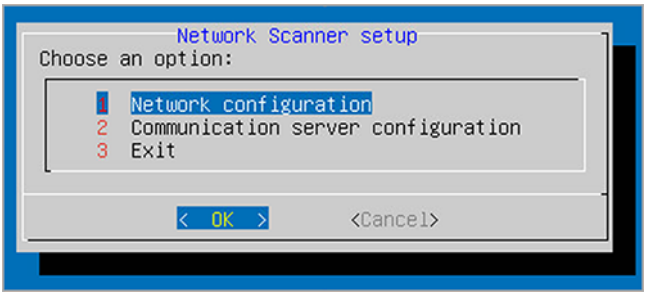
5.4.3. Network Security Virtual Appliance bereitstellen

Dieser Abschnitt beschreibt die Bereitstellung der Network Security Virtual Appliance, einer Komponente von Sandbox Analyzer, die den Netzwerkdatenverkehr erfasst und verdächtige Stichproben zur Verhaltensanalyse übermittelt.

Gehen Sie zur Bereitstellung der Network Security Virtual Appliance wie folgt vor:

1. Melden Sie sich beim GravityZone Control Center an.
2. Gehen Sie zur Seite **Netzwerk > Pakete**.
3. Aktivieren Sie in der Tabelle das Kontrollkästchen **Network Security Virtual Appliance**.
4. Klicken Sie oben links auf die Schaltfläche **Download** und wählen Sie die Option **(VMware OVA)**.
5. Verwenden Sie Ihr Tool für das Virtualisierungsmanagement (z. B. vSphere Client), um die heruntergeladene OVA-Datei in Ihre virtuelle Umgebung zu importieren.
6. Wählen Sie im Bereitstellungsassistenten die Netzwerkschnittstellenkarte (NIC) für die Kommunikation mit GravityZone und die NIC für die Erfassung des Datenverkehrs aus.
7. Schalten Sie die Appliance an.
8. Greifen Sie von Ihrem Tool für die Virtualisierungsverwaltung auf die Konsolenoberfläche von GravityZone SVE SVA Network Security Virtual Appliance zu.
9. Geben Sie als Anmeldeinformationen `root` als Benutzernamen und `sve` als Passwort ein.
10. Rufen Sie durch Ausführung des folgenden Befehls das Konfigurationsmenü auf:

```
/opt/bitdefender/bin/nsva-setup
```



Network Security-Appliance-Konsole

11. Rufen Sie die Option **Communication server configuration** auf.
12. Geben Sie die IP-Adresse oder den Hostnamen und den Port eines GravityZone-Kommunikationsservers an.

    Verwenden Sie die folgende Syntax: `http://<IP/Hostname>:<Port>`. Der Standard-Port ist `8443`.
13. Speichern Sie die Konfiguration.

Netzwerksensor zur Detonation von pcap-Dateien konfigurieren

Der Netzwerksensor kann Inhalte aus Netzwerkerfassungsdateien (pcap) extrahieren und automatisch zur Detonation an die Sandbox Analyzer-Instanz übermitteln.

Gehen Sie zur Detonation von pcap-Dateien wie folgt vor:

1. Melden Sie sich bei der Network Security Virtual Appliance an.
2. Geben Sie als Anmeldeinformationen `root` als Benutzernamen und `sve` als Passwort ein.
3. Führen Sie den folgenden Befehl aus:

   ```
   /opt/bitdefender/bin/scan-pcap <local pcap path>
   ```

   Im Befehl oben steht `<local pcap path>` für den Speicherort, von dem die pcap-Datei in die Network Security Virtual Appliance hochgeladen wird.

Weitere Informationen zur Verwendung des Netzwerksensors finden Sie im Kapitel **Richtlinien > Sandbox Analyzer** im GravityZone-Administratorhandbuch.

5.5. Full Disk Encryption installieren

GravityZone Full Disk Encryption wird als Dienst angeboten, der mit einem Lizenzschlüssel aktiviert werden muss. Geben Sie dazu im Bereich **Konfiguration > Lizenz** den Lizenzschlüssel ein.

Weitere Informationen zu Lizenzschlüsseln finden Sie hier: „Lizenzmanagement“ (S. 126).

Der Bitdefender-Sicherheitsagent unterstützt Full Disk Encryption ab Version 6.2.22.916 unter Windows und ab Version 4.0.0173876 unter macOS. Um sicherzugehen, dass die Agenten vollständig mit diesem Modul kompatibel sind, gibt es zwei Möglichkeiten:

- Installieren Sie die Sicherheitsagenten einschließlich dem Verschlüsselungsmodul.
- Verwenden Sie die Aufgabe **Neu konfigurieren**.

Weitere Informationen zur Verwendung von Full Disk Encryption in Ihrem Netzwerk finden Sie im Kapitel **Sicherheitsrichtlinien > Verschlüsselung** im GravityZone-Administratorhandbuch.

5.6. Schutz für Exchange installieren

Security for Exchange integriert sich automatisch mit den Excchange-Servern je nach Server-Rolle. Für jede Rolle werden entsprechend der folgenden Übersicht nur die kompatiblen Funktionen installiert:

	Microsoft Exchange 2019/2016/2013		Microsoft Exchange 2010/2007		
Bestandteile	**Edge**	**Postfach**	**Edge**	**Hub**	**Postfach**
Transport-Ebene					
Malware-Filter	x	x	x	x	
Antispam-Filterung	x	x	x	x	
Inhaltsfilterung	x	x	x	x	
Anhangsfilterung	x	x	x	x	
Exchange-Informationsspeicher					
Bedarf-Malware-Scans		x			x

5.6.1. Vor der Installation

Bevor Sie Security for Exchange installieren, sollten Sie sich vergewissern, dass alle Voraussetzungen erfüllt sind, da sonst eventuell Bitdefender Endpoint Security Tools ohne das Exchange-Schutz-Modul installiert wird.

Damit das Exchange-Schutz-Modul möglichst reibungslos läuft und etwaige Konflikte und unerwünschte Ergebnisse vermieden werden, sollten Sie andere Malware-Schutz- und E-Mail-Filter-Agenten deinstallieren.

Bitdefender Endpoint Security Tools findet und entfernt die meisten Virenschutzprodukte automatisch und deaktiviert auch den Malware-Schutz-Agenten, der seit Version 2013 in Exchange Server enthalten ist. Eine Liste aller automatisch gefundenen und entfernten Sicherheitssoftware finden Sie in diesem Artikel.

Den eingebauten Exchange-Malware-Schutz-Agenten können Sie jederzeit manuell wieder aktivieren. Dies wird jedoch nicht empfohlen.

5.6.2. Schutz auf Exchange-Servern installieren

Um Ihre Exchange-Server zu schützen, müssen Sie Bitdefender Endpoint Security Tools mit der Exchange-Schutz-Rolle auf jedem dieser Server installieren.

Dazu haben Sie verschiedene Möglichkeiten:

- Lokale Installation durch Herunterladen und Ausführen des Installationspakets auf dem jeweiligen Server.
- Ferninstallation durch Ausführen der Aufgabe **Installieren**.
- Per Fernzugriff durch Ausführen der Aufgabe **Client neu konfigurieren**, falls Bitdefender Endpoint Security Tools bereits das Dateisystem auf dem Server schützt.

Weitere Details zur Installation finden Sie unter „Sicherheitsagent installieren“ (S. 141).

5.7. HVI wird installiert

Um HVI auf virtuellen Maschinen vom Xen-Hosts aus zu nutzen, müssen die folgenden Schritte ausgeführt werden:

1. Installationsvoraussetzungen überprüfen
2. Security Server installieren

3. HVI-Ergänzungspaket installieren

Vorbereitende Maßnahmen

- XenServer ist mit GravityZone verbunden.
- XenCenter ist auf ihrer Maschine installiert.

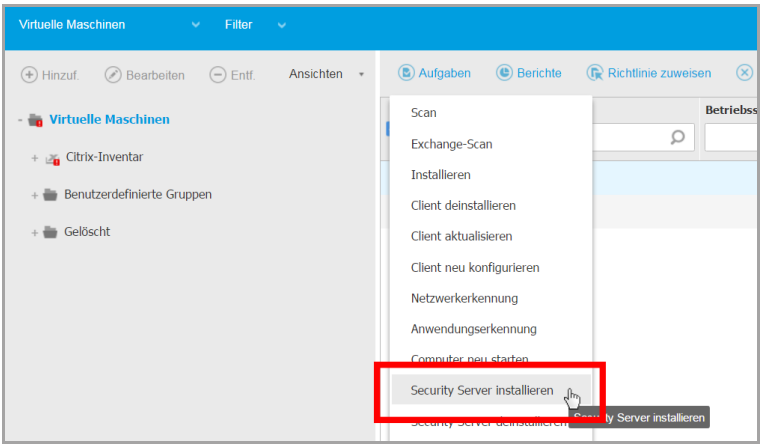
Security Server installieren

Security Server auf einem oder mehreren Hosts installieren:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Virtuelle Maschinen** aus der Ansichtsauswahl.
3. Durchsuchen Sie das Citrix-Inventar und öffnen Sie die Kästchen des gewünschten Hosts. Zur Schnellauswahl können Sie den Root-Container auch direkt anwählen (Citrix-Inventar). Im Installationsassistenten können Sie Hosts einzeln auswählen.

   Beachten Sie
   Sie können nicht Hosts von verschiedenen Ordnern gleichzeitig auswählen.

4. Klicken Sie auf die Schaltfläche **Aufgaben** am oberen Rand der Tabelle und wählen Sie **Security Server installieren** aus dem Menü. Das Fenster **Security Server-Installation** wird angezeigt.



Security Server installieren

5. Wählen Sie den Host, auf dem Sie die Security Server-Instanzen installieren möchten.
6. Wählen Sie die gewünschten Konfigurationseinstellungen.

   Wichtig
   Wenn Sie bei der gleichzeitigen Installation mehrerer Instanzen von Security Server gemeinsame Einstellungen verwenden möchten, müssen die Hosts denselben Speicher benutzen, per DHCP-Server zugewiesene IP-Adressen haben und Teil desselben Netzwerks sein.

   Wenn Sie jeden Security Server anders konfigurieren möchten, können Sie im nächsten Schritt des Assistenten die gewünschten Einstellungen für jeden Host einzeln vornehmen. Die folgend genannten Schritte gelten, wenn die Option **Jeden Security Server einzeln konfigurieren** verwendet wird.
7. Klicken Sie auf **Weiter**.

   Beachten Sie
   Je nach Ihrer Vorauswahl gelten einige der hier beschriebenen Optionen möglicherweise nicht für Ihre Situation.

8. Geben Sie einen aussagekräftigen Namen für den Security Server ein.

9. Wählen Sie den Container, in den Sie den Security Server aus dem **Container**-Menü einfügen möchten.
10. Wählen Sie den Ziel-Speicherort.
11. Wählen Sie die Art der Speicherzuweisung. Für die Installation der Appliance wird die klassische Speicherzuweisung empfohlen.

    Wichtig
    Wenn bei Verwendung der schlanken Speicherzuweisung der Speicherplatz knapp wird, hängt sich die Security Server auf, wodurch der Host nicht mehr geschützt ist.

12. Konfigurieren Sie die Speicher- und CPU-Ressourcenzuteilung je nach VM-Konsolidierungsrate auf dem Host. Wählen Sie **Gering**, **Mittel** oder **Hoch**, um die empfohlenen Einstellungen für die Ressourcenzuteilung zu laden, oder **Manuell**, um die Ressourcenzuteilung manuell zu konfigurieren.
13. Legen Sie die Zeitzone der Appliance fest.
14. Vergeben Sie ein Administrator-Password für die Security Server -Konsole. Wenn Sie ein Administratorpasswort festlegen, setzt dieses das Standard-Root-Passwort ("sve") außer Kraft.
15. Wählen Sie die Netzwerkkonfigurationsart für das Bitdefender-Netzwerk. Die IP-Adresse des Security Server darf im Laufe der Zeit nicht geändert werden, da sie von Linux-Agenten zur Kommunikation verwendet wird.

    Wenn Sie DHCP wählen, konfigurieren Sie den DHCP-Server so, dass er eine IP-Adresse für die Appliance reserviert.

    Wenn Sie die Option "statisch" wählen, müssen Sie IP-Adresse, Subnetz-Maske, Gateway und DNS eingeben.

16. Klicken Sie auf **Speichern**.

Auf der Seite **Netzwerk > Aufgaben** können Sie Aufgaben anzeigen und verwalten.

HVI Ergänzungspaket installieren

1. Gehen Sie zur Seite **Konfiguration > Update**.
2. Wählen Sie das HVI-Ergänzungspaket in der Liste **Komponenten** aus und klicken Sie das Feld **Download** oben in der Tabelle an.

3. Gehen Sie zur Seite **Netzwerk** und wählen Sie in der Auswahlliste **Virtuelle Maschinen**.
4. Wählen Sie nun im Menu **Ansichten** auf der linken Seite **Server** aus.
5. Wählen Sie einen oder mehrere Xen-Hosts aus dem Netzwerkinventar. Sie können die verfügbaren Hosts ganz einfach über die Option **Typ > Hosts** im Menu **Filter** anzeigen.
6. Klicken Sie das Feld **Aufgaben** auf der rechten Seite an und wählen Sie **HVI Ergänzungspaket installieren**. Das Installationsfenster öffnet sich.
7. Entscheiden Sie, wann die Installation durchgeführt werden soll. Sie können die Installation direkt nach dem Speichern der Aufgabe oder zu einem späteren Zeitpunkt durchführen. Falls die Installation zu der festgelegten Zeit nicht vollständig durchgeführt werden kann, wird der Vorgang automatisch den Einstellungen entsprechend wiederholt. Falls Sie zum Beispiel mehrere Hosts ausgewählt haben und ein Host zum festgelegten Installationszeitpunkt nicht verfügbar ist, wird die Aufgabe zum festgelegten Zeitpunkt wiederholt.
8. Die Übernahme der Änderungen und Abschluss der Installation erfordert einen Neustart des Hosts. Falls der Host unbeaufsichtigt neu starten soll, wählen Sie **Automatischer Neustart Host**.
9. Klicken Sie auf **Speichern**. Eine Bestätigungsmeldung wird angezeigt.

   Auf der Seite **Netzwerk > Aufgaben** können Sie Aufgaben anzeigen und verwalten.

5.8. Speicherschutz installieren

Security for Storage ist ein Bitdefender-Dienst zum Schutz von NAS-Geräten (Network-attached Storage) und Filesharing-Systemen, die das Internet Content Adaptation Protocol (ICAP) unterstützen. Informationen zu unterstützten Filesharing-Systemen finden Sie unter „Speicherschutz“ (S. 57).

So verwenden Sie Security for Storage in Kombination mit Ihrer GravityZone-Lösung:

1. Installieren und konfigurieren Sie mindestens zwei Security Server in Ihrer Umgebung als ICAP-Server. Bitdefender Security Server analysieren Dateien, senden Ergebnisse an Speichersysteme und führen bei Bedarf entsprechende Aktionen durch. Bei Überlastung leitet der erste Security Server die übrigen Daten an den zweiten weiter.

Beachten Sie
Wir empfehlen, Security Server, die dem Speicherschutz dienen, getrennt von Security Servern zu installieren, die für andere Rollen wie Malware-Scans eingesetzt werden.

Details zur Installation von Security Servern finden Sie in diesem Handbuch unter **Security Server installieren**.

2. Konfigurieren Sie das Modul **Speicherschutz** über die GravityZone-Richtlinieneinstellungen.

   Nähere Informationen finden Sie unter **Sicherheitsrichtlinien > Richtlinien für Computer und virtuelle Maschinen > Speicherschutz** im GravityZone-Administratorhandbuch.

Details zur Konfiguration und Verwaltung von ICAP-Servern auf bestimmten NAS-Geräten oder Filesharing-Systemen entnehmen Sie bitte der Dokumentation der entsprechenden Plattform.

5.9. Mobilgeräteschutz installieren

Security for Mobile ist eine Lösung zur Verwaltung mobiler Geräte für iPhones, iPads und Android-Geräte. Eine vollständige Liste der unterstützten Betriebssystemversionen finden Sie unter Systemanforderungen.

Damit Sie Security for Mobile vom Control Center aus verwalten können, müssen Sie Active-Directory-Benutzern oder benutzerdefinierten Benutzern Mobilgeräte hinzufügen und anschließend die App GravityZone Mobile Client auf den Geräten installieren. Nach der Einrichtung können Sie Verwaltungsaufgaben auf Mobilgeräten ausführen.

Bevor Sie loslegen, sollten Sie eine öffentliche (externe) Adresse für den Kommunikationsserver konfigurieren.

So installieren Sie Security for Mobile:

1. Wenn Sie die Integration mit Active Directory nicht benutzen, müssen Sie Benutzer für Eigentümer mobiler Geräte erstellen.
2. Benutzern Geräte hinzufügen.
3. GravityZone Mobile Client auf Geräten installieren und aktivieren.

5.9.1. Externe Adresse für den Kommunikationsserver konfigurieren

In der Standardeinrichtung von GravityZone können mobile Geräte nur verwaltet werden, wenn sie direkt mit dem Unternehmensnetzwerk verbunden sind (über WLAN oder VPN). Der Grund dafür ist, dass mobile Geräte bei der Registrierungen so konfiguriert werden, dass sie eine Verbindung zur lokalen Adresse der Kommunikationsserver-Appliance herstellen.

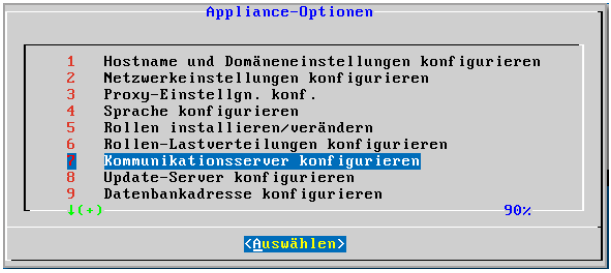
Um mobile Geräte an einem beliebigen Ort über das Internet zu verwalten, müssen Sie eine öffentlich erreichbare Adresse für den Kommunikationsserver konfigurieren.

Zur Verwaltung mobiler Geräte, die nicht mit dem Unternehmensnetzwerk verbunden sind, stehen Ihnen die folgenden Möglichkeiten zur Verfügung:

- Port-Weiterleitung im Unternehmens-Gateway für die Appliance konfigurieren, auf der die Kommunikationsserver-Rolle läuft.
- Einen zusätzlichen Netzwerkadapter zur Appliance, auf der die Kommunikationsserver-Rolle läuft, hinzufügen und ihm eine öffentliche IP-Adresse zuweisen.

In beiden Fällen müssen Sie für den Kommunikationsserver die externe Adresse konfigurieren, die für die Verwaltung mobiler Geräte benutzt werden soll:

1. Greifen Sie über Ihre Virtualisierungsverwaltungs-Software (z. B. vSphere Client) auf die Appliance-Console zu.
2. Wählen Sie aus dem Hauptmenü **Kommunikationsserver konfigurieren**.



Fenster "Anwendungsoptionen"

3. Wählen Sie **Externe Adresse des MDM-Servers konfigurieren**

Fenster "Kommunikationsserver konfigurieren"

4. Geben Sie die externe Adresse ein.

   Verwenden Sie die folgende Syntax: `https://<IP/Domain>:<Port>`.

Fenster für die Eingabe der externen Adresse des MDM-Servers

   - Wenn Sie Port-Weiterleitung verwenden, müssen Sie erstens die öffentliche IP-Adresse oder den Domain-Namen und zweitens den auf dem Gateway offenen Port eingeben.
   - Wenn Sie die öffentliche Adresse des Kommunikationsservers verwenden, müssen Sie erstens die öffentliche IP-Adresse oder oder den Domain-Namen und zweitens den Kommunikationsserver-Port angeben. Der Standard-Port ist `8443`.

5. Wählen Sie **OK**, um die Änderungen zu speichern.

5.9.2. Benutzerdefinierte Benutzer erstellen und organisieren

In Situationen ohne Active Directory müssen Sie zunächst benutzerdefinierte Benutzer erstellen, um eine Möglichkeit zu haben, die Eigentümer von Mobilgeräten zu identifizieren. Angegebene Benutzer mobiler Geräte werden in keiner Weise mit dem Active Directory oder mit anderen im Control Center definierten Benutzern verknüpft.

Benutzerdefinierte Benutzer erstellen

So erstellen Sie einen benutzerdefinierten Benutzer:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Mobilgeräte** aus der Ansichtsauswahl.
3. Wählen Sie im linken Fenster **Benutzerdefinierte Gruppen**.
4. Klicken Sie auf das Symbol **Benutzer hinzufügen** in der Symbolleiste. Ein Konfigurationsfenster wird sich öffnen.
5. Geben Sie die Informationen des gewünschten Benutzers an:
   - Einen aussagekräftigen Benutzernamen (z. B. den vollen Namen des Benutzers)
   - Die E-Mail-Adresse des Benutzers

   Wichtig
   - Vergewissern Sie sich, dass die E-Mail-Adresse gültig ist. Wenn Sie ein Gerät hinzufügen, erhält der Benutzer eine E-Mail mit den Installationsanweisungen.
   - Jede E-Mail-Adresse kann nur zu einem Benutzer gehören.

6. Klicken Sie auf **OK**.

Benutzerdefinierte Benutzer organisieren

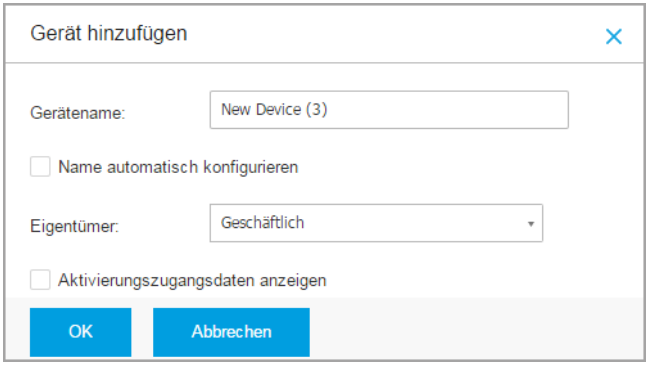
So organisieren Sie benutzerdefinierte Benutzer:

1. Erstellen Sie benutzerdefinierte Gruppen.
   a. Wählen Sie im linken Fenster **Benutzerdefinierte Gruppen**, und klicken Sie auf das Symbol **Hinzufügen** in der Symbolleiste (über dem Fenster).
   b. Geben Sie einen aussagekräftigen Namen für die Gruppe ein, und klicken Sie auf **OK** Die neue Gruppe wird jetzt unter **Benutzerdefinierte Gruppen** angezeigt.
2. Verschieben Sie benutzerdefinierte Benutzer in entsprechende benutzerdefinierte Gruppen.
   a. Wählen Sie im rechten Fenster die Benutzer.
   b. Verschieben Sie Ihre Auswahl per Drag und Drop in die gewünschte Gruppe im linken Fenster.

5.9.3. Benutzern Geräte hinzufügen

So fügen Sie einem Benutzer ein Gerät hinzu:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Mobilgeräte** aus der Ansichtsauswahl.
3. Suchen Sie den Benutzer in den Active-Directory-Ordnern oder in benutzerdefinierten Gruppen.
4. Klicken Sie auf das Symbol ⊕ **Gerät hinzufügen** am oberen Rand der Netzwerktabelle. Ein Konfigurationsfenster wird sich öffnen.



Ein Mobilgerät für einen Benutzer hinzufügen

5. Geben Sie einen aussagekräftigen Namen für das Gerät ein.
6. Mit der Option **Name automatisch konfigurieren** wird der Gerätename automatisch generiert. Nach dem Hinzufügen erhält das Gerät einen generierten Namen. Sobald das Gerät aktiviert ist, wird es automatisch mithilfe der entsprechenden Hersteller- und Modell-Informationen umbenannt.
7. Wählen Sie den Eigentümertyp des Geräts (geschäftlich/enterprise oder privat).
8. Wählen Sie die Option **Aktivierungszugangsdaten anzeigen** aus, nachdem Sie auf **OK** geklickt haben, wenn Sie den GravityZone Mobile Client auf dem Gerät des Benutzers installieren möchten.
9. Klicken Sie auf **OK**. Es wird sofort eine E-Mail an den Benutzer gesendet, die Installationsanweisungen und Aktivierungsdetails für das Gerät enthält. Die

Aktivierungsdetails enthalten das Aktivierungs-Token und die Adresse des Kommunikationsservers (und den entsprechenden QR-Code).

Beachten Sie

- Sie können die Aktivierungsdetails eines Geräts jederzeit einsehen, indem Sie im Control Center auf seinen Namen klicken.
- Sie können auch einer Auswahl an Benutzern und Gruppen mobile Geräte hinzufügen. In diesem Fall können Sie im Konfigurationsfenster nur die Eigentümer der Geräte definieren. Mobile Geräte, die durch eine Mehrfachauswahl erstellt wurden, erhalten standardmäßig einen generischen Namen. Sobald ein Gerät registriert ist, ändert sich sein Name automatisch; ebenso die Hersteller- und Modell-Einträge.

5.9.4. GravityZone Mobile Client auf Geräten installieren

Die Anwendung GravityZone Mobile Client wird ausschließlich über den Apple App Store und Google Play vertrieben.

So installieren Sie GravityZone Mobile Client auf einem Gerät:

1. Suchen Sie die Anwendungen im offiziellen App-Store.
   - Link zu Google Play
   - Link zum Apple App Store
2. Laden Sie die Anwendung herunter, und installieren Sie sie auf dem Gerät.
3. Starten Sie die Anwendung, und nehmen Sie die nötige Konfiguration vor:
   a. Tippen Sie auf Android-Geräten auf **Aktivieren**, um GravityZone Mobile Client als Geräteadministrator zu aktivieren. Lesen Sie die Informationen gründlich durch.

      Beachten Sie

      - Die Sperraufgaben für Android-Geräte (ab 7.0) erzwingen die Eingabe des über Ihre GravityZone-Konsole festgelegten Passworts nur dann, wenn auf dem Gerät kein Sperrschutz konfiguriert wurde. Andernfalls werden die bestehenden Optionen zum Sperren des Bildschirms wie Muster, PIN, Passwort, Fingerabdruck oder Smart Lock zum Schutz des Gerätes verwendet.
      - Die Entsperraufgabe ist für Android-Geräte (ab 7.0) nicht mehr verfügbar.

- Aus technischen Gründen stehen die Sperr- und Löschaufgaben unter Android 11 nicht zur Verfügung.

b. Geben Sie das Aktivierungs-Token und die Adresse des Kommunikationsservers ein, oder scannen Sie den QR-Code in der E-Mail ein.

c. Tippen Sie auf **Vertrauen**, wenn Sie aufgefordert werden, das Zertifikat für den Kommunikationsserver zu akzeptieren. So kann der GravityZone Mobile Client den Kommunikationsserver verifizieren und akzeptiert nur Nachrichten von diesem Kommunikationsserver. So können so genannte Man-in-the-Middle-Angriffe verhindert werden.

d. Tippen Sie auf **Aktivieren**.

e. Auf iOS-Geräten werden Sie aufgefordert, das MDM-Profil zu installieren. Wenn ihr Gerät passwortgeschützt ist, werden Sie aufgefordert, das Passwort einzugeben. Sie müssen GravityZone zudem den Zugriff auf Ihre Geräteeinstellungen gewähren, da der Installationsvorgang sonst zum vorherigen Schritt zurückspringt. Folgen Sie den Anweisungen auf Ihrem Bildschirm, um die Profilinstallation abzuschließen.

Beachten Sie
Damit die Ortungsfunktion richtig funktioniert, müssen die Standortdaten im Hintergrund immer aktiviert sein, nicht nur wenn die App verwendet wird.

5.10. Installieren von Report-Builder

Mit dem Report-Builder können Sie Abfragen und detaillierte abfragebasierte Berichte in GravityZone erstellen und verwalten.

Der Report Builder besteht aus zwei Rollen, Datenbank und Prozessoren, die in der GravityZone Virtual Appliance enthalten sind und getrennt voneinander und von anderen GravityZone-Rollen installiert werden müssen. Nach der Installation von Report Builder sollten in Ihrer GravityZone-Umgebung mindestens drei Instanzen der GravityZone Virtual Appliance laufen:

- Eine oder mehrere GravityZone-Appliances, auf der/denen alle Rollen installiert sind außer Report-Builder-Datenbank und Report-Builder-Prozessoren.
- Eine Instanz der GravityZone Virtual Appliance mit der Report-Builder-Datenbankrolle.

- Eine Instanz der GravityZone Virtual Appliance mit der Report-Builder-Prozessorenrolle.

Um eine problemlose Installation zu ermöglichen, müssen Sie zunächst sicherstellen, dass Ihre virtuellen Umgebungen die Hardware- und Softwareanforderungen erfüllen. Dann halten Sie Folgendes bereit:

- Ein Image einer GravityZone Virtual Appliance, mit dem Sie die Report-Builder-Datenbank- und -Prozessorenrollen installieren.
- DNS-Name oder IP-Adresse der GravityZone Virtual Appliance, auf der die GravityZone-Datenbankrolle installiert ist.
- Benutzername und Passwort eines Domain-Administrators.
- Das Passwort für die GravityZone-Datenbank. Falls Sie das Passwort vergessen, können Sie in der Konsolenoberfläche der Appliance für GravityZone ein neues definieren.

Die Installation von Report-Builder erfolgt in zwei Stufen:

- Installieren der Rolle 'Datenbank' für Report-Builder
- Installieren der Rolle 'Verarbeitung' für Report-Builder

Am besten ist es, wenn Sie zunächst GravityZone installieren und dann Control Center einrichten (sofern erforderlich). Aktualisieren Sie anschließend GravityZone, installieren Sie den Schutz an den Endpunkten und abschließend die Report-Builder-Rollen.

Wichtig
Es muss erst die Report-Builder-Datenbankrolle installiert werden und danach die Report-Builder-Prozessorenrolle.

5.10.1. Installieren der Rolle 'Datenbank' für Report-Builder

Report-Builder-Datenbank ist die erste Rolle, die Sie installieren müssen. So installieren Sie diese Rolle:

1. Importieren Sie die GravityZone Virtual Appliance in Ihre virtuelle Umgebung.
2. Schalten Sie die Appliance an.
3. Greifen Sie von Ihrem Virtualisierungsverwaltungsprogramm auf die Konsolenoberfläche der GravityZone Virtual Appliance zu.

4. Legen Sie ein Passwort für den eingebauten Systemadministrator `bdadmin` fest.
5. Melden Sie sich mit dem Passwort an, das Sie zum Zugriff auf die Konfigurationsoberfläche der Appliance festgelegt haben. Mithilfe der Pfeiltasten und der `Tabulator`-Taste können Sie durch die Menüs und Optionen navigieren. Drücken Sie die `Eingabetaste`, um eine bestimmte Option auszuwählen.

   Zunächst erscheint die Oberfläche der Appliance in englischer Sprache.

   Sie können die Sprache der Oberfläche wie folgt ändern:
   a. Wählen Sie im Hauptmenü den Punkt **Configure Language**.
   b. Wählen Sie dann eine der angezeigten Sprachen. Eine Bestätigungsmeldung wird angezeigt.

      Beachten Sie
      Um die gewünschte Sprache zu finden, müssen Sie evtl. runter scrollen.

   c. Wählen Sie **OK**, um die Änderungen zu speichern.
6. Gehen Sie zu **Erweiterte Einstellungen**, und wählen Sie **Mit vorhandener Datenbank verbinden**.
7. Geben Sie die IP-Adresse und das Passwort für die GravityZone-Datenbank ein.
8. Wählen Sie im Menü **Erweiterte Einstellungen** die Option **Rollen installieren/deinstallieren**.
9. Gehen Sie zu **Rollen hinzufügen oder entfernen**, und wählen Sie **Report-Builder-Datenbank**. Drücken Sie die `Leertaste`, um diese Rolle zu installieren, und die `Eingabetaste`, um den Vorgang fortzusetzen. Drücken Sie nochmals die `Enter`-Taste, um den Vorgang zu bestätigen, und warten Sie, bis die Installation abgeschlossen ist.

Beachten Sie
Die Report-Builder-Datenbank kann nur als eigenständige Instanz installiert und betrieben werden. Replica-Set-Backups werden nicht unterstützt.

5.10.2. Installieren der Rolle 'Verarbeitung' für Report-Builder

Report-Builder-Prozessoren ist die zweite Rolle, die Sie installieren müssen. So installieren Sie diese Rolle:

1. Importieren Sie die GravityZone Virtual Appliance in Ihre virtuelle Umgebung.

2. Schalten Sie die Appliance an.
3. Greifen Sie von Ihrem Virtualisierungsverwaltungsprogramm auf die Konsolenoberfläche der GravityZone Virtual Appliance zu.
4. Legen Sie ein Passwort für den eingebauten Systemadministrator `bdadmin` fest.
5. Melden Sie sich mit dem Passwort an, das Sie eingerichtet haben. Die Konfigurationsoberfläche der Appliance wird geöffnet. Mithilfe der Pfeiltasten und der `Tabulator`-Taste können Sie durch die Menüs und Optionen navigieren. Drücken Sie die `Eingabetaste`, um eine bestimmte Option auszuwählen.

   Zunächst erscheint die Oberfläche der Appliance in englischer Sprache.

   Sie können die Sprache der Oberfläche wie folgt ändern:
   a. Wählen Sie im Hauptmenü den Punkt **Configure Language**.
   b. Wählen Sie dann eine der angezeigten Sprachen. Eine Bestätigungsmeldung wird angezeigt.

      Beachten Sie
      Um die gewünschte Sprache zu finden, müssen Sie evtl. runter scrollen.

   c. Wählen Sie **OK**, um die Änderungen zu speichern.
6. Gehen Sie zu **Erweiterte Einstellungen**, und wählen Sie **Mit vorhandener Datenbank verbinden**.
7. Geben Sie die IP-Adresse und das Passwort für die GravityZone-Datenbank ein.
8. Wählen Sie im Menü **Erweiterte Einstellungen** die Option **Rollen installieren/deinstallieren**.
9. Gehen Sie zu **Rollen hinzufügen oder entfernen**, und wählen Sie **Report-Builder-Prozessoren**. Drücken Sie die `Leertaste`, um diese Rolle zu installieren, und die `Eingabetaste`, um den Vorgang fortzusetzen. Drücken Sie nochmals die `Enter`-Taste, um den Vorgang zu bestätigen, und warten Sie, bis die Installation abgeschlossen ist.

Beachten Sie
Die Report-Builder-Prozessorenrolle kann nur als eigenständige Instanz installiert und betrieben werden.

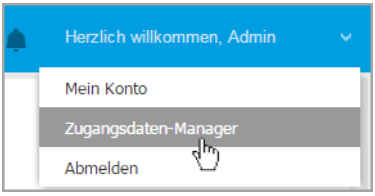
Nach der Installation von Report Builder wird im Bereich **Berichte** von Control Center die neue Menüoption **Abfragen** angezeigt.

Die Rolle 'Datenbank' und die Rolle 'Verarbeitung' für Report-Builder werden zusammen mit den anderen GravityZone-Rollen im Bereich **Infrastruktur** der Seite **Konfiguration > Update** angezeigt.

5.11. Zugangsdaten-Manager

Der Zugangsdaten-Manager hilft Ihnen dabei, die Zugangsdaten festzulegen, die zum Zugriff auf die verfügbaren vCenter-Server-Inventare sowie zur Fernauthentifizierung bei verschiedenen Betriebssystemen in Ihrem Netzwerk benötigt werden.

Um den Zugangsdaten-Manager zu öffnen, klicken Sie auf Ihren Benutzernamen in der rechten oberen Ecke der Seite, und wählen Sie **Zugangsdaten-Manager**.



Das Zugangsdaten-Manager-Menü

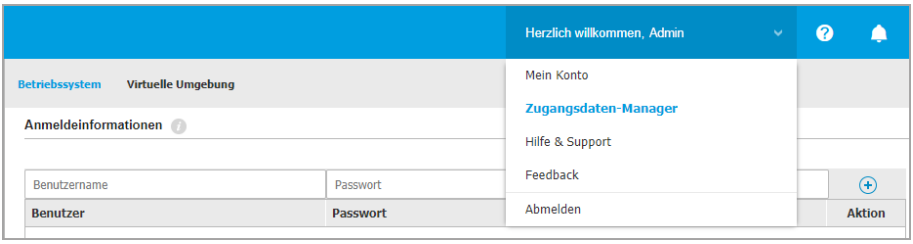
Das Fenster **Zugangsdaten-Manager** hat zwei Reiter:

- Betriebssystem
- Virtuelle Umgebung

5.11.1. Betriebssystem

Im Reiter **Betriebssystem** können Sie die Administrator-Zugangsdaten verwalten, die für die Fernauthentifizierung während der Ausführung von Installationsaufgaben auf Computern und virtuellen Maschinen in Ihrem Netzwerk nötig sind.

So fügen Sie Zugangsdaten hinzu:



Zugangsdaten-Manager

1. Geben Sie in die entsprechenden Felder im oberen Bereich der Tabelle den Namen und das Passwort eines Administratorkontos für jedes der Betriebssysteme ein. Sie können jedem Konto eine Beschreibung hinzufügen, um es später leichter identifizieren zu können. Wenn Computer in einer Domäne sind, reicht es aus, die Anmeldeinformationen des Domänenadministrators einzugeben.

   Bei der Eingabe des Namens eines Nutzerkontos Windows-Konvention verwenden:

   - Für Active Directory-Maschinen wird folgende Syntax verwendet: `username@domain.com` und `Domäne\Benutzername`. Um sicherzugehen, dass die eingegebenen Zugangsdaten funktionieren, geben Sie sie in beiden Ausdrucksweisen ein (`Benutzername@domain.com` und `Domain\Benutzername`).
   - Bei Arbeitsgruppen-Maschinen genügt die Eingabe des Benutzernamens ohne Angabe des Namens der Arbeitsgruppe.

2. Klicken Sie auf die Schaltfläche ⊕ **Hinzufügen** auf der rechten Seite der Tabelle. Die neuen Zugangsdaten werden der Tabelle hinzugefügt.

> **Beachten Sie**
> Wenn Sie die Authentifizierungsdaten noch nicht angegeben haben, müssen Sie diese bei Ausführung von Installationsaufgaben eingeben. Die angegebenen Zugangsdaten werden automatisch im Zugangsdaten-Manager gespeichert, sodass Sie sie beim nächsten Mal nicht mehr eingeben müssen.

5.11.2. Virtuelle Umgebung

Im Reiter Virtuelle Umgebung können Sie die Zugangsdaten für die verfügbaren virtuellen Server-Systeme verwalten.

Um auf die mit dem Control Center integrierte virtuelle Infrastruktur zugreifen zu können, müssen Sie Ihre Benutzerzugangsdaten für jedes verfügbare virtualisierte Server-System angeben. Control Center stellt mithilfe Ihrer Zugangsdaten eine Verbindung zur virtualisierten Infrastruktur her und zeigt nur diejenigen Ressourcen an, auf die Sie Zugriff haben (wie im virtualisierten Server definiert).

So legen Sie die Zugangsdaten fest, die für die Verbindung zu einem virtualisierten Server nötig sind:

1. Wählen Sie den Server aus dem entsprechenden Menü.

   Beachten Sie
   Wenn das Menü nicht verfügbar ist, wurde entweder noch keine Integration konfiguriert oder alle nötigen Zugangsdaten wurden bereits konfiguriert.

2. Geben Sie Ihren Benutzernamen und Ihr Passwort und eine aussagekräftige Beschreibung ein.
3. Klicken Sie auf den Button **Hinzufügen**. Die neuen Zugangsdaten werden der Tabelle hinzugefügt.

   Beachten Sie
   Wenn Sie Ihre Zugangsdaten zur Authentifizierung nicht im Zugangsdaten-Manager konfigurieren, müssen Sie sie angeben, sobald Sie das Inventar irgendeines Virtualisierte-Server-Systems durchsuchen. Wenn Sie Ihre Zugangsdaten einmal eingegeben haben, werden sie im Zugangsdaten-Manager gespeichert, sodass Sie sie beim nächsten Mal nicht mehr eingeben müssen.

   Wichtig
   Wenn Sie Ihr Passwort für Ihren virtualisierten Server ändern, müssen Sie es auch im Zugangsdaten-Manager aktualisieren.

5.11.3. Zugangsdaten aus dem Zugangsdaten-Manager löschen

So löschen Sie obsolete Zugangsdaten aus dem Zugangsdaten-Manager:

1. Bewegen Sie den Mauszeiger zur Tabellenzeile mit den Zugangsdaten, die Sie löschen möchten.
2. Klicken Sie auf die Schaltfläche ⊗ **Löschen** auf der rechten Seite der entsprechenden Tabellenzeile. Das ausgewählte Konto wird gelöscht.

6. AKTUALISIEREN VON GRAVITYZONE

Bitdefender veröffentlicht sämtliche Updates des Produkts oder der Sicherheitsinhalte über die Bitdefender-Server im Internet. Alle Updates sind verschlüsselt und digital signiert, sodass sie nicht verfälscht werden können.

GravityZone beinhaltet eine Update-Server-Rolle, die als zentrale Update-Verteilerstation für Ihre GravityZone-Installation dient. Der Update-Server sucht nach neuen GravityZone-Updates und lädt sie von den Bitdefender-Update-Servern im Internet herunter, wonach sie lokal im Netzwerk zur Verfügung stehen. Die GravityZone-Komponenten können so konfiguriert werden, dass sie automatisch Updates vom lokalen Update-Server, und nicht aus dem Internet beziehen.

Wenn ein neues Update zur Verfügung steht, überprüft die GravityZone-Appliance, der Sicherheitsagent oder der Security Server die digitale Signatur des Updates auf Authentizität und den Inhalt des Pakets auf Unversehrtheit. Anschließend wird jede Update-Datei geparst und ihre Version mit der installierten Datei verglichen. Neuere Dateien werden lokal heruntergeladen und mit ihrem MD5-Hashwert verglichen, um sicher zu gehen, dass sie nicht verändert wurden.

Sobald eine dieser Überprüfungen nicht bestanden wird, wird der Update-Prozess sofort angehalten, und ein Fehler wird ausgegeben. Andernfalls wird das Update als gültig und installationsbereit betrachtet.

Zur Aktualisierung der in Ihrer Umgebung installierten GravityZone-Appliances und der Installationspakete der GravityZone-Komponenten melden Sie sich über ein Unternehmens-Administratorkonto an und öffnen die Seite **Konfiguration > Update**.

6.1. GravityZone-Appliances aktualisieren

Durch Updates der GravityZone-Appliance macht Bitdefender neue Funktionen verfügbar und verbessert bereits verfügbare Funktionen. Diese werden im Control Center angezeigt.

Vor der Durchführung eines Updates sollten Sie Folgendes überprüfen:

- Den Update-Status
- Angezeigte Informationen oder Warnmeldungen.
- Das Änderungsprotokoll

So überprüfen Sie den Update-Status:

1. Öffnen Sie die Seite **Konfiguration > Update > GravityZone-Rollen**.
2. Sehen Sie im Bereich **Aktueller Status** die Meldung über den allgemeinen Status Ihrer Installation ein. Wenn GravityZone aktualisiert werden muss, ist die Schaltfläche **Update** verfügbar.
3. Sehen Sie im Abschnitt **Infrastruktur** die Details zu jeder in Ihrem Netzwerk eingesetzten GravityZone-Rolle ein. Da Rollen unabhängig voneinander aktualisiert werden, können Sie für jede Rolle Folgendes anzeigen: den Namen der Appliance, auf der sie gehostet wird, ihre IP-Adresse, die aktuelle Version, die neueste verfügbare Version und den Aktualisierungsstatus.

So überprüfen Sie das Änderungsprotokoll:

1. Öffnen Sie die Seite **Konfiguration > Update > GravityZone-Rollen**.
2. Klicken Sie auf den Link **Änderungsprotokoll anzeigen**. In einem Pop-up-Fenster wird eine Liste mit allen Versionen und dazugehörigen Änderungen angezeigt.

   Versionshinweise für jede neue Produktversion werden auch im Bitdefender-Support-Center veröffentlicht.

Es gibt zwei Möglichkeiten, ein GravityZone-Update durchzuführen:

- Manuell
- Automatisch

6.1.1. Manuelles Update

Wählen Sie diese Methode, wenn Sie die volle Kontrolle darüber haben möchten, wann das Update durchgeführt werden soll.

Manuelles GravityZone-Update:

1. Öffnen Sie die Seite **Konfiguration > Update > GravityZone-Rollen**.
2. Klicken Sie auf die Schaltfläche **Update** (falls verfügbar).

   Das Update kann einige Zeit in Anspruch nehmen. Bitte warten Sie, bis das Update abgeschlossen ist.
3. Löschen Sie den Browser-Cache.

Während des Updates meldet das Control Center alle Benutzer ab und informiert sie über das laufende Update. Sie können den Fortschritt des Update-Vorgangs im Detail einsehen.

Nach Abschluss des Updates zeigt Control Center die Anmeldeseite an.

6.1.2. Automatisches Update

Durch die automatische Installation von Updates stellen Sie sicher, dass GravityZone stets über die neuesten Funktionen und Sicherheits-Patches verfügt.

GravityZone hat zwei Arten von automatischen Updates:

- Produkt-Updates
- Updates von Drittanbietersoftware

Produkt-Updates

Diese Updates umfassen neue Funktionen in GravityZone und beheben Probleme, die sich aus diesen Funktionen ergeben.

Da Updates GravityZone-Benutzer in ihrer Arbeit stören, sind sie so ausgelegt, dass sie nach einem festgelegten Zeitplan durchgeführt werden. So können Updates zu einem für Sie günstigen Zeitpunkt durchgeführt werden. Automatische Produkt-Updates sind standardmäßig deaktiviert.

So können Sie Produkt-Updates aktivieren und planen:

1. Öffnen Sie die Seite **Konfiguration > Update > GravityZone-Rollen**.
2. Markieren Sie das Kästchen **Automatische GravityZone-Produkt-Updates aktivieren**.
3. Setzen Sie die Schaltfläche **Wiederholung** auf **Täglich**, **Wöchentlich** (wählen Sie einen oder mehrere Wochentage) oder **Monatlich**.
4. **Intervall** festlegen. Sie können einen Zeitpunkt für den Update-Start festlegen, sobald ein neues Update verfügbar ist.

GravityZone zeigt standardmäßig 30 Minuten vor Beginn des automatischen Updates eine Warnmeldung für alle Control Center-Benutzer an. Entfernen Sie das Häkchen im Kästchen **Benachrichtigung 30 Minuten vor dem Update**, um diese Warnung zu deaktivieren.

Updates von Drittanbietersoftware

Die GravityZone-Virtual-Appliance hat verschiedene Softwareprodukte von anderen Anbietern eingebettet. Diese Art Update bietet, sobald wie möglich, Patches für diese Software, um Sicherheitsrisiken so klein wie möglich zu halten.

Diese Updates werden im Hintergrund aufgespielt und behindern die Funktion von und Interaktion mit dem Control Center nicht.

Standardmäßig ist diese Option aktiviert. Wenn Sie die Option deaktivieren möchten, gehen Sie wie folgt vor:

1. Öffnen Sie die Seite **Konfiguration > Update > GravityZone-Rollen**.
2. Entfernen Sie die Markierung des Kästchens **Automatische Sicherheitsupdates für GravityZone-Komponenten von Drittanbietern aktivieren**

   Drittanbieter-Software-Patches werden dann zusammen mit dem GravityZone-Produkt-Update aufgespielt.

6.2. Update-Server konfigurieren

Standardmäßig lädt der Update-Server stündlich Updates aus dem Internet. Wir empfehlen, die Standard-Update-Server-Einstellungen nicht zu verändern.

So überprüfen und konfigurieren Sie die Update-Server-Einstellungen:

1. Gehen Sie zur Seite **Update** in der Control Center und klicken Sie den Reiter **Komponenten** an.
2. Klicken Sie auf das Feld **Einstellungen** oben links auf der Seite; es erscheint das Fenster **Update-Servereinstellungen**.
3. Unter **Update-Serverkonfiguration** können Sie die wichtigsten Einstellungen überprüfen und konfigurieren.
   - **Paketadresse.** Die Adresse, von der Pakete heruntergeladen werden.
   - **Update-Adresse.** Der Update-Server ist so eingerichtet, dass er auf `upgrade.bitdefender.com:80` nach Updates sucht und sie von dort herunterlädt. Dies ist eine generische Adresse, die Sie automatisch zu dem nächsten Server Ihrer Region weiterleitet, der Bitdefender-Updates gespeichert hat.
   - **Schnittstelle.** Diesen Port müssen Sie angeben, wenn Sie die verschiedenen GravityZone-Komponenten so konfigurieren, dass sie Updates vom Update-Server beziehen. Der Standard-Port ist `7074`.
   - **IP.** IP-Adresse des Update-Servers.
   - **Update-Intervall (Stunden).** Wenn Sie den Update-Zeitraum ändern möchten, geben Sie in diesem Feld einen neuen Wert ein. Der Standardwert ist 1.
4. Sie können den Update-Server so einstellen, dass Security Server und Endpunktkits automatisch heruntergeladen werden.

5. Der Update-Server kann als Gateway für Daten dienen, die von im Netzwerk installierten Bitdefender-Client-Produkten an den Bitdefender-Server gesendet werden. Diese Daten können anonyme Berichte über Virusaktivität und Produktabstürze sowie Daten für die Online-Registrierung enthalten. Die Gateway-Rollen zu aktivieren, ist zur Steuerung des Datenverkehrs und bei Netzwerken ohne Internetzugang sinnvoll.

   Beachten Sie
   Sie können die Produktmodule, die statistische oder Absturzdaten an die Bitdefender-Labors senden, jederzeit deaktivieren. Zur Fernsteuerung dieser Optionen auf den von Control Center verwalteten Computern und virtuellen Maschinen können Sie Richtlinien verwenden.

6. Klicken Sie auf **Speichern**.

6.3. Neuste Produkt-Updates laden

Informationen zu bestehenden GravityZone-Komponentenpaketen finden Sie unter **Komponenten**. Angezeigt werden Informationen wie aktuelle Version, Update-Version (sofern zutreffend) und der Status von Update-Vorgängen, die Sie gestartet haben.

So aktualisieren Sie eine GravityZone-Komponente:

1. Gehen Sie zur Seite **Update** in der Control Center und klicken Sie den Reiter **Komponenten** an.
2. Komponenten, die aktualisiert werden sollen, in der Liste **Produkt** anklicken. Alle vefügbaren Versionen werden in der Tabelle **Pakete** angezeigt. Markieren Sie das Kästchen der Version, die Sie herunterladen möchten.

   Beachten Sie
   Neue Pakete haben den Status **Nicht heruntergeladen** . Sobald Bitdefender eine neuere Version herausgibt, wird die älteste nicht heruntergeladene Version aus der Tabelle entfernt.

3. Klicken Sie auf **Aktionen** oben in der Tabelle und dann auf **Veröffentlichen**. Die ausgewählte Version wird heruntergeladen und der Status entsprechend geändert. Laden Sie den Tabelleninhalt neu, indem Sie auf die Schaltfläche **Neu laden** klicken. Überprüfen Sie anschließend den entsprechenden Status.

Wichtig
Standardmäßig enthält die GravityZone-Appliance nicht die Security Server-Pakete. Sie müssen die für Ihre Umgebung nötigen Security Server-Pakete manuell herunterladen.

6.4. Staging von Updates

Staging ermöglicht Ihnen das Testen neuer Kits oder Produkt-Updates in einer abgeschlossenen, kontrollierten Umgebung, bevor diese im Netzwerk veröffentlicht werden. Die Stagingumgebung sollte das Produkt zu Testzwecken so genau wie möglich spiegeln. So können Sie mögliche Probleme in Ihrer Umgebung noch vor der Produktivsetzung erkennen.

Mit der Stagingfunktion können Sie eine Richtlinie für die kritischen Endpunkte der Produktionsumgebung erstellen. Sie können diese Endpunkte erst aktualisieren, wenn die Updates in der Stagingumgebung und auf den unkritischen Maschinen der Produktionsumgebung getestet wurden. Weitere Informationen finden Sie unter „Veröffentlichen von Updates in einem Update-Ring“ (S. 208).

Beachten Sie

- Staging ist standardmäßig deaktiviert.
- Security Server (VMware mit NSX) unterstützt Staging nicht.
- Staging wird von BEST for Windows Legacy nicht unterstützt. Die Legacy-Endpunkte in der Stagingumgebung müssen in die Produktionsumgebung verschoben werden.

6.4.1. Vorbereitende Maßnahmen

Für den Stagingmodus muss die GravityZone-Infrastruktur die folgenden Bedingungen erfüllen:

- Der Update-Server muss auf der virtuellen Appliance allein installiert sein.

  Gehen Sie folgendermaßen vor, falls der Update-Server gemeinsam mit weiteren Rollen auf der Appliance installiert wurde:

  1. Löschen Sie die alte Update-Server-Rolle.
  2. Stellen Sie eine neue GravityZone-Appliance bereit.

     Wichtig
     Installieren Sie noch keine Rollen.

3. Verbinden Sie die neue Appliance mit der vorhandenen GravityZone-Datenbank.
4. Installieren Sie die Rolle Update-Server auf der neuen Appliance.

Weitere Informationen zur Installation der GravityZone-Rolle finden Sie unter „Die GravityZone-Appliance verwalten“ (S. 111).

- Die Update-Server-Appliance muss mindestens 120 GB haben.
- Die Web-Konsole-Appliance muss mindestens 120 GB haben.

6.4.2. Verwenden der Stagingfunktion

Zum Einrichten der Stagingumgebung und zum Testen der aktuellen Updates ist Folgendes erforderlich:

1. Aktivieren Sie Staging, und legen Sie die Einstellungen für den Update-Server fest.
2. Definieren Sie eine Stagingrichtlinie für die Test-Endpunkte.
3. Installieren Sie die Pakete auf den Test-Endpunkten.
4. Weisen Sie den Testendpunkten die Stagingrichtlinie zu.
5. Aktualisieren Sie die Testendpunkte mit der aktuellen Version, und testen Sie das Update in der Stagingumgebung.
6. Führen Sie einen zweiten Test durch, bevor Sie alle Endpunkte der Produktionsumgebung aktualisieren. Sie können das Update zunächst auf den unkritischen Endpunkten testen.

Aktivieren der Stagingfunktion

So können Sie den Stagingmodus für GravityZone-Updates aktivieren:

1. Gehen Sie zur Seite **Konfiguration** > **Update**, und klicken Sie auf den Reiter **Komponenten**.
2. Klicken Sie auf das Feld **Einstellungen** oben links auf der Seite; es erscheint das Fenster **Update-Servereinstellungen**.
3. Markieren Sie das Kästchen **Bereitstellung aktivieren**.
4. Unter **Produktion-Server-Konfiguration** konfiguren Sie die Haupteinstellungen:

- **Paketadresse.** Download-Adresse für Pakete:`download.bitdefender.com/SMB/Hydra/release`
- **Update-Adresse.** Download-Adresse für Produkt-Updates:`upgrade.bitdefender.com:80`.
- **Schnittstelle.** Der Standard-Port ist `7074`. Sie können dieses Feld nicht bearbeiten.
- **IP.** IP-Adresse des Update-Servers. Sie können dieses Feld nicht bearbeiten.
- **Update-Intervall (Stunden).** Wenn Sie den Update-Zeitraum ändern möchten, geben Sie in diesem Feld einen neuen Wert ein. Der Standardwert ist 1.

5. Der Produktions- und der Update-Server können als Gateways für Daten dienen, die von im Netzwerk installierten Bitdefender-Client-Produkten an die Bitdefender-Server gesendet werden. Diese Daten können anonyme Berichte über Virusaktivität und Produktabstürze sowie Daten für die Online-Registrierung enthalten. Die Gateway-Rollen zu aktivieren, ist zur Steuerung des Datenverkehrs und bei Netzwerken ohne Internetzugang sinnvoll.

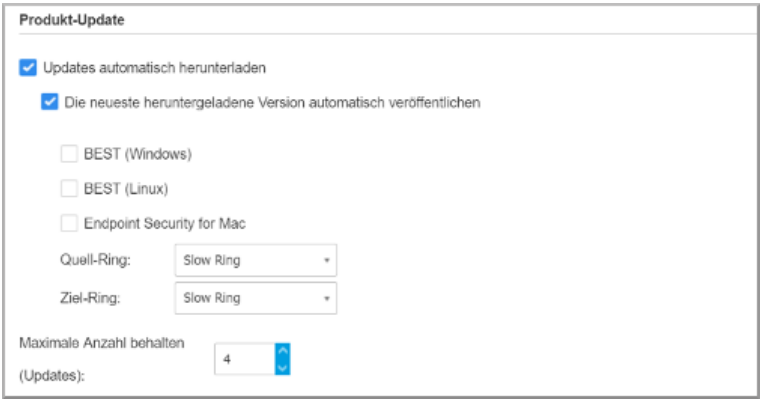
   Beachten Sie
   Sie können die Produktmodule, die statistische oder Absturzdaten an die Bitdefender-Labors senden, jederzeit deaktivieren. Zur Fernsteuerung dieser Optionen auf den von Control Center verwalteten Computern und virtuellen Maschinen können Sie Richtlinien verwenden.

6. Unter **Konfiguration des Bereitstellungsservers** können Sie die folgenden Optionen konfigurieren:
   - **Schnittstelle.** Der Standard-Port ist `7077`.
   - **IP.** IP-Adresse des Update-Servers. Sie können dieses Feld nicht bearbeiten.
7. Unter **Pakete** können Sie den Update-Server so konfigurieren, dass Security Server- und Endpunkt-Kits automatisch heruntergeladen und veröffentlicht werden.

Pakete – Automatische Veröffentlichung

Sie können auch die maximale Anzahl der auf der GravityZone-Appliance zu speichernden Kits einstellen. Geben im Menü **(Kits) maximal** Sie eine Zahl zwischen 4 und 10 ein.

8. Unter **Produkte Update** können Sie den Update Server so einstellen, dass Updates für den Sicherheitsagenten automatisch heruntergeladen werden.



Pakete – Automatische Veröffentlichung

Sie können auch festlegen, dass die frisch heruntergeladenen Versionen automatisch veröffentlicht werden:

a. Wählen Sie in der Liste mindestens einen Sicherheitsagenten aus.

b. Legen Sie den Quell-Ring und den Ziel-Ring fest:

- **Quell-Ring**. Der Ring, in dem die Updates an die Bereitstellungsumgebung versendet werden. Wenn eine Version von den Erstanwendern validiert wurde, wird er im Slow Ring veröffentlicht. Dies ist der Standardwert. Die neuesten Updates werden im Fast Ring veröffentlicht.
- **Ziel-Ring**. Der Ring, in dem die Updates in der Produktionsumgebung veröffentlicht werden. Sie haben die Auswahl zwischen Fast Ring und Slow Ring.

Sie können die maximale Anzahl der auf der GravityZone-Appliance zu speichernden Updates einstellen. Geben im Menü **(Updates) maximal** eine Zahl zwischen 4 und 10 ein.

9. Klicken Sie auf **Speichern**.

Wenn Sie die Bereitstellung aktiviert haben, können Sie Ihre Bereitstellungsumgebung zum Testen der verfügbaren Produkt-Kits und Updates einrichten.

Wichtig
Wenn sie Bereitstellung deaktivieren, werden alle unveröffentlichten Pakete und Produkt-Updates gelöscht.

Definieren der Bereitstellungsrichtlinie

Sie müssen eine Bereitstellungsrichtlinie definieren:

1. Gehen Sie zur **Richtlinien**-Seite.
2. Eine Richtlinie für die Testumgebung aussuchen oder erstellen
3. Im Bereich **Allgemein** > **Update** wird die Adresse des Bereitstellungsservers in die Tabelle **Update-Server** eingegeben.
4. Konfigurieren Sie die weiteren Richtlinieneinstellungen nach Bedarf. Weitere Einzelheiten entnehmen Sie dem Kapitel **Sicherheitsrichtlinien** des GravityZone-Administratorhandbuchs.
5. Klicken Sie auf **Speichern**.

Bereitstellungspakete

So installieren Sie das aktuelle Paket auf den Test-Endpunkten:

1. Gehen Sie zur Seite **Konfiguration > Update** und öffnen Sie den Reiter **Komponenten**.
2. Zur Anzeige der aktuellsten Produktversion klicken Sie **Updates suchen**.
3. Komponenten, die aktualisiert werden sollen, in der Liste **Produkt** anklicken.
4. Wählen Sie in der Tabelle **Pakete** das Paket, das Sie testen wollen. Sie können für jedes Produkt mehrere Kits herunterladen, jedoch maximal so viele, wie in den **Update-Server-Einstellungen** festgelegt ist. Sobald diese Grenze erreicht ist, wird die älteste Version aus der Tabelle gelöscht.
5. Um das Paket auf Ihre GravityZone-Appliance zu laden, klicken Sie **Aktionen** an und öffnen Sie **Download**.
6. Wenn Sie ein Paket gewählt haben, klicken Sie **Speichern** an. Das Fenster Paketkonfiguration öffnet sich.
7. Paket konfigurieren. Weitere Informationen finden Sie unter „Installationspakete erstellen“ (S. 146).
8. Installieren Sie das Kit auf den Test-Endpunkten.
9. Verhalten der Endpunkte überwachen.
10. Nach erfolgreicher Installation eines Pakets und bei normalem Verhalten der Endpunkte kann das Paket im Produktionsnetzwerk veröffentlicht werden.

    Zur Veröffentlichtung des Pakets öffnen Sie es in der Tabelle **Pakete**, klicken Sie auf **Aktionen** oben in der Tabelle und wählen Sie **Veröffentlichen**.

    Wichtig
    Sie können keine Pakete veröffentlichen, die älter sind, als das bereits veröffentlichte.

11. Wenn Sie bei der Handhabung eines Pakets auf Probleme stoßen, können Sie ein Support-Ticket erstellen. Weitere Informationen finden Sie unter „Hilfe erhalten“ (S. 230).

    Zum Löschen des Pakets aus der GravityZone-Appliance klicken Sie **Aktionen** und öffnen Sie **Löschen**.

Zuweisen der Bereitstellungsrichtlinie

So weisen Sie den Test-Endpunkten die Bereitstellungsrichtlinie zu:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Computer und virtuelle Maschinen** aus der Ansichtsauswahl.
3. Wählen Sie die gewünschte Gruppe aus dem linken Fenster. Alle Computer der ausgewählten Gruppe werden in der Tabelle im rechten Fenster angezeigt.
4. Markieren Sie das Kästchen des gewünschten Computers bzw. der gewünschten Gruppe. Sie können auch mehrere Objekte auswählen, diese müssen dann jedoch Objekte desselben Typs und von derselben Ebene sein.
5. Klicken Sie auf die Schaltfläche **Richtlinie zuweisen** am oberen Ende der Tabelle.
6. Nehmen Sie im Richtlinien-Zuweisungsfenster die erforderlichen Einstellungen vor. Weitere Einzelheiten entnehmen Sie dem Abschnitt **Sicherheitsrichtlinien > Verwalten von Richtlinien > Zuweisen von Richtlinien zu Endpunkten** des GravityZone-Administratorhandbuchs.

Bereitstellungs-Produkt-Updates

So installieren Sie die aktuellen Updates:

1. Gehen Sie zur Seite **Konfiguration > Update** und öffnen Sie den Reiter **Komponenten**.
2. Zur Anzeige der aktuellsten Produkt-Updates öffnen Sie **Updates suchen** .
3. Wählen Sie ein beliebiges Bitdefender-Produkt aus der Liste **Produkt**.

   Beachten Sie
   Bereitstellung (Staging) kann nur mit Updates für Sicherheitsagenten, nicht aber für Security Server verwendet werden.

4. Wählen Sie aus der Tabelle **Updates** das Update, das Sie testen wollen.
5. Um das Update auf Ihre GravityZone-Appliance zu laden, klicken Sie **Aktionen** an und öffnen Sie **Download**.

   Sie können für jedes Produkt mehrere Updates herunterladen, jedoch maximal so viele, wie in den **Update-Server-Einstellungen** festgelegt ist. Sobald diese Grenze erreicht ist, wird die älteste Version aus der Tabelle gelöscht.

6. Nach Auswahl eines Updates erst **Aktionen** und dann **Zur Bereitstellung hinzufügen** anklicken. Das Update wird, wie in den Richtlinieneinstellungen vorgegeben, an den Test-Endpunkten installiert. Weitere Informationen finden Sie unter „Definieren der Bereitstellungsrichtlinie“ (S. 205).
7. Wenn das Update erfolgreich installiert wurde und die Endpunkte ein normales Verhalten zeigen, können Sie das Update an die Maschinen in der Produktionsumgebung versenden. Installieren Sie zunächst als zweiten Test das Update auf den unkritischen Maschinen, bevor Sie die kritischen Endpunkte aktualisieren. Weitere Informationen finden Sie unter „Veröffentlichen von Updates in einem Update-Ring“ (S. 208).
8. Wenn Sie bei der Handhabung eines Updates auf Probleme stoßen, können Sie ein Support-Ticket erstellen. Weitere Informationen finden Sie unter „Hilfe erhalten“ (S. 230).

   Zum Löschen eines nicht veröffentlichten Updates von der GravityZone-Appliance klicken Sie auf **Aktionen** und dann auf **Löschen**. Nur noch nicht veröffentlichte Updates können gelöscht werden.

Veröffentlichen von Updates in einem Update-Ring

Damit Sie das Update auf den unkritischen Endpunkten der Produktionsumgebung testen können, müssen Sie zunächst die vorhandenen Richtlinien bearbeiten und ihnen eine Fast Ring-Richtlinie zuweisen.

Beachten Sie
Allen von Ihnen erstellten Richtlinien wird automatisch eine Slow Ring-Richtlinie zugewiesen.

1. Gehen Sie zur **Richtlinien**-Seite.
2. Bearbeiten Sie die Richtlinieneinstellung für die unkritischen Endpunkte in der Produktionsumgebung. Wählen Sie im Bereich **Update-Ring** die Einstellung **Fast Ring**.

   Beachten Sie
   Ein im Fast Ring veröffentlichtes Update darf nicht älter sein als das im Slow Ring veröffentlichte Update.

3. Veröffentlichen Sie das Update im Fast Ring:

a. Gehen Sie zur Seite **Konfiguration** > **Update**, und öffnen Sie den Reiter **Komponenten**.

b. Wählen Sie in der Tabelle 'Updates' ein Update aus, klicken Sie auf **Aktionen** oben in der Tabelle, und wählen Sie **Veröffentlichen**.

c. Wählen Sie die Option 'Fast Ring'.

> **Beachten Sie**
> Direkt nach der Veröffentlichung eines Updates steht dieses im Fast Ring und im Slow Ring zur Verfügung.

Zu diesem Zeitpunkt werden alle Endpunkte mit Fast Ring-Richtlinie mit der veröffentlichten Version aktualisiert.

4. Achten Sie auf das Verhalten der im Fast Ring aktualisierten Endpunkte.
5. Nach erfolgreicher Installation eines Updates und bei normalem Verhalten der Endpunkte kann das Update dann auch im Slow Ring veröffentlicht werden.

a. Gehen Sie zur Seite **Konfiguration** > **Update**, und öffnen Sie den Reiter **Komponenten**.

b. Wählen Sie in der Tabelle 'Updates' ein Update aus, klicken Sie auf **Aktionen** oben in der Tabelle, und wählen Sie **Veröffentlichen**.

c. Wählen Sie die Option 'Slow Ring'.

Jeder Endpunkt der Produktionsumgebung wird nun mit der von Ihnen veröffentlichten Version aktualisiert.

6. Wenn Sie bei der Handhabung eines Pakets auf Probleme stoßen, können Sie ein Support-Ticket erstellen. Weitere Informationen finden Sie unter „Hilfe erhalten“ (S. 230).

6.5. Offline-Produkt-Updates

GravityZone nutzt standardmäßig ein Internet-basiertes Update-System. Für isolierte Netzwerke bietet Bitdefender ein alternatives Update-Verfahren, bei dem die Komponenten und Sicherheitsinhalte auch offline zur Verfügung gestellt werden.

6.5.1. Vorbereitende Maßnahmen

Für Offline-Updates benötigen Sie Folgendes:

- Eine in einem Netzwerk mit Internet-Zugang installierte GravityZone-Instanz („Online-Instanz“). Die Online-Instanz muss Folgendes haben:
  - direkten Internetzugang
  - Zugriff auf die Ports 80 und 443. Näheres zu den von GravityZone genutzten Ports erfahren Sie in diesem Artikel.
  - nur die Datenbank- und Update-Server-Rollen installiert
- Eine oder mehrere in einem Netzwerk ohne Internet-Zugang installierte GravityZone-Instanzen („Offline-Instanzen“).
- Beide GravityZone-Instanzen müssen dieselbe Appliance-Version haben.

6.5.2. Einrichten der GravityZone-Online-Instanz

Während dieser Phase werden Sie eine GravityZone-Instanz in einem Netzwerk mit Internetzugang installieren und sie dann so konfigurieren, dass sie als Offline-Update-Server fungiert.

1. Installieren Sie GravityZone auf einer Maschine mit Internetverbindung.
2. Installieren Sie nur die Datenbank- und die Update-Server-Rolle.
3. Greifen Sie auf das TTY-Terminal der Maschine in Ihrer virtuellen Umgebung zu (oder stellen Sie eine Verbindung zum Terminal über SSH her).
4. Melden Sie sich als Benutzer `bdadmin` und dem von Ihnen eingerichteten Passwort an.
5. Verschaffen Sie sich **Root**-Rechte, indem Sie den Befehl `sudo su` ausführen.
6. Führen Sie die folgenden Befehle aus, um das `gzou-mirror`-Offline-Paket zu installieren:

```
# apt update # gzcli update # apt install gzou-mirror
```

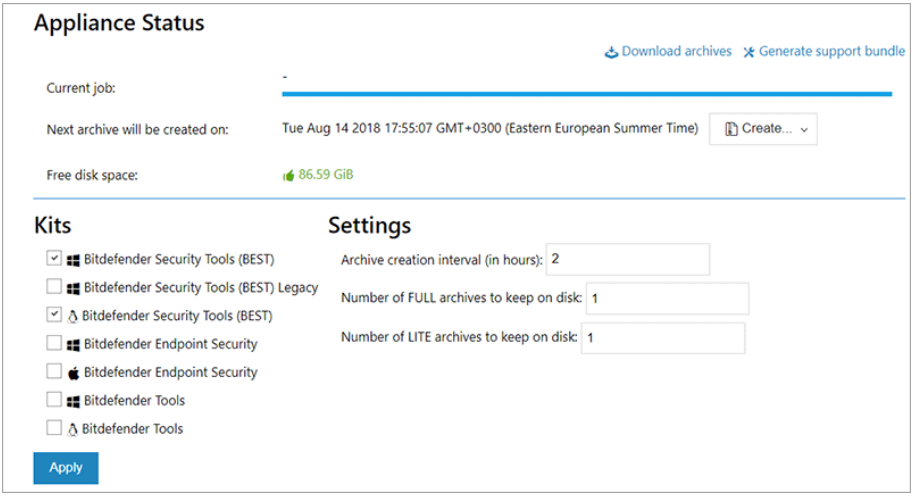
Der `gzou-mirror` hat die folgenden Rollen:

- Konfigurieren Sie den Update-Server so, dass er automatisch Offline-Update-Archive erzeugt.
- Richten Sie auf der Online-Instanz einen Web-Dienst ein, der Konfigurations- und Download-Optionen für die Offline-Update-Archive bereitstellt.

6.5.3. Konfiguration und Download der Erst-Update-Dateien

In dieser Phase werden Sie mithilfe des auf der Online-Instanz installierten Web-Diensts die Update-Archiv-Einstellungen konfigurieren und dann die für die Einrichtung der Offline-Instanz nötigen Archivdateien erstellen. Danach müssen Sie die Update-Dateien herunterladen und auf einem Wechseldatenträger speichern.

1. Auf den Web-Dienst greifen Sie über eine URL der folgenden Form zu: `https://Online-Instanz-Update-Server-IP-oder-Hostname`, mit dem Benutzernamen `bdadmin` und dem von Ihnen festgelegten Passwort.



Die Online-Instanz - Web-Dienst

2. Konfigurieren Sie das Offline-Update-Archiv wie folgt:
   - Wählen Sie unter **Kits** die Endpunkt-Agenten-Kits, die im Offline-Update-Archiv enthalten sein sollen.
   - Nehmen Sie unter **Einstellungen** die gewünschten Anpassungen für Ihr Update-Archiv vor.

     Ein auf der Online-Instanz installierter Cronjob überprüft einmal pro Minute, ob neue Update-Dateien zur Verfügung stehen und ob der freie Festplattenspeicherplatz mehr als 10 GB beträgt. In regelmäßigen Abständen

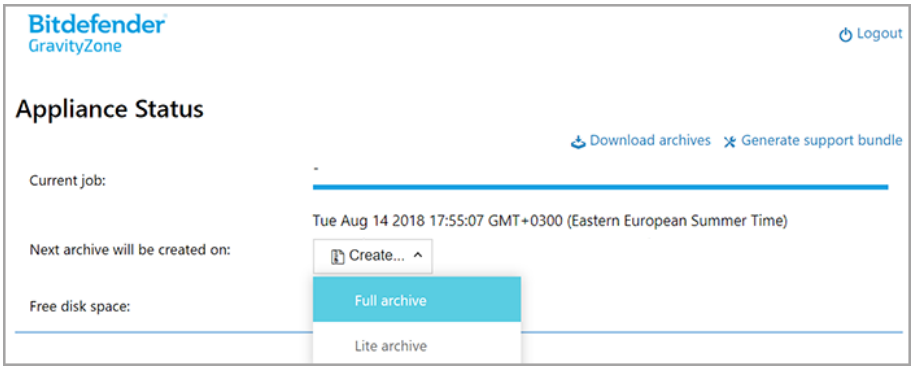
(definiert durch die Option **Archiverstellungsintervall (in Stunden)**) erstellt der Cronjob die folgenden Dateien:

- **Vollständiges Archiv (Produkt + Sicherheitsinhalte)**, wenn neue Update-Dateien zur Verfügung stellen
- **Lite-Archiv** (nur Sicherheitsinhalte), wenn es keine neuen Update-Dateien gibt

Die Archive werden am folgenden Speicherort erstellt:

`https://Online-Instanz-Update-Server-IP-oder-Hostname/snapshots`

3. Klicken Sie auf **Create > Full**, um das erste vollständige Archiv zu erstellen. Warten Sie, bis das Archiv erstellt wurde.

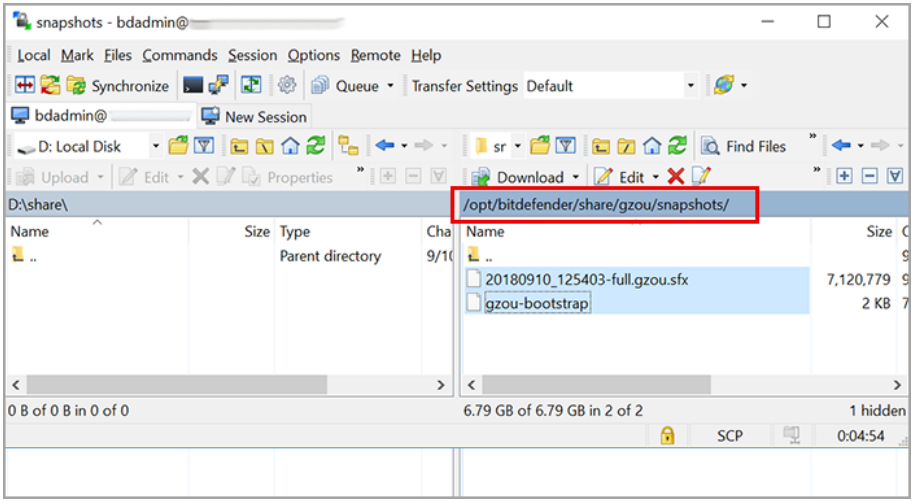


Die Online-Instanz – Web-Dienst: Erstellung des Archivs

4. Laden Sie das vollständige Update-Archiv und die Datei `gzou-bootstrap` von der Online-Instanz herunter. Dazu stehen Ihnen mehrere Möglichkeiten zur Auswahl:
   - Über den Web-Dienst: Klicken Sie auf **Archive herunterladen**, um die Seite mit den Links zu den Update-Dateien zu öffnen. Klicken Sie auf die Links zum vollständigen Update-Archiv und zur Datei `gzou-bootstrap`, um sie auf Ihren Endpunkt herunterzuladen.
   - Öffnen Sie über einen SCP/SCTP-Client (z. B. WinSCP) eine SCP-Sitzung mit der Online-Instanz und übertragen Sie die oben genannten Dateien an einen

beliebigen Speicherort in Ihrem Netzwerk. Der Standardpfad auf der Online-Instanz ist:

```
/opt/bitdefender/share/gzou/snapshots
```



Übermittlung von Update-Dateien über SCP

- Über eine SAMBA-Freigabe. Rufen Sie die Offline-Update-Archive über eine schreibgeschützte SAMBA-Freigabe vom folgenden Speicherort ab:

  ```
  \\Online-Instanz-Update-Server-IP-oder-Hostname\gzou-snapshots
  ```

  Beachten Sie
  Die Zugangsdaten für die SAMBA-Freigabe, sofern angefordert, sind dieselben wie die für die Online-Instanz (Benutzername `bdadmin` und das ansprechende Passwort).

6.5.4. Einrichten der GravityZone-Offline-Instanz

In diesem Schritt werden Sie die Offline-Instanz installieren und konfigurieren, um über die von der Online-Instanz erzeugten Archive Updates zu erhalten. Sofern nicht anderweitig angegeben, müssen alle Befehle mit **Root**-Rechten ausgeführt werden.

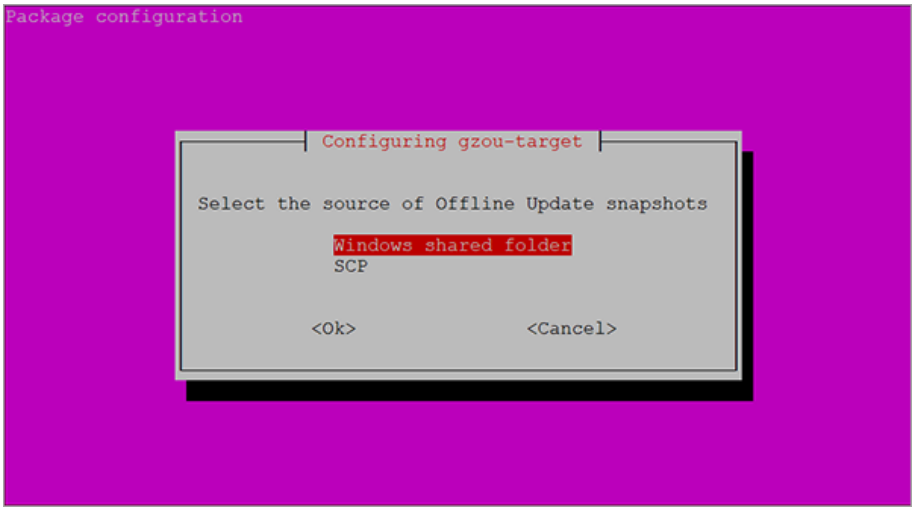
1. Installieren Sie GravityZone auf einer Maschine der isolierten Umgebung.
2. Installieren Sie nur die Datenbank- und die Update-Server-Rolle.
3. Kopieren Sie das Update-Archiv und die Datei `gzou-bootstrap`, die Sie von der Online-Instanz heruntergeladen haben, mithilfe eines Wechseldatenträgers in das Verzeichnis `/home/bdadmin directory` der Offline-Instanz.

   Wichtig
   Damit das Offline-Update funktioniert, müssen die folgenden Punkte gegeben sein:
   - Das Update-Archiv und die Datei `gzou-bootstrap` befinden sich im selben Ordner.
   - Das Update-Archiv ist ein **vollständiges** Archiv.

4. Führen Sie die Datei `gzou-bootstrap` wie folgt aus:
   a. Greifen Sie auf das TTY-Terminal der Maschine in Ihrer virtuellen Umgebung zu (oder stellen Sie eine Verbindung zum Terminal über SSH her).
   b. Wandeln Sie einen `gzou-bootstrap`-Befehl in eine ausführbare Datei um:

   ```
   #
   chmod +x gzou-bootstrap
   ```

   c. Ausführen: `./gzou-bootstrap`
5. Wählen Sie eine Möglichkeit, die Update-Archive zur Offline-Instanz zu übertragen:
   - Klicken Sie auf **Windows shared folder** (Samba-Freigabe). In diesem Fall müssen Sie den Pfad zu einer Windows-Freigabe des isolierten Netzwerks angeben, zu der die Offline-Instanz automatisch eine Verbindung herstellt, um die Update-Archive abzurufen. Geben Sie die für den angegebenen Speicherort nötigen Zugangsdaten ein.
   - Wählen Sie SCP, wenn Sie die Dateien manuell über SCP in den Ordner `/opt/bitdefender/share/gzou/snapshots/` der Offline-Instanz übertragen.



Offline-GravityZone-Instanz – Konfiguration der Übertragungsmethode für die Update-Dateien

Beachten Sie
So können Sie die Übertragungsmethode später noch einmal ändern:

a. Greifen Sie auf das TTY-Terminal der Offline-Instanz in Ihrer virtuellen Umgebung zu (oder stellen Sie eine Verbindung zum Terminal über SSH her).

b. Melden Sie sich als Benutzer `bdadmin` und dem von Ihnen eingerichteten Passwort an.

c. Verschaffen Sie sich Root-Rechte, indem Sie den Befehl `sudo su` ausführen.

d. Führen Sie folgenden Befehl aus:

```
# rm -f /opt/bitdefender/etc/gzou-target.json # dpkg-recon
```

Ein Dialogfenster wird angezeigt, indem Sie die gewünschten Änderungen vornehmen können.

6. Wechseln Sie zur Offline-GravityZone-Befehlszeilen Oberfläche und installieren Sie die übrigen Rollen.

7. Rufen Sie über Ihren Browser die Offline-Konsole auf, und geben Sie (im Offline-Modus) Ihren Lizenzschlüssel ein.

6.5.5. Verwenden von Offline-Updates

Wenn Sie die GravityZone-Instanzen eingerichtet haben, aktualisieren Sie Ihre Offline-Installation wie folgt:

1. Laden Sie das neueste Offline-Update-Archiv von der Online-Instanz auf eine beliebige Netzwerkfreigabe herunter. Weitere Informationen finden Sie unter „Konfiguration und Download der Erst-Update-Dateien“ (S. 211).
2. Kopieren Sie mithilfe eines Wechseldatenträgers das Update-Archiv zur konfigurierten Samba-Freigabe des isolierten Netzwerks. Weitere Informationen finden Sie unter „Einrichten der GravityZone-Offline-Instanz“ (S. 213).

   Die Dateien werden automatisch im folgenden Offline-Instanz-Verzeichnis abgelegt:

   ```
   /opt/bitdefender/share/gzou/snapshots/
   ```

6.5.6. Verwenden der Web-Konsole

Rufen Sie durch Eingabe der IP bzw. des Hostnamens der Appliance im Browser die Web-Konsole auf. Sie können die verfügbaren Optionen folgendermaßen bearbeiten:

- Control Center
- Allgemeine Einstellungen

Control Center

Appliance-Status zeigt die Details des zuletzt durchgeführten Jobs (Archivtyp, Datum und Uhrzeit) und den nächsten geplanten Job an.

Sie haben folgende Möglichkeit:

- **Archiv für Sicherheitsinhalte anlegen**
- **Erstellen eines vollständigen Archivs**

Im Bereich **Erstellte Archive** können Sie Sicherheitsinhalte und vollständige Archive herunterladen.

Wählen Sie das Archiv bzw. die Archive in der Liste aus, und klicken Sie auf **Herunterladen**.

Sie können sich auch den verfügbaren Speicherplatz auf der Appliance-Festplatte anzeigen lassen.

Allgemeine Einstellungen

Sie können einen Download-Zeitplan für die GravityZone-Kits erstellen.

1. Klicken Sie auf **Einstellungen bearbeiten**.
2. Wählen Sie in der Liste **Verfügbare Kits** ein oder mehrere Kits aus.
3. Im Abschnitt **Planen** können Sie ein Intervall für die Erstellung der Archive sowie die Anzahl der Archive, die auf der Festplatte gespeichert werden sollen, festlegen.
4. Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.

7. SCHUTZ DEINSTALLIEREN

Sie können GravityZone-Komponenten deinstallieren und neu installieren, wenn Sie zum Beispiel einen Lizenzschlüssel für eine andere Maschine benötigen, um Fehler zu beheben oder ein Upgrade zu installieren.

Um den Bitdefender-Schutz von den Endpunkten in Ihrem Netzwerk ordnungsgemäß zu entfernen, folgen Sie bitte den Anweisungen in diesem Kapitel.

- Endpunkt-Schutz deinstallieren
- HVI deinstallieren
- Exchange-Schutz deinstallieren
- Mobilgeräteschutz deinstallieren
- Deinstallation von Sandbox Analyzer On-Premises
- Deinstallieren von Report-Builder
- Deinstallieren der GravityZone-Server-Rollen

7.1. Endpunkt-Schutz deinstallieren

Um den Bitdefender-Schutz sicher zu entfernen, müssen Sie zuerst die Sicherheitsagenten und dann, falls nötig, den Security Server deinstallieren. Wenn Sie nur den Security Server deinstallieren wollen, stellen Sie sicher, dass sein Agent zuerst mit einem anderen Security Server verbunden ist.

- Sicherheitsagenten deinstallieren
- Security Server deinstallieren

7.1.1. Sicherheitsagenten deinstallieren

Die Sicherheitsagenten können auf zwei Arten deinstalliert werden:

- Per Fernzugriff über Control Center
- Manuell auf der Zielmaschine

Warnung
Die Sicherheitsagenten und Sicherheitsserver sind wichtig, um Bedrohungen der Endpunkte abzuwehren; ihre Deinstallation kann das gesamte Netzwerk gefährden.

Fern-Deinstallation

So deinstallieren Sie den Bitdefender-Schutz per Fernzugriff von jedem beliebigen verwalteten Endpunkt aus:

1. Öffnen Sie die Seite **Netzwerk**.
2. Wählen Sie **Computer und virtuelle Maschinen** aus der Ansichtsauswahl.
3. Wählen Sie den gewünschten Container im linken Fenster. Alle Computer des ausgewählten Containers werden in der Tabelle im rechten Fenster angezeigt.
4. Wählen Sie die Endpunkte aus, von denen Sie den Bitdefender-Sicherheitsagenten deinstallieren möchten.
5. Klicken Sie auf **Aufgaben** oben in der Tabelle und wählen Sie dann **Client deinstallieren**. Ein Konfigurationsfenster wird geöffnet.
6. Im Fenster **Agent deinstallieren** können Sie auswählen, ob Sie in Quarantäne befindliche Dateien an den Endpunkten behalten oder löschen wollen.

   Bei mit VMware vShield integrierten Umgebungen müssen Sie die erforderlichen Zugangsdaten für jede Maschine auswählen, da die Deinstallation sonst fehlschlägt. Wählen Sie **Zugangsdaten für die vShield-Integration verwenden**, geben Sie dann die erforderlichen Daten in die unten angezeigte Zugangsdaten-Manager-Tabelle ein.
7. Klicken Sie auf **Speichern**, um die Aufgabe zu erstellen. Eine Bestätigungsmeldung wird angezeigt.

Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten.

Unter „Schutz für Endpunkte installieren“ (S. 130) können Sie die Sicherheitsagenten neu installieren.

Lokale Deinstallation

So deinstallieren Sie den Sicherheitsagenten von Bitdefender auf einer Windows-Maschine:

1. Abhängig von Ihrem Betriebssystem:
   - Bei Windows 7 öffnen Sie **Start > Systemsteuerung > Programm deinstallieren** im Abschnitt **Programme**.
   - Bei Windows 8 öffnen Sie **Einstellungen > Systemsteuerung > Programm deinstallieren** im Abschnitt **Programme**.

- Bei Windows 8.1 klicken Sie mit der rechten Maustaste **Start** und wählen Sie dann **Systemsteuerung > Programme & Funktionen**.
- Bei Windows 10 öffnen Sie **Start > Einstellungen > System > Apps & Funktionen**.

2. Wählen Sie in der Programmliste den Bitdefender-Agenten.
3. Klicken Sie auf **Deinstallieren**.
4. Geben Sie das Bitdefender-Passwort ein, falls es in den Sicherheitsrichtlinien aktiviert ist. Während der Deinstallation können Sie den Prozessfortschritt anzeigen.

So deinstallieren Sie den Bitdefender-Sicherheitsagenten manuell von einer Linux-Maschine:

1. Terminal öffnen.
2. Root-Zugang erhalten Sie über den Befehl `su` oder `sudo su`.
3. Öffnen Sie mit dem Befehl `cd` den folgenden Pfad: `/opt/BitDefender/bin`
4. Führen Sie folgendes Script aus:

```
# ./remove-sve-client
```

5. Zum Fortfahren geben Sie das Bitdefender-Passwort ein, sofern dies in den Sicherheitsrichtlinien aktiviert ist.

So deinstallieren Sie den Bitdefender-Agenten von einem Mac:

1. Öffnen Sie **Finder > Anwendungen**.
2. Öffnen Sie den Bitdefender-Ordner.
3. Doppelklicken Sie **Bitdefender Mac deinstallieren**.
4. Klicken Sie im Bestätigungsfenster **Überprüfen** und **Deinstallieren**.

Unter „Schutz für Endpunkte installieren“ (S. 130) können Sie die Sicherheitsagenten neu installieren.

7.1.2. Security Server deinstallieren

Gehen Sie zur Deinstallation des Security Server genauso vor wie bei der Installation, entweder über das Control Center oder über die menügestützte Oberfläche der virtuellen GravityZone-Appliance.

Security Server in Control Center deinstallieren:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Virtuelle Maschinen** aus der Ansichtsauswahl.
3. Wählen Sie das Rechenzentrum oder den Ordner, in dem sich der Host, auf dem Security Server installiert ist, befindet. Die Endpunkte werden im rechten Fenster angezeigt.
4. Markieren Sie das Kästchen des Hosts, auf dem der Security Server installiert ist.
5. Im Menü **Aufgaben** wählen Sie **Security Server deinstallieren**.
6. Geben Sie die vShield-Zugangsdaten ein (falls zutreffend) und klicken Sie auf **Ja**, um die Aufgabe zu erstellen.

Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten.

Wenn Security Server auf der selben virtuellen Appliance installiert ist wie andere GravityZone-Rollen, können Sie ihn über die Befehlszeilenoberfläche der Appliance entfernen. Folgen Sie diesen Schritten:

1. Greifen Sie über Ihre Virtualisierungsverwaltungs-Software (z. B. vSphere Client) auf die Appliance-Console zu.

   Mithilfe der Pfeiltasten und der `Tabulator`-Taste können Sie durch die Menüs und Optionen navigieren. Drücken Sie die `Eingabetaste`, um eine bestimmte Option auszuwählen.
2. Öffnen Sie **Erweiterte Einstellungen** im Menü **Appliance-Optionen**.
3. Wählen Sie **Security-Server deinstallieren**. Ein Bestätigungsfenster wird geöffnet.
4. Drücken Sie die `Y`-Taste oder die `Eingabetaste` und wählen Sie **Ja**, um fortzufahren. Warten Sie, bis die Deinstallation abgeschlossen ist.

7.2. HVI deinstallieren

Um HVI von einem Host zu entfernen, genügt es, das HVI Ergänzungspaket zu deinstallieren. Sie können den Security Server weiterhin als Scan-Server verwenden, vorausgesetzt Sie haben einen gültigen Lizenzschlüssel für Security for Virtualized Environments.

Falls Sie Bitdefender vollständig entfernen möchten, müssen Sie sowohl das HVI-Ergänzungspaket als auch den Security Server deinstallieren.

HVI-Ergänzungspaket deinstallieren

Sie haben zwei Möglichkeiten zur Entfernung des Ergänzungspakets:

- Per Fernzugriff über die Control Center durch Ausführung einer Deinstallationsaufgabe.
- Per Fernzugriff über XenCenter durch Ausführung einiger Befehle auf dem Ziel-Host.

So können Sie das HVI-Paket über die Control Center entfernen:

1. Melden Sie sich im Control Center an.
2. Gehen Sie zur Seite **Netzwerk** und wählen Sie in der Auswahlliste **Virtuelle Maschinen**.
3. Wählen Sie nun im Menu **Ansichten** auf der linken Seite **Server** aus.
4. Wählen Sie einen oder mehrere Xen-Hosts aus dem Netzwerkinventar. Sie können die verfügbaren Hosts ganz einfach über die Option **Typ > Hosts** im Menu **Filter** anzeigen.
5. Klicken Sie das Feld **Aufgaben** auf der rechten Seite an und wählen Sie **HVI-Ergänzungspaket desinstallieren**. Das Konfigurationsfenster wird angezeigt.
6. Planen Sie einen Zeitpunkt für die Entfernung des Pakets. Sie können die Installation direkt nach dem Speichern der Aufgabe oder zu einem späteren Zeitpunkt durchführen. Falls die Entfernung zum festgelegten Zeitpunkt nicht vollständig durchgeführt werden kann, wird der Vorgang automatisch den Einstellungen entsprechend wiederholt. Falls Sie zum Beispiel mehrere Hosts ausgewählt haben und ein Host zum Zeitpunkt der Entfernung nicht verfügbar ist, wird die Aufgabe zum festgelegten Zeitpunkt wiederholt.

7. Der Host muss zum Abschluss der Entfernung neu gestartet werden. Falls der Host unbeaufsichtigt neu starten soll, wählen Sie **Autom. Neustart (falls erforderlich)**.
8. Klicken Sie auf **Speichern**. Eine Bestätigungsmeldung wird angezeigt.

   Auf der Seite **Netzwerk > Aufgaben** können Sie Aufgaben anzeigen und verwalten.

So können Sie das HVI-Paket über das XenCenter entfernen:

1. In XenCenter einloggen
2. Die Konsole des Xen-Host öffnen.
3. Password für den XenServer-Host eingeben.
4. Führen Sie die folgenden Befehle aus:

```
# rpm -ebitdefender-xen-dom0 # rm -rf /etc//xensource/installed-r
  /bitdefender\:bitdefender-hvi/ # rm -rf/opt/bitdef* # Servicexa
```

Security Server deinstallieren

Deinstallation des Security Server auf einem oder mehreren Hosts:

1. Melden Sie sich im Control Center an.
2. Gehen Sie zur Seite **Netzwerk**.
3. Wählen Sie **Virtuelle Maschinen** aus der Ansichtsauswahl.
4. Durchsuchen Sie das Citrix-Inventar und öffnen Sie die Kästchen des gewünschten Hosts. Zur Schnellauswahl können Sie das Netzwerk-Inventar so filtern, dass nur die Security Server angezeigt werden.
5. Klicken Sie das Feld **Aufgaben** oben in der Tabelle an und öffnen Sie im Menü **Security Server deinstallieren**. Eine Bestätigungsmeldung wird angezeigt. Klicken Sie **Ja** um fortzufahren.

Auf der Seite **Netzwerk > Aufgaben** können Sie Aufgaben anzeigen und verwalten.

7.3. Exchange-Schutz deinstallieren

Sie können den Exchange-Schutz von jedem Microsoft-Exchange-Server entfernen, wenn für diese Rolle Bitdefender Endpoint Security Tools installiert ist. Sie können die Deinstallation auch über Control Center vornehmen.

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Computer und virtuelle Maschinen** aus der Ansichtsauswahl.
3. Wählen Sie den gewünschten Container im linken Fenster. Die Entitäten werden im rechten Fenster angezeigt.
4. Wählen Sie den Endpunkt, von dem der Exchange-Schutz deinstalliert werden soll.
5. Klicken Sie **Client neu konfigurieren** im **Aufgaben**- Menü im oberen Teil der Tabelle an. Ein Konfigurationsfenster wird geöffnet.
6. Entfernen Sie im Bereich **Allgemein** das Häkchen im Kästchen **Exchange-Schutz**.

   Warnung
   Stellen Sie über das Konfigurationsfenster sicher, dass alle anderen am Endpunkt aktiven Rollen ausgewählt sind. Andernfalls werden diese ebenfalls deinstalliert.

7. Klicken Sie auf **Speichern**, um die Aufgabe zu erstellen.

Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten.

Unter „Schutz für Exchange installieren“ (S. 176) können Sie den Exchange-Schutz neu installieren.

7.4. Deinstallation von Sandbox Analyzer On-Premises

Gehen Sie zur Deinstallation von Sandbox Analyzer On-Premises wie folgt vor:

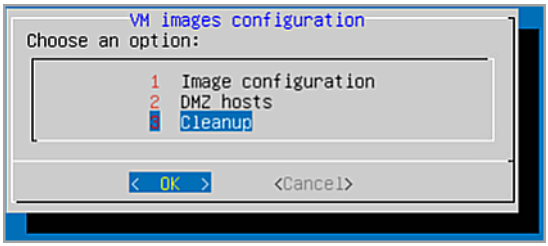
1. Entfernen Sie die Images der virtuellen Maschine (VM) aus der Sandbox Analyzer-Appliance-Konsole.
   a. Melden Sie sich bei der Sandbox Analyzer-Appliance-Konsole an.

      Mithilfe der Pfeiltasten und der `Tabulator`-Taste können Sie durch die Menüs und Optionen navigieren.

      Drücken Sie die `Eingabetaste`, um eine bestimmte Option auszuwählen.

   b. Rufen Sie im Menü **Sandbox configuration** die Option **VM Images** auf.

c. Rufen Sie im Menü **VM images configuration** die Option **Cleanup** auf.



Sandbox Analyzer-Appliance-Konsole - Sandbox Configuration - Cleanup

d. Bestätigen Sie, dass Sie die installierten virtuellen Maschinen-Images entfernen möchten.

   Warten Sie, bis der Vorgang abgeschlossen ist. Während dieses Vorgangs werden auch alle Daten im Zusammenhang mit den virtuellen Maschinen-Images gelöscht.

2. Löschen Sie die virtuelle Sandbox Analyzer-Appliance:
   a. Schalten Sie die virtuelle Sandbox Analyzer-Appliance aus.
   b. Löschen Sie die Appliance aus dem ESXi-Inventar.

7.5. Mobilgeräteschutz deinstallieren

Beim Entfernen des Bitdefender-Schutzes von einem mobilen Gerät muss dies sowohl auf Control Center als auch auf dem Gerät erfolgen.

Nach der Löschung eines Geräts aus dem Control Center gilt Folgendes:

- Die Verknüpfung von GravityZone Mobile Client wird aufgehoben, er wird aber nicht vom Gerät entfernt.
- Sämtliche Protokolle, die sich auf das gelöscht Gerät beziehen, sind weiterhin verfügbar.
- Ihre persönlichen Daten und Anwendungen werden nicht tangiert.
- Auf iOS-Geräten wird das MDM-Profil entfernt. Wenn das Gerät nicht mit dem Internet verbunden ist, bleibt das MDM-Profil installiert, bis eine neue Verbindung verfügbar ist.

Warnung

- Gelöschte Mobilgeräte können Sie nicht wiederherstellen.
- Stellen Sie sicher, dass das Zielgerät vor dem Löschen nicht im Sperrmodus ist. Wenn Sie versehentlich ein gesperrtes Gerät löschen, müssen Sie es auf den Auslieferungszustand zurücksetzen, um es zu entsperren.

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie in der Ansichtsauswahl **Mobilgeräte** aus.
3. Klicken Sie am oberen Rand des Netzwerkfensters auf **Filter** und wählen Sie **Geräte** in der Kategorie **Ansicht**. Klicken Sie auf **Speichern**.
4. Wählen Sie den gewünschten Container im linken Fenster. Alle Geräte werden im rechten Fenster angezeigt.
5. Markieren Sie das Kästchen des Geräts, dessen Schutzfunktion Sie entfernen wollen.
6. Klicken Sie die Schaltfläche ⊖ **Löschen** am oberen Rand der Tabelle.

Danach müssen Sie die Software von Ihrem Gerät deinstallieren.

So deinstallieren Sie Bitdefender-Schutz von einem Android-Gerät:

1. Öffnen Sie **Sicherheit > Geräte-Administratoren**.
2. Entfernen Sie das Häkchen im GravityZone-Kästchen. Ein Bestätigungsfenster wird angezeigt.
3. Tippen Sie auf **Deaktivieren**. Es erscheint eine Warnung mit dem Hinweis, dass Ihre Antidiebstahl-Funktionen nicht länger aktiv sind und dass Ihr Zugang zu Firmennetzwerken und -daten endet.
4. Deinstallieren Sie den GravityZone Mobile Client wie jede andere Anwendung.

So deinstallieren Sie Bitdefender-Schutz von einem iOS-Gerät:

1. Gehen Sie auf das Bitdefender GravityZone Mobile Client-Icon und halten Sie es für ein paar Sekunden gedrückt.
2. Tippen Sie auf den ⊗ Kreis, sobald dieser erscheint. Die Anwendung ist gelöscht.

Um Ihren Mobilschutz neu zu installieren, gehen Sie zu„Mobilgeräteschutz installieren“ (S. 182)

7.6. Deinstallieren von Report-Builder

Um Report Builder vollständig aus Ihrer GravityZone-Lösung zu entfernen, müssen Sie zunächst die Report-Builder-Prozessorenrolle deinstallieren, danach die Report-Builder-Datenbankrolle.

So deinstallieren Sie die Rolle 'Verarbeitung' von Report-Builder:

1. Melden Sie sich über Ihre Virtualisierungs-Verwaltungssoftware (z. B. vSphere Client) bei der Konsolenoberfläche der Report-Builder-Verarbeitung an. Mithilfe der Pfeiltasten und der `Tabulator`-Taste können Sie durch die Menüs und Optionen navigieren. Drücken Sie die `Eingabetaste`, um eine bestimmte Option auszuwählen.
2. Wählen Sie im Hauptmenü den Punkt **Erweiterte Einstellungen**.
3. Gehen Sie zu **Rollen installieren/deinstallieren**, und wählen Sie **Rollen hinzufügen oder entfernen**.
4. Deaktivieren Sie durch Drücken der `Leertaste` die Rolle **Report-Builder-Prozessoren**, und drücken Sie die `Eingabetaste`. Ein Bestätigungsfenster wird angezeigt.
5. Wählen Sie **Ja**, und drücken Sie die `Eingabetaste`, um den Vorgang fortzusetzen, und warten Sie bis die Deinstallation abgeschlossen ist.

So deinstallieren Sie die Rolle 'Datenbank' von Report-Builder:

1. Melden Sie sich über Ihre Virtualisierungs-Verwaltungssoftware (z. B. vSphere Client) bei der Konsolenoberfläche der Report-Builder-Datenbank an. Mithilfe der Pfeiltasten und der `Tabulator`-Taste können Sie durch die Menüs und Optionen navigieren. Drücken Sie die `Eingabetaste`, um eine bestimmte Option auszuwählen.
2. Wählen Sie im Hauptmenü den Punkt **Erweiterte Einstellungen**.
3. Gehen Sie zu **Rollen installieren/deinstallieren**, und wählen Sie **Rollen hinzufügen oder entfernen**.
4. Deaktivieren Sie durch Drücken der `Leertaste` die Rolle **Report-Builder-Datenbank**, und drücken Sie die `Eingabetaste`. Ein Bestätigungsfenster wird angezeigt.

5. Wählen Sie **Ja**, und drücken Sie die `Eingabetaste`, um den Vorgang fortzusetzen, und warten Sie bis die Deinstallation abgeschlossen ist.

Warnung
Wenn Sie die Report-Builder-Appliances in Ihrer virtuellen Umgebung abschalten, ohne die Rollen „Datenbank“ und „Prozessoren“ zu deinstallieren, können Sie keine Verbindung mehr mit dem GravityZone Control Center herstellen.

7.7. GravityZone Virtual Appliance-Rollen deinstallieren

Sie können die Rollen der virtuellen GravityZone-Appliance über die menügestützte Oberfläche deinstallieren. Selbst wenn Sie eine davon entfernen, bleibt Ihr Netzwerkschutz erhalten. Trotzdem benötigen Sie mindestens eine Instanz jeder Rolle, damit GravityZone ordnungsgemäß funktioniert.

In einem Szenario mit einer einzigen Appliance und allen GravityZone-Rollen sind die Endpunkte weiterhin geschützt, wenn eine Rolle entfernt wird, obwohl einige der Appliance-Funktionen je nach Rolle nicht mehr verfügbar sind.

In einem Szenario mit mehreren GravityZone-Appliances kann eine Rolle sicher deinstalliert werden, solange eine andere Instanz der gleichen Rolle verfügbar ist. Mehrere Instanzen der Rollen von Kommunikationsserver und Web-Konsole sind so ausgelegt, dass sie auf unterschiedlichen Appliances installiert und per Lastenverteilung mit anderen Rollen verbunden werden können. Daher wird bei Deinstallation einer Instanz einer bestimmten Rolle ihre Funktion von anderen Rollen übernommen.

Falls nötig, können Sie den Kommunikationsserver von einer Appliance entfernen und seine Funktion einer anderen Instanz dieser Rolle zuweisen. Zur reibungslosen Migration gehen Sie bitte wie folgt vor:

1. Öffnen Sie die Seite **Richtlinien** in Control Center.
2. Wählen Sie eine vorhandene Richtlinie aus oder klicken Sie **Hinzufügen**, um eine neue zu erstellen.
3. Öffnen Sie **Kommunikation** unter **Allgemein**.
4. Klicken Sie in der Tabelle **Kommunikationszuweisung für Endpunkte** auf das Feld **Name**. Die Liste der gefundenen Kommunikationsserver wird angezeigt.
5. Wählen Sie den Kommunikationsserver, der für Endpunkte gelten soll.
6. Klicken Sie auf die Schaltfläche **Hinzufügen** auf der rechten Seite der Tabelle. Falls es in der Liste mehr als einen Kommunikationsserver gibt, können Sie

deren Priorität mithilfe der Aufwärts- und Abwärts-Pfeile rechts neben jeder Entität konfigurieren.

7. Klicken Sie auf **Speichern**, um die Richtlinie zu erstellen. Die Endpunkte kommunizieren mit Control Center über den angegebenen Kommunikationsserver.
8. Deinstallieren Sie die alte Kommunikationsserver-Rolle in der GravityZone-Befehlszeilenoberfläche.

Warnung
Wenn Sie die alte Kommunikationsserver-Rolle deinstallieren, ohne vorher eine Richtlinie zu erstellen, ist die Kommunikation dauerhaft erloschen, und Sie müssen den Sicherheitsagenten neu installieren.

So deinstallieren Sie GravityZone Virtual Appliance-Rollen:

1. Melden Sie sich über Ihr Virtualisierungs-Verwaltungs-Software (z.B. vSphere Client) in der Konsolenoberfläche an. Mithilfe der Pfeiltasten und der `Tabulator`-Taste können Sie durch die Menüs und Optionen navigieren. Drücken Sie die `Eingabetaste`, um eine bestimmte Option auszuwählen.
2. Wählen Sie **Erweiterte Einstellungen**.
3. Wählen Sie **Rollen installieren/deinstallieren**.
4. Öffnen Sie **Rollen hinzufügen oder entfernen**.
5. Mit der `Leertaste` markieren Sie die Rolle, die deinstalliert werden soll und drücken Sie `Eingabe`. Ein Bestätigungsfenster meldet Ihnen, dass die Rolle entfernt wird.
6. Drücken Sie `Eingabe` zum Fortfahren und warten Sie, bis die Deinstallation abgeschlossen ist.

Um eine Rolle neu zu installieren, gehen Sie auf „Rollen installieren/deinstallieren“ (S. 116).

8. HILFE ERHALTEN

Bitdefender hat es sich zur Aufgabe gemacht, seinen Kunden beispiellos schnellen und sorgfältigen Support zu bieten. Sollten Probleme im Zusammenhang mit Ihrem Bitdefender-Produkt auftreten oder Sie Fragen dazu haben, so wenden Sie sich bitte an unser Online-Support-Center. Dort gibt es verschiedene Ressourcen, mit deren Hilfe Sie schnell die richtige Lösung oder Antwort finden können. Sie können auch das Kundenbetreuungs-Team von Bitdefender kontaktieren. Unsere Kundenbetreuer beantworten Ihre Fragen zügig und bieten Ihnen die benötigte Unterstützung.

Beachten Sie
Im Support-Center finden Sie weiterführende Informationen zu unseren Support-Leistungen und Support-Richtlinien.

8.1. Bitdefender-Support-Center

Im Bitdefender-Support-Center finden Sie alle Hilfe und Informationen rund um Ihr Bitdefender-Produkt.

Dabei stehen Ihnen verschiedene Ressourcen zur Verfügung, um die richtige Lösung oder Antwort zu finden:

- Artikel in der Wissensdatenbank
- Bitdefender-Support-Forum
- Produktdokumentation

Zudem können Sie auch Ihre favorisierte Suchmaschine nutzen, um mehr zu erfahren über Computersicherheit, die Bitdefender-Produkte und das Unternehmen.

Artikel in der Wissensdatenbank

Die Bitdefender-Wissensdatenbank ist eine Online-Datenbank mit Informationen rund um die Bitdefender-Produkte. Hier sind in einem leicht zugänglichen Format Berichte zu den Ergebnissen des fortlaufenden technischen Supports sowie der Bugfix-Aktivitäten der Bitdefender-Support- und Entwicklungsteams gespeichert. Hinzu kommen Artikel zur Virenvorbeugung, detaillierte Erklärungen zur Verwaltung von Bitdefender-Lösungen und vieles mehr.

Die Bitdefender-Wissensdatenbank ist öffentlich zugänglich und komplett durchsuchbar. Die darin enthaltenen Informationen sind äußerst umfangreich und

stellen eine weitere Methode dar, mit der Bitdefender-Kunden mit dem notwendigen technischen Wissen versorgt werden. Alle berechtigen Informationsanfragen oder Fehlermeldungen von Bitdefender-Kunden finden sich über kurz oder lang im Bitdefender-Wissensdatenbank wieder und dienen als Bugfix-Anleitungen, Umgehungslösungen oder Informationsartikel, die die Hilfedateien des Produkts ergänzen sollen.

Die Bitdefender-Wissensdatenbank für Unternehmensprodukte steht Ihnen jederzeit unter http://www.bitdefender.de/support/business.html zur Verfügung.

Bitdefender-Support-Forum

Das Bitdefender-Support-Forum bietet Bitdefender-Anwendern eine Möglichkeit, schnelle Hilfe zu erhalten oder anderen Hilfestellung zu geben. Hier können Sie Ihre Probleme und Fragen rund um Ihr Bitdefender-Produkt posten.

Support-Techniker von Bitdefender überwachen neue Einträge in das Forum, um Ihnen helfen zu können. Außerdem können Sie eine Antwort auf Ihre Frage oder einen Lösungsvorschlag von einem bereits erfahrenen Bitdefender-Anwender erhalten.

Bevor Sie einen Eintrag ins Forum stellen, suchen Sie bitte im Forum nach einem ähnlichen oder verwandten Themenbereich.

Das Bitdefender Support-Forum finden Sie unter http://forum.bitdefender.com. Es steht in 5 verschiedenen Sprachen zur Verfügung: Englisch, Deutsch, Französisch, Spanisch und Rumänisch. Mit einem Klick auf **Business Protection** gelangen Sie in den Bereich Unternehmensprodukte.

Produktdokumentation

Die Produktdokumentation ist die umfassendste Informationsquelle rund um Ihr Produkt.

Am einfachsten gelangen Sie über die Seite **Hilfe & Support** im Control Center zur Dokumentation. Klicken Sie oben rechts in der Konsole auf Ihren Benutzernamen, dann auf **Hilfe & Support** und schließlich auf den Link des gewünschten Handbuchs. Dadurch wird ein neuer Reiter in Ihrem Browser geöffnet.

Sie können die Dokumentation auch im Support-Center im Bereich **Dokumentation**, der auf jeder Produktseite verfügbar ist, einsehen und herunterladen.

8.2. Hilfe anfordern

Nutzen Sie unser Online-Support-Center, um Unterstützung anzufordern. Füllen Sie das Kontaktformular aus und senden Sie es ab.

8.3. Verwenden des Support-Tools

Das Support-Tool von GravityZone ermöglicht Benutzern und Support-Mitarbeitern den schnellen Zugriff auf alle Informationen, die Sie zur Problembehandlung benötigen. Führen Sie das Support-Tool auf den betroffenen Computern aus und senden Sie das daraufhin erstellte Archiv mit den Informationen für die Problembehandlung an einen Bitdefender-Support-Mitarbeiter.

8.3.1. Das Support-Tool unter Windows verwenden

Ausführen des Support-Tools

Sie haben folgende Möglichkeiten, das Protokoll auf einem betroffenen Computer zu erzeugen:

- Befehlszeile

  Bei Problemen, wenn BEST auf dem Computer installiert ist.

- Installationsproblem

  Für den Fall, dass BEST nicht auf dem Computer installiert ist und die Installation fehlschlägt.

Über die Befehlszeile

Über die Kommandozeile können Sie Protokolle direkt auf dem betroffenen Computer erfassen. Diese Methode ist dann besonders nützlich, wenn Sie keinen Zugriff auf das GravityZone-Control Center haben oder der Computer nicht mit der Konsole kommuniziert.

1. Öffnen Sie die PowerShell als Administrator.
2. Wechseln Sie zum Installationsordner des Produkts. Der Standardpfad ist:

   ```
   C:\Programme\Bitdefender\Endpoint Security
   ```

3. Führen Sie den folgenden Befehl aus:

   ```
   Product.Support.Tool.exe collect
   ```

Dadurch werden die Protokolle erzeugt und standardmäßig unter `C:\Windows\Temp` gespeichert.

Wenn Sie die Protokolle lieber in einem anderen Ordner speichern möchten, passen Sie die obige Zeile wie folgt an:

```
Product.Support.Tool.exe collect [path="<path-to-file>"]
```

Beispiel:

```
Product.Support.Tool.exe collect path="D:\Test"
```

Während der Befehl ausgeführt wird, wird auf dem Bildschirm ein Fortschrittsbalken angezeigt. Wenn der Vorgang abgeschlossen ist, wird der Name und Speicherort des Archivs angezeigt, das die Protokolle enthält.

Um die Protokolle an den Bitdefender Enterprise Support zu übermitteln, rufen Sie `C:\Windows\Temp` bzw. den benutzerdefinierten Speicherort aus und suchen Sie die Archivdatei mit dem Namen `ST_[computername]_[currentdate]`. Fügen Sie das Archiv zur weiteren Problembehandlung als Anhang Ihrem Support-Ticket hinzu.

Installationsproblem

1. Klicken Sie hier, um das BEST Support Tool herunterzuladen.
2. Führen Sie die ausführbare Datei als Administrator aus. Es wird ein neues Fenster angezeigt.
3. Wählen Sie einen Speicherort zum Speichern des Protokollarchivs.

   Während die Protokolle erfasst werden, wird ein Fortschrittsbalken auf dem Bildschirm angezeigt. Wenn der Vorgang abgeschlossen ist, wird der Name und Speicherort des Archivs angezeigt.

Um die Protokolle an den Bitdefender Enterprise Support zu übermitteln, rufen Sie den ausgewählten Speicherort aus und suchen Sie die Archivdatei mit dem Namen `ST_[computername]_[currentdate]`. Fügen Sie das Archiv zur weiteren Problembehandlung als Anhang Ihrem Support-Ticket hinzu.

8.3.2. Das Support-Tool unter Linux

Für Linux-Betriebssysteme ist das Support-Tool im Bitdefender-Sicherheitsagenten integriert.

Linux-Systeminformationen können Sie über das Support-Tool mit dem folgendem Befehl erhalten:

```
# /opt/BitDefender/bin/bdconfigure
```

Dabei stehen folgende Optionen zur Verfügung:

- `--help` zeigt eine Liste aller Support-Tool-Befehle an.
- `enablelogs` aktiviert Produkt- und Kommunikationsmodulprotokolle (alle Dienste werden automatisch neu gestartet).
- `disablelogs` deaktiviert Produkt- und Kommunikationsmodulprotokolle (alle Dienste werden automatisch neu gestartet).
- `deliverall` erstellt
  - ein Archiv, das die Produkt- und Kommunikationsmodul-Protokolle enthält. Es wird an den Ordner `/tmp` im folgenden Format zugestellt: `Bitdefender_Maschinenname_Zeitstempel.tar.gz`.

  Nach dem das Archiv erstellt wurde:

  1. Wenn Sie die Protokolle deaktivieren möchten, werden Sie um eine Bestätigung gebeten. Wenn nötig, werden die Dienste automatisch neu gestartet.
  2. Wenn Sie Protokolle löschen möchten, werden Sie um eine Bestätigung gebeten.
- `Alle zustellen -Standard` liefert dieselben Informationen wie die vorherige Option, Standardaktionen werden jedoch auf die Protokolle ausgeführt, ohne dass der Benutzer dies bestätigt (die Protokolle werden deaktiviert und gelöscht).

Sie können auch den Befehl `/bdconfigure` direkt aus dem BEST-Paket (vollständig oder Downloader) ausführen, ohne dass das Produkt installiert sein muss.

So melden Sie ein GravityZone-Problem, das Ihre Linux-Systeme beeinträchtigt (verwenden Sie dazu die oben beschriebenen Optionen):

1. Aktivieren Sie Produkt- und Kommunikationsmodulprotokolle.

2. Versuchen Sie, das Problem nachzustellen.
3. Deaktivieren Sie Protokolle.
4. Erstellen Sie ein Protokollarchiv.
5. Öffnen Sie ein E-Mail-Support-Ticket über das Formular auf der Seite **Hilfe & Support** des Control Center; geben Sie eine Beschreibung des Problems ein und hängen Sie das Protokollarchiv an.

Das Support-Tool für Linux liefert die folgenden Informationen:

- Die Ordner `etc`, `var/log`, `/var/crash` (sofern vorhanden) und `var/epag` von `/opt/BitDefender`; darin sind die Bitdefender-Protokolle und -Einstellungen enthalten.
- Die Datei `/var/log/BitDefender/bdinstall.log`, die Informationen zu Installation enthält
- Die Datei `network.txt`, die Netzwerkeinstellungen und Informationen zur Netzwerkverbindung der Maschine enthält.
- Die Datei `product.txt`, die sämtliche Inhalte aller `update.txt`-Dateien aus `/opt/BitDefender/var/lib/scan` und eine rekursive vollständige Liste aller Dateien aus `/opt/BitDefender` enthält
- Die Datei `system.txt`, die allgemeine Systeminformationen enthält (Distribution und Kernel-Version, verfügbarer RAM und freier Festplattenspeicher)
- Die Datei `users.txt`, die Benutzerinformationen enthält
- Andere Informationen zum Produkt im Zusammenhang mit dem Systen, z. B. externe Verbindungen von Prozessen und CPU-Auslastung
- Systemprotokolle

8.3.3. Das Support-Tool unter Mac verwenden

Wir benötigen folgende Angaben für jede Anfrage an den technischen Support von Bitdefender:

- Eine detaillierte Beschreibung des aufgetretenen Problems.
- Gegebenenfalls einen Screenshot von der angezeigten Fehlermeldung.
- Das Support-Tool-Protokoll.

So können Sie mit dem Support-Tool Informationen zu Ihrem Mac-System einholen:

1. Laden Sie das ZIP-Archiv mit dem Support-Tool herunter.
2. Extrahieren Sie die **BDProfiler.tool**-Datei aus dem Archiv.
3. Öffnen Sie ein Terminalfenster.
4. Öffnen Sie den Speicherort der Datei **BDProfiler.tool**.
   Zum Beispiel:

   ```
   cd /Users/Bitdefender/Desktop;
   ```

5. Fügen Sie der Datei Ausführberechtigungen hinzu:

   ```
   chmod +x BDProfiler.tool;
   ```

6. Führen Sie das Tool aus.
   Zum Beispiel:

   ```
   /Users/Bitdefender/Desktop/BDProfiler.tool;
   ```

7. Drücken Sie `J` und geben Sie das Kennwort ein, wenn Sie zur Eingabe des Administratorkennworts aufgefordert werden.

   Warten Sie einige Minuten, bis das Tool das Protokoll erstellt hat. Die entsprechende Archivdatei (**Bitdefenderprofile_output.zip**) finden Sie dann auf Ihrem Desktop.

8.4. Kontaktinformation

Effiziente Kommunikation ist der Schlüssel zu einem erfolgreichen Unternehmen. Seit mehr als 18 Jahren überbietet Bitdefender konstant die bereits hochgesteckten Erwartungen seiner Kunden und Partner und diese Tradition wollen wir auch in Zukunft fortführen. Für jedwede Fragen stehen wir Ihnen gerne zur Verfügung.

8.4.1. Internet-Adressen

Vertrieb: enterprisesales@bitdefender.com
Support-Center:http://www.bitdefender.de/support/business.html

Dokumentation: gravityzone-docs@bitdefender.com
Lokale Vertriebspartner:http://www.bitdefender.de/partners
Partnerprogramm: partners@bitdefender.com
Presse: presse@bitdefender.de
Virus-Einsendungen: virus_submission@bitdefender.com
Spam-Einsendungen: spam_submission@bitdefender.com
Report Abuse: abuse@bitdefender.com
Website: http://www.bitdefender.com

8.4.2. Händler vor Ort

Bitdefender-Händler stehen für vertriebliche und allgemeine Fragen und Informationen in ihren jeweiligen Regionen jederzeit zur Verfügung.

So finden Sie einen Bitdefender-Händler in Ihrem Land:

1. Gehen Sie zu http://www.bitdefender.de/partners.
2. Öffnen Sie die **Partner-Suche**.
3. Die Kontaktinformationen zum örtlichen Bitdefender Distributor sollten automatisch eingeblendet werden. Sollte dies nicht der Fall sein, so wählen Sie Ihr Land aus, um die Informationen anzuzeigen.
4. Falls Sie in Ihrem Land keinen Bitdefender-Händler finden, können Sie uns gerne unter enterprisesales@bitdefender.com kontaktieren.

8.4.3. Bitdefender-Niederlassungen

Bitdefender-Niederlassungen stehen Ihnen für betriebliche und allgemeine Fragen und Informationen in ihren jeweiligen Bereichen jederzeit zur Verfügung. Die genauen Kontaktdaten und Adressen finden Sie in der unten stehenden Auflistung.

USA

Bitdefender, LLC
PO Box 667588
Pompano Beach, Fl 33066
United States
Telefon (Vertrieb&Technischer Support): 1-954-776-6262
Vertrieb: sales@bitdefender.com
Web: http://www.bitdefender.com
Support-Center: http://www.bitdefender.com/support/business.html

Frankreich

Bitdefender
49, Rue de la Vanne
92120 Montrouge
Fax: +33 (0)1 47 35 07 09
Telefon: +33 (0)1 47 35 72 73
E-Mail: b2b@bitdefender.fr
Website: http://www.bitdefender.fr
Support-Center: http://www.bitdefender.fr/support/business.html

Spanien

Bitdefender España, S.L.U.
Avda. Diagonal, 357, 1º 1ª
08037 Barcelona
España
Fax: (+34) 93 217 91 28
Telefon (Geschäftsstelle&Vertrieb): (+34) 93 218 96 15
Telefon (Technischer Support): (+34) 93 502 69 10
Vertrieb: comercial@bitdefender.es
Website: http://www.bitdefender.es
Support-Center: http://www.bitdefender.es/support/business.html

Deutschland

Bitdefender GmbH
Technologiezentrum Schwerte
Lohbachstrasse 12
D-58239 Schwerte
Deutschland
Telefon (Geschäftsstelle&Vertrieb): +49 (0) 2304 94 51 60
Telefon (Technischer Support): +49 (0) 2304 99 93 004
Vertrieb: firmenkunden@bitdefender.de
Website: http://www.bitdefender.de
Support-Center: http://www.bitdefender.de/support/business.html

Großbritannien und Irland

Genesis Centre Innovation Way
Stoke-on-Trent, Staffordshire

ST6 4BF
UK
Telefon (Vertrieb&Technischer Support): (+44) 203 695 3415
E-Mail: info@bitdefender.co.uk
Vertrieb: sales@bitdefender.co.uk
Website: http://www.bitdefender.co.uk
Support-Center: http://www.bitdefender.co.uk/support/business.html

Rumänien

BITDEFENDER SRL
Orhideea Towers
15A Orhideelor Street
060071 Bucharest, Sector 6
Fax: +40 21 2641799
Telefon (Vertrieb&Technischer Support): +40 21 2063470
Vertrieb: sales@bitdefender.ro
Website: http://www.bitdefender.ro
Support-Center: http://www.bitdefender.ro/support/business.html

Vereinigte Arabische Emirate

Bitdefender FZ-LLC
Dubai Internet City, Building 17
Office # 160
Dubai, UAE
Telefon (Vertrieb&Technischer Support): 00971-4-4588935 / 00971-4-4589186
Fax: 00971-4-44565047
Vertrieb: sales@bitdefender.com
Web: http://www.bitdefender.com
Support-Center: http://www.bitdefender.com/support/business.html

A. Anhänge

A.1. Unterstützte Dateitypen

Die Malware-Scan-Engines der Bitdefender-Sicherheitslösungen können sämtliche Dateitypen scannen, in denen Bedrohungen versteckt sein könnten. Die folgende Liste zeigt die am häufigsten gescannten Dateitypen.

{*; 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. Sandbox Analyzer-Objekte

A.2.1. Unterstützte Dateitypen und Dateiendungen für die manuelle Übermittlung

Die folgenden Dateiendungen werden unterstützt und können im Sandbox Analyzer manuell detoniert werden:

Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/Script, HTML (Unicode), JAR (Archiv), JS, LNK, MHTML (DOC), MHTML (PPT), MHTML (XLS), Microsoft Excel, Microsoft PowerPoint, Microsoft Word, MZ/PE-Dateien (ausführbar), PDF, PEF (ausführbar), PIF (ausführbar), RTF, SCR, URL (binär), VBE, VBS, WSF, WSH, WSH-VBS, XHTML.

Sandbox Analyzer kann die oben genannten Dateitypen auch dann erkennen, wenn sie sich in Archiven der folgenden Typen befinden: 7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, LZMA komprimiertes Archiv, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (Multivolume), ZOO, XZ.

A.2.2. Dateitypen, die durch die Vorfilterung von Inhalten bei der automatischen Übermittlung unterstützt werden

Die Vorfilterung der Inhalte bestimmt Dateitypen durch eine Kombination aus Objektinhalt und Dateiendung. Das bedeutet, dass eine ausführbare Datei mit der Dateiendung `.tmp` als Anwendung erkannt und bei Verdacht an denSandbox Analyzer übermittelt wird.

- Anwendungen - Dateien im PE32-Format, einschließlich, aber nicht beschränkt auf die folgenden Dateiendungen: exe, dll, com.
- Dokumente - Dateien im Dokumentformat, einschließlich, aber nicht beschränkt auf die folgenden Dateiendungen: xlsx, xls, ppt, doc, docx, docx, dot, chm, xlm, docm, dotm, dotm, potm, potx, ppam, ppax, pps, pps, ppsm, pptx, sldm, sldx, xlm, xltm, rtf, pdf.

- Skripte: `ps, wsf, ws, php, py, js, vb, vbs, pyc, pyo, wsc, wsh, psc1, jse, vbe.`
- Archive: `zip, jar, 7z, bz, bz2, tgz , msi, rar, rev, z, arj, iso, lha, lhz, uu, uue, xxe, lzma, ace, r00.`
- E-Mails (im Dateisystem gespeichert): `eml, tnef.`

A.2.3. Standardausschlüsse bei automatischer Übermittlung

`asc, avi, bmp, gif, jpeg, jpg, mkv, mp4, pgp, png, txt.`

A.2.4. Empfohlene Anwendungen für die Detonations-VMs

Für die ordnungsgemäße Funktion von Sandbox Analyzer On-Premises müssen bestimmte Anwendungen auf den virtuellen Maschinen für die Detonation installiert sein, damit die übermittelten Stichproben geöffnet werden können.

Anwendungen	Dateitypen
Microsoft Office-Suite	xls, xltm, xltx, ppt, doc, dotx, docm, potm, potx, ppam, ppax, pps, ppsm, ppsx
Adobe Flash Player	swf
Adobe Reader (Zur Anzeige von PDF-Dokumenten)	pdf
Windows-Standard	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