

The background of the cover is a dark, futuristic digital landscape. It features glowing blue and white lines, curves, and patterns that resemble data streams or network connections. A prominent bright light source in the center-right creates a lens flare effect, illuminating the surrounding digital structures. The overall aesthetic is high-tech and secure.

**Bitdefender®**

**Security for AWS**

**AMAZON EC2-INTEGRATIONSANLEITUNG**

## Bitdefender Security for AWS Amazon EC2-Integrationsanleitung

Veröffentlicht 2018.02.02

Copyright© 2018 Bitdefender

### Rechtlicher Hinweis

**Alle Rechte vorbehalten.** Bestandteile dieses Handbuchs 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.

**Warnung und Haftungsausschluss.** Dieses Produkt und die dazugehörige Dokumentation sind urheberrechtlich geschützt. Die Informationen in diesem Dokument werden „ohne Mängelgewähr“ gegeben. Obwohl dieses Dokument mit äußerster Sorgfalt erstellt und geprüft wurde, übernehmen die Autoren keinerlei Haftung für tatsächlich oder angeblich auftretende Schäden bzw. Datenverluste, die direkt oder indirekt durch die Informationen in diesem Dokument entstehen könnten oder bereits entstanden sind.

Dieses Handbuch enthält Verweise auf andere, nicht von Bitdefender erstellte oder von Bitdefender kontrollierte Webseiten und somit übernimmt Bitdefender auch keine Verantwortung für die Inhalte dieser Webseiten. Der Besuch der in diesem Dokument aufgelisteten Drittanbieter-Webseiten erfolgt damit auf eigene Gefahr. Bitdefender stellt diese Links der Einfachheit zur Verfügung. Dies bedeutet nicht, dass Bitdefender den Inhalt einer Website Dritter befürwortet oder Verantwortung dafür übernimmt.

**Warenzeichen.** Es erscheinen eingetragene Warenzeichen in diesem Dokument. Alle eingetragenen und nicht eingetragenen Warenzeichen in diesem Dokument sind das alleinige Eigentum der jeweiligen Besitzer.

# Inhaltsverzeichnis

- 1. Einführung ..... 1
  - 1.1. Anwendungsbereich dieses Dokuments ..... 1
  - 1.2. Über Bitdefender Security for AWS ..... 1
  - 1.3. Bitdefender Security for AWS-Architektur ..... 2
    - 1.3.1. Web-Konsole (GravityZone Control Center) ..... 3
    - 1.3.2. Security Server (Scan-Server) ..... 3
    - 1.3.3. Bitdefender Endpoint Security Tools (Sicherheitsagent) ..... 3
- 2. Vorbereitende Maßnahmen ..... 4
- 3. Den Dienst abonnieren ..... 5
  - 3.1. Abonnieren des Dienstes als Partner ..... 5
  - 3.2. Abonnieren des Dienstes als Direktkunde ..... 6
  - 3.3. Überprüfen des Abonnementstatus ..... 10
    - 3.3.1. AWS-Marketplace-Abonnementstatus\* ..... 10
    - 3.3.2. Abonnementstatus für Amazon Pay\* ..... 11
    - 3.3.3. Status des kostenlosen Testabonnements ..... 11
  - 3.4. Lizenzierung ..... 12
  - 3.5. Nutzung und Zahlung ..... 13
- 4. Einrichten von Bitdefender Security for AWS ..... 14
  - 4.1. Integrieren von Amazon EC2 mit dem GravityZone Control Center ..... 14
    - 4.1.1. Erstellen der Amazon-EC2-Integration ..... 14
    - 4.1.2. Bearbeiten der Amazon-EC2-Integration ..... 23
  - 4.2. Installieren des Sicherheitsagenten auf den Instanzen ..... 23
- 5. Erste Schritte mit Bitdefender Security for AWS ..... 25
  - 5.1. Verbindung zur GravityZone Control Center ..... 25
  - 5.2. Verwalten Ihrer EC2-Instanzen ..... 25
    - 5.2.1. Anzeigen des Amazon-EC2-Inventars ..... 25
    - 5.2.2. Filtern von Amazon-EC2-Instanzen ..... 27
    - 5.2.3. Synchronisieren des Amazon-EC2-Inventars ..... 28
    - 5.2.4. Erstellen von Amazon-EC2-spezifischen Berichten ..... 29
    - 5.2.5. Überwachen der Benutzeraktivitätsprotokolle ..... 29
    - 5.2.6. Konfigurieren der Amazon-EC2-Control Center-Benachrichtigungen ..... 30
- 6. Deinstallieren von Bitdefender Security for AWS ..... 32
  - 6.1. Deinstallieren des Sicherheitsagenten von den EC2-Instanzen ..... 32
  - 6.2. Entfernen der Amazon-EC2-Integration ..... 33
  - 6.3. Kündigen des Bitdefender Security for AWS-Abonnements ..... 34
- A. Anhänge ..... 36
  - A.1. Unterstützte EC2-Instanzen ..... 36
  - A.2. Nützliche Links ..... 38

# 1. EINFÜHRUNG

## 1.1. Anwendungsbereich dieses Dokuments

Dieses Dokument liefert eine Anleitung zur Installation und Verwendung von Bitdefender Security for AWS zum Schutz von Amazon-EC2-Instanzen. Sie werden durch den gesamten Einrichtungsvorgang geführt, vom Abonnieren des Dienstes bis zur Installation und Verwaltung des Schutzes auf Amazon-EC2-Instanzen in der Cloud-Konsole von Bitdefender GravityZone.

Im Folgenden finden Sie alle Informationen zu den in der Cloud-Konsole von GravityZone verfügbaren Bitdefender Security for AWS-Funktionen. Ausführliche Informationen zur Installation des Bitdefender-Sicherheitsagenten finden Sie im **Installationshandbuch**. Einzelheiten zur Verwaltung des Schutzes im GravityZone Control Center finden Sie im **Administratorhandbuch**. Sie finden beide Handbücher unter **Hilfe & Support**.

Dieses Dokument richtet sich an System- und Sicherheitsadministratoren sowie Infrastrukturmanager, die mit der Verwaltung der EC2-Instanzen auf der AWS-Plattform betraut sind, und jeden anderen, der an ausführlichen Informationen zu Bitdefender Security for AWS interessiert ist.

## 1.2. Über Bitdefender Security for AWS

Herkömmliche Endpunktlösungen sind erweisen sich in virtualisierten oder Cloud-basierten Umgebungen häufig als ineffizient. Durch die direkte Bindung an die physische Hardware, sind althergebrachte Sicherheitslösungen oft sehr ressourcenhungrig und sorgen so für Engpässe und Dienstbeeinträchtigungen. Diese Probleme wirken sich negativ auf die Produktivität aus und machen zudem die Kosteneinsparungen durch den Wechsel in die Cloud wieder zunichte.

Aufbauend auf zum Patent angemeldeten Anti-Malware-Technologien zentralisiert Bitdefender Security for Amazon Web Services die Funktionen zum Schutz vor Malware auf dedizierten Scan-Servern, die von Bitdefender außerhalb der geschützten Instanzen gehostet werden. So wird ein minimaler Ressourcenverbrauch der Sicherheitslösung auf jeder Instanz bei maximaler Performance und Schutzwirkung gewährleistet. Integriert mit dem Webdienst Amazon Elastic Compute Cloud (EC2), schützt Bitdefender Security for AWS Dateisysteme, Prozesse und Speicher auf Windows- und Linux-Instanzen. Dabei

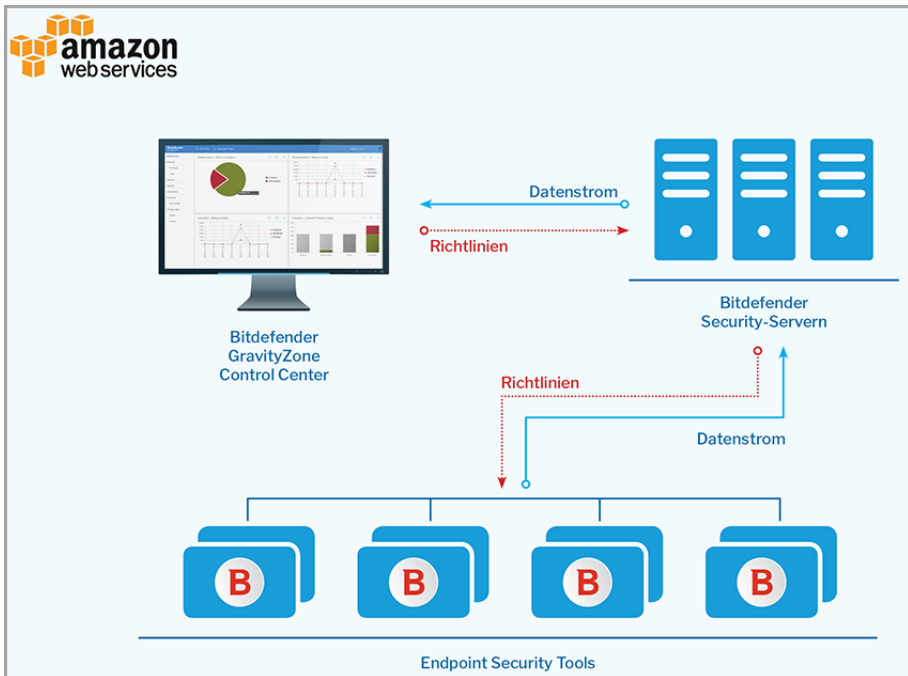
bleibt der Ressourcenverbrauch des Agenten gering, wodurch sich unmittelbare Einsparungen für Amazon-Benutzer ergeben.

Bitdefender Security for AWS ist mit dem GravityZone Control Center integriert. Dabei handelt es sich um eine von Bitdefender gehostete, einheitliche Verwaltungskonsole, die in der Cloud verfügbar ist und ein in Echtzeit synchronisiertes Inventar der EC2-Instanzen bereitstellt.

### 1.3. Bitdefender Security for AWS-Architektur

Bitdefender Security for AWS umfasst die folgenden Komponenten:

- [Web-Konsole \(GravityZone Control Center\)](#)
- [Security Server \(Scan-Server\)](#)
- [Bitdefender Endpoint Security Tools \(Sicherheitsagent\)](#)



Bitdefender Security for AWS-Architektur

### 1.3.1. Web-Konsole (GravityZone Control Center)

Die Sicherheitslösungen in Bitdefender GravityZone werden über die Control Center-Web-Konsole von zentraler Stelle aus verwaltet. So wird eine bequeme Verwaltung und ein einfacher Zugriff auf die allgemeine Sicherheitslage, auf weltweite Sicherheitsbedrohungen und die zentrale Steuerung aller Sicherheitsmodule zum Schutz der Amazon-Instanzen gewährleistet.

Das Control Center lässt sich mit Ihrem EC2-Resource-Inventory integrieren, damit der Schutz einfach und bequem auf nicht verwalteten Amazon-Instanzen bereitgestellt werden kann.

### 1.3.2. Security Server (Scan-Server)

Security Server ist eine dedizierte virtuelle Maschine zur Deduplizierung und Zentralisierung eines Großteils der Malware-Schutzfunktionen der Malware-Schutz-Agenten, die als Scan-Server fungiert.

Security Server-Maschinen werden von Bitdefender in verschiedenen Amazon-Regionen gehostet. Die EC2-Instanzen verbinden sich je nach AWS-Region, in der sie gehostet werden, automatisch mit dem am nächsten gelegenen Security Server.

### 1.3.3. Bitdefender Endpoint Security Tools (Sicherheitsagent)

Um Ihre Amazon-Instanzen mit Bitdefender Security for AWS zu schützen, müssen Sie die GravityZone-Sicherheitsagenten auf jeder Instanz installieren.

GravityZone stellt den Schutz der Amazon-Instanzen 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 der virtuellen Maschine anpasst.

## 2. VORBEREITENDE MAßNAHMEN

Zur Konfiguration der GravityZone-Integration mit Amazon EC2 müssen die folgenden Bedingungen erfüllt sein:

- Der Bitdefender Security for AWS-Dienst wurde für Ihr GravityZone-Unternehmenskonto lizenziert oder Sie nutzen ein Testabonnement.
- Ihre Umgebung erfüllt die im **Installationshandbuch** beschriebenen Anforderungen für Bitdefender Endpoint Security Tools (Sicherheitsagent). Das Handbuch finden Sie unter **Hilfe & Support**.
- Die AWS-EC2-Sicherheitsgruppen wurden ordnungsgemäß konfiguriert. Zur Remote-Installation des Sicherheitsagenten auf den EC2-Instanzen, müssen Sie die den zu schützenden Instanzen zugeordneten Sicherheitsgruppen wie folgt konfigurieren:
  - Gestatten Sie für die Remote-Installation den SSH-Zugriff über die Security-Console-Instanz.
  - Gestatten Sie für die lokale Installation den SSH- und Remotedesktopprotokoll-Zugriff über den Computer, über den Sie die Verbindung herstellen.



## 3. DEN DIENST ABONNIEREN

Es gibt zwei Möglichkeiten zum Abonnieren von Bitdefender Security for Amazon Web Services, die Endkunden und Partnerorganisationen in GravityZone zur Verfügung stehen:

1. [Über das Partner Advantage Network für Bitdefender-Partner](#)
2. [Über die Produktseite im AWS Marketplace für direkte Endkunden](#)

### 3.1. Abonnieren des Dienstes als Partner

Gehen Sie als direkter Bitdefender-Vertriebspartner oder -Partner folgendermaßen vor, um den AWS-Dienst über das Bitdefender-PAN-Portal zu abonnieren:

- Melden Sie sich bei Ihrem [Bitdefender Partner Advantage Network](#)-Benutzerkonto an, rufen Sie die AWS-Sicht auf und wählen Sie eine der beiden verfügbaren Optionen, um:
  1. ein neues GravityZone-Unternehmen anzulegen.
  2. sich bei einem bestehenden GravityZone-Benutzerkonto anzumelden. Sollten Sie sich für diese Option entscheiden, stellen Sie bitte sicher, dass Sie Ihr Hauptpartnerkonto verwenden, über das Sie Ihre verbundenen Kunden und Wiederverkäufer verwalten.

Diese Integration zwischen dem PAN und dem Control Center ist aus Abrechnungsgründen erforderlich und erlaubt es uns, die AWS-Nutzung im Zusammenhang mit Ihren GravityZone-Unternehmen ordnungsgemäß aufzuzeichnen und zu melden. Im Control Center wird mit dieser Aktion die Amazon-EC2-Integrationsoption für Ihr Partnerkonto und für alle von Ihnen verwalteten Unternehmen angezeigt.

- Optional können Sie [Ihre Amazon-EC2-Integration auf der Seite Integrationen im Control Center konfigurieren](#). Als direkter Partner ist es nicht zwingend erforderlich, die Integration zu konfigurieren und den AWS-Dienst für Ihr eigenes Netzwerk zu nutzen, wenn Sie über kein AWS-Konto verfügen. Dieser Schritt ist nur für Kunden und Partner erforderlich, die Ihre EC2-Instanzen schützen möchten. Nach Einrichtung der Integration und Bereitstellung des ersten Sicherheitsagenten profitieren Sie von einer kostenlosen 30-tägigen Testphase für den Dienst.



- Sie können für jedes Ihrer verwalteten Unternehmen monatliche Amazon-EC2-Nutzungsberichte erstellen.
- Weitere Informationen zu Ihrem PAN-Konto erhalten Sie von Ihrem Bitdefender-Account-Manager.

Als Partner eines direkten Bitdefender-Vertriebspartners können Sie die Amazon-EC2-Integration im GravityZone-Control Center anzeigen, sofern für diesen Vertriebspartner das Recht zum Wiederkauf dieses Dienstes im PAN aktiviert ist.

- Bei Bedarf können Sie Ihren Bitdefender-Vertriebspartner wechseln, indem Sie die Partner-ID auf der Seite Mein Unternehmen eingeben.
- Wenn die Amazon-EC2-Integrationsoptionen nicht angezeigt werden, wenden Sie sich bitte an Ihren Bitdefender-Vertriebspartner.

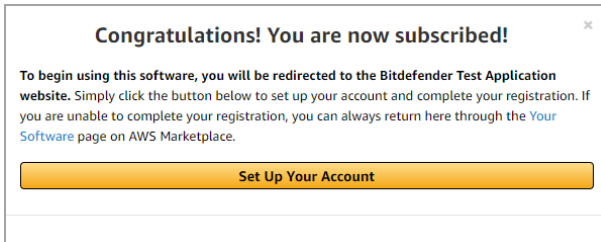
## 3.2. Abonnieren des Dienstes als Direktkunde

Ein Abonnement ist im AWS Marketplace derzeit nur für neue GravityZone-Kunden sowie für Bestandskunden verfügbar, die in der Vergangenheit noch kein AWS-Abonnement abgeschlossen haben.

Für ein Bitdefender Security for AWS-Abonnement müssen Direktkunden bereits über ein aktives AWS-Benutzerkonto verfügen. Als Best Practice wird dringend empfohlen, dass Sie Ihrem AWS-Stammkonto zugeordnete IAM-Benutzerkonten anlegen und verwenden. [Hier](#) erhalten Sie weitere Informationen zu IAM. Stellen Sie zudem sicher, dass Sie ein Produktionskonto verwenden, bei dem eine monatliche AWS-Abrechnung für die Nutzung des Bitdefender-Dienstes erfolgt.

Gehen Sie zum Abonnieren von Bitdefender Security for AWS über den Amazon Marketplace wie folgt vor:

1. Melden Sie sich bei Ihrem AWS-Benutzerkonto an.
2. Rufen Sie im Amazon Marketplace die Seite [Bitdefender Security for AWS](#) auf.
3. Klicken Sie rechts auf der Seite auf **Continue**. Sie werden auf Seite mit den Abonnementinformationen weitergeleitet.
4. Klicken Sie nach Durchsicht der Abonnementinformationen auf **Subscribe**. Eine Bestätigungsmeldung wird angezeigt.



Amazon-Marketplace-Abonnementbestätigung

Damit haben Sie Ihr Bitdefender Security for AWS-Abonnement abgeschlossen. Danach werden Sie aufgefordert, Ihr Bitdefender GravityZone-Benutzerkonto einzurichten.

5. Klicken Sie zum Fortfahren auf **Set Up Your Account**. Sie werden auf ein auf der Bitdefender-Website bereitgestelltes Abonnementformular weitergeleitet. Befolgen Sie ab hier bitte die Schritte, die Ihrem jeweiligen Bitdefender-Kundenstatus entsprechen:
  - a. **Als Neukunde:**
    - i. Geben Sie die erforderlichen Informationen ein.

Bitdefender Security for Amazon Web Services

Already a GravityZone customer? [Click here](#)

Fill in your details to create a new GravityZone account:

Full Name:\*

Email:\*

Phone Number:\*

Company Name:\*

Country:\*

City:\*

Postal Code:\*

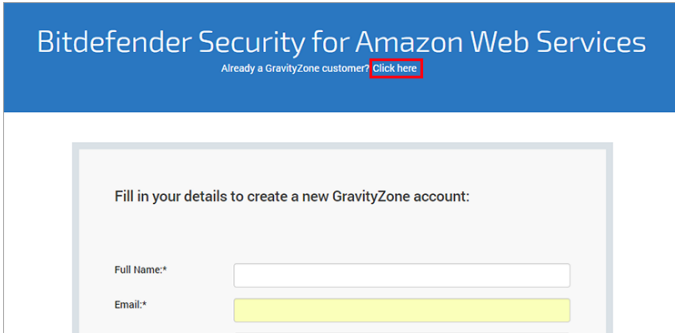
Formular für Bitdefender-Neukunden

ii. Klicken Sie zum Abschluss auf **Registrierung abschließen**.

Wurden gültige Informationen eingegeben, werden für Sie im GravityZone Control Center ein Kundenunternehmen und ein Benutzerkonto angelegt. Sie erhalten per E-Mail eine Bestätigung über den Abschluss des Dienstabonnements im Amazon Marketplace. Sie erhalten zudem eine E-Mail-Bestätigung über das neue GravityZone-Benutzerkonto mit Ihren Zugangsdaten. Jetzt können Sie über den Link in der E-Mail auf das GravityZone Control Center zugreifen.

b. **Als Bestandskunde** müssen Sie nur Ihre Zugangsdaten für das GravityZone Control Center angeben:

i. Klicken Sie auf den Link unter dem Formularnamen.



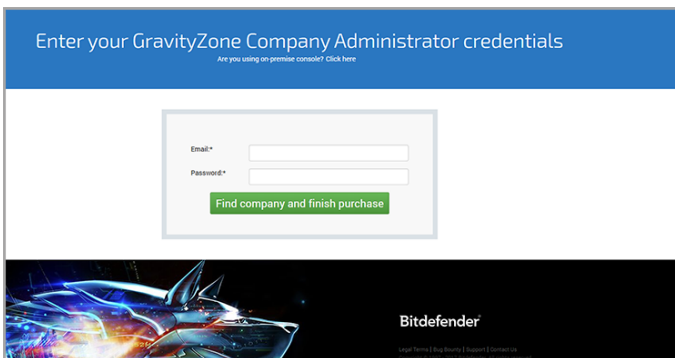
Link für Bitdefender-Bestandskunden

ii. Geben Sie bitte Ihre GravityZone Informationen ein.



**Beachten Sie**

Sie müssen die Zugangsdaten eines Unternehmensadministratorkontos angeben.



Formular für Bitdefender-Bestandskunden

iii. Klicken Sie auf **Abonnement bestätigen**. Wurden gültige Zugangsdaten eingegeben, wird eine Bestätigungsmeldung angezeigt. Rufen Sie das GravityZone Control Center und melden Sie sich bei Ihrem Benutzerkonto an.

Sie können jetzt mit der [Konfiguration der Amazon-EC2-Integration](#) beginnen.

Weitere Informationen zum Abschluss eines Bitdefender Security for AWS-Abonnements über den Amazon Marketplace finden Sie in [diesem Artikel in der Wissensdatenbank](#).

## 3.3. Überprüfen des Abonnementstatus

Rufen Sie zur Überprüfung des Abonnementstatus das GravityZone Control Center auf und klicken Sie im Menü ober rechts auf der Seite auf **Mein Unternehmen**. Auf dieser Seite finden Sie die Informationen zu Ihrem Abonnement.

### 3.3.1. AWS-Marketplace-Abonnementstatus\*

*\* Gilt für Neukunden, die ihr Abonnement nach dem 5. Dezember 2017 abgeschlossen haben.*

Als Kunde mit einem Abonnement für AWS Marketplace können Sie den Abonnementstatus auf der Seite **Mein Unternehmen** im Bereich **AWS-Marketplace-Abonnement** überprüfen.


Der Abonnementstatus kann einer der folgenden sein:

- **Lizenziert:** der Dienst wurde über ein [Abonnement für AWS Marketplace](#) lizenziert. Mit einem lizenzierten Abonnement können Sie Bitdefender Security for AWS auf beliebig vielen Instanzen nutzen. Die Abrechnung für die Nutzung erfolgt dabei monatlich.
- **Gekündigt:** Der Kunde hat das Abonnement für den Dienst in AWS Marketplace gekündigt. Weitere Informationen finden Sie unter „[Kündigen des Bitdefender Security for AWS-Abonnements](#)“ (S. 34).

AWS-Marketplace-Abonnement

---

Status: Lizenziert



Klicken Sie auf das Logo oben, um Ihr Amazon-Marketplace-Konto bequem aufzurufen und dort Ihr Bitdefender-Abonnement zu verwalten.

GravityZone > Mein Unternehmen - Abonnementdaten

### 3.3.2. Abonnementstatus für Amazon Pay\*

\* Gilt für Bestandskunden mit aktiven Abonnements, die vor dem 5. Dezember 2017 abgeschlossen wurden.

Kunden mit einem Abonnement für Amazon Pay können ihren Abonnementstatus auf der Seite **Mein Unternehmen** im Bereich **AWS-Abonnement** überprüfen.

Der Abonnementstatus kann einer der folgenden sein:

- **Lizenziert.** Dieser Status wird angezeigt, nachdem Sie Zahlungen an Bitdefender über Ihr Amazon-Pay-Konto angewiesen haben. In diesem Fall wird die Kreditkarte, die Ihrem Amazon-Pay-Konto zugewiesen ist, monatlich entsprechend Ihrer Nutzung von Bitdefender Security for AWS belastet. Bitte beachten Sie, dass diese Lizenzierungsart nicht mehr unterstützt wird und durch das Abonnement für Amazon Marketplace ersetzt wurde.
- **Gekündigt.** Dieser Status wird angezeigt, nachdem Sie das Abonnement für den Dienst über die entsprechende Kündigungs-Schaltfläche gekündigt haben. In diesem Fall:
  - Alle auf Ihren Instanzen installierten Bitdefender-Sicherheitsagenten laufen dann ab.
  - Die Zahlungsermächtigung für das Abonnement in Amazon Payments wird automatisch widerrufen. Die Nutzungsstunden des aktuellen Monats bis zum Zeitpunkt der Kündigung des Abonnements werden Ihnen jedoch noch in Rechnung gestellt.
- **Gesperrt.** Dieser Status wird angezeigt, wenn innerhalb von 2 Monaten mehrere Versuche, Ihre Kreditkarte zu belasten, fehlgeschlagen sind. In diesem Fall müssen Sie sich an den Bitdefender-Support wenden, um den Fehlbetrag zu überweisen und Ihr Konto wieder zu aktivieren.

### 3.3.3. Status des kostenlosen Testabonnements

Auf der [Produktseite](#) innerhalb der Bitdefender-Website können Sie sich für eine kostenlose Testversion registrieren. Nach der Registrierung müssen Sie zunächst die [Konfiguration der Amazon-EC2-Integration](#) durchführen. Dann können Sie Ihre Abonnementinformationen auf der Seite **Mein Unternehmen** im Bereich **AWS-Abonnement** überprüfen.

Der Abonnementstatus kann einer der folgenden sein:

- **-Testversion.** Sobald Sie die Amazon-EC2-Integration konfiguriert und den Agenten installiert haben, startet der 30 Tage lange Testzeitraum für diesen Dienst. Außer dem Teststatus können Sie sich auch die verbleibenden Tage des Testzeitraums anzeigen lassen. Während der Testphase können Sie beliebig viele Instanzen mit den im GravityZone Control Center verfügbaren Sicherheitsdiensten vollumfänglich schützen und verwalten.
- **Abgelaufen.** Dieser Status wird auf Konten, auf denen das Amazon-Pay-Abonnement noch nicht konfiguriert wurde, angezeigt, wenn die 30 Tage des Testabonnements abgelaufen sind. Um den Dienst weiter zu nutzen, müssen Sie über AWS Marketplace ein Abonnement abschließen. Über einen Klick auf das Widget gelangen Sie zu unserer Produktseite im AWS Marketplace. Dort können Sie ein Abonnement abschließen.

### 3.4. Lizenzierung

Bei Bitdefender Security for AWS handelt es sich um einen Pay-per-Use-Dienst mit monatlichen Abonnement. Bei der Berechnung der Nutzung werden nur laufende Instanzen berücksichtigt, auf denen der Sicherheitsagent installiert ist.

- Wenn Sie sich über den Amazon Marketplace für den Dienst registriert haben, erhalten Sie sofort ein lizenziertes Abonnement. Amazon wird eine monatliche Rechnung für Ihre Nutzung im Vormonat stellen und Sie stellen diese im Rahmen der konsolidierten Fakturierung über Ihr AWS-Benutzerkonto zur Verfügung.
- Wenn Sie sich auf unserer Website für ein kostenloses Probeabonnement für Bitdefender Security for AWS entscheiden, beginnt die 30-tägige Testphase mit der Installation des ersten Sicherheitsagenten auf einer EC2-Instanz. Während der Testphase können Sie alle Funktionen nutzen und der Dienst steht auf beliebig vielen Instanzen zur Verfügung. Um den Dienst nach Ablauf der Testphase auch weiterhin nutzen zu können, müssen Sie [den Dienst über den Amazon Marketplace abonnieren](#).
- Wenn Sie das Dienstabonnement als Bitdefender-Partner über das PAN-Portal abschließen, profitieren Sie von einer 30-tägigen Testphase, die mit der Installation des ersten Sicherheitsagenten auf einer EC2-Instanz beginnt. Die Testphase gilt ebenso für alle untergeordneten Unternehmen, die mit Ihrem Partnerkonto verknüpft sind. Nach Ablauf der Testphase wird der Dienst automatisch für Ihre verwalteten Unternehmen lizenziert, ohne dass Sie einen Lizenzschlüssel eingeben müssen.



Eine Anleitung zum Überprüfen des Abonnementstatus finden Sie unter [„Überprüfen des Abonnementstatus“](#) (S. 10).



### Beachten Sie

Bitdefender Security for AWS ist mit allen GravityZone-Cloud-Lösungen kompatibel.

## 3.5. Nutzung und Zahlung

Bitdefender bietet nutzungsabhängige Lizenzen für seine AWS\_Sicherheitslösung. Dabei wird nur die tatsächliche Uptime Ihrer geschützten Instanzen stundenweise abgerechnet.

Bei der Berechnung der Nutzung werden nur laufende Instanzen berücksichtigt. Die Nutzung wird stundenweise für jede Instanz aufgezeichnet, vom Zeitpunkt des Starts bis zum Anhalten bzw. Beenden der Instanz. Liegt die Nutzungsdauer unter einer Stunde wird gemäß der Vorgaben für EC2-Nutzungsberichte eine volle Stunde gemeldet.

Für Endkunden, die sich über den AWS Marketplace registriert haben, wird von GravityZone die Nutzung für jeden Instanztyp in Ihrem Unternehmen stündlich aufgezeichnet und an Amazon gemeldet. Anhand dieser Informationen stellt Amazon eine monatliche Gebühr für alle laufenden Instanztypen in Rechnung. Die Rechnungsstellung und Abrechnung erfolgt dabei jeweils zum Monatsanfang für die Nutzung im Vormonat.

Für Partner und deren Kunden meldet GravityZone in gleicher Weise die stündliche Nutzung an die Bitdefender-PAN-Plattform jeweils zu Monatsbeginn. Direkte Partner erhalten dann eine Rechnung von Bitdefender, die sich nach der stündlichen Nutzung Ihres Clientnetzwerks richtet.

Der Preis errechnet sich aus den Instanzstunden für jede Instanz.

Eine vollständige Liste der mit Bitdefender Security for AWS im Amazon Marketplace verfügbaren EC-Instanzgrößentypen finden Sie unter [Supported EC2 instances](#).

Ihre Nutzungsdaten erhalten Sie, indem Sie einen **Bericht zur monatlichen Nutzung von Amazon EC2** generieren. Hier erhalten Sie detaillierte Informationen zur stündlichen Nutzung aller verwalteten Instanzen, die zu denen von Ihnen verwalteten Unternehmen gehören. Weitere Informationen finden Sie unter [„Erstellen von Amazon-EC2-spezifischen Berichten“](#) (S. 29).

## 4. EINRICHTEN VON BITDEFENDER SECURITY FOR AWS

Zum Schutz Ihrer EC2-Instanzen mit Bitdefender Security for AWS müssen Sie die folgenden Schritte ausführen:

- Erstellen Sie die Amazon-EC2-Integration in Bitdefender GravityZone
- Installieren Sie den Sicherheitsagenten auf den EC2-Instanzen

### 4.1. Integrieren von Amazon EC2 mit dem GravityZone Control Center

#### 4.1.1. Erstellen der Amazon-EC2-Integration

Die Amazon-EC2-Integration mit GravityZone basiert ab sofort auf der Anmeldung mit kontoübergreifendem Zugriff. Durch dieses Verfahren wird vermieden, dass langfristige AWS-Zugangsdaten wie Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel geteilt werden.

Für das Amazon-EC2-Integrationsverfahren müssen Sie einen **ARN** (Amazon Resource Name - eindeutige Kennung für AWS-Ressourcen) angeben, der mit einer Ihrem AWS-Benutzerkonto zugehörigen Rolle verknüpft ist.

#### **Beachten Sie**

Es wird empfohlen, die Amazon-Integration mit einem eigens für diesen Zweck angelegten Benutzerkonto einzurichten. Der IAM-Benutzer benötigt die IAMFullAccess-Berechtigung, um die für die AWS-Integration in GravityZone benötigte Rolle anzulegen. Weitere Informationen zu den Best Practices im Zusammenhang mit IAM-Benutzerkonten finden Sie [hier](#).

Vor der Konfiguration der AWS-Integration:

- Stellen Sie sicher, dass Sie die entsprechenden Zugangsdaten für das AWS-Benutzerkonto zur Hand haben.
- Öffnen Sie die AWS-Konsole und GravityZone Control Center in zwei getrennten Browser-Tabs. Für eine erfolgreiche AWS-Integration müssen Sie in beiden Tabs arbeiten.

#### **Wichtig**

Bevor Sie den Vorgang starten müssen Sie zunächst den standardmäßigen GravityZone-Sitzungstimeout unter **Control Center > Mein Konto** von 15 Minuten auf

mindestens 1 Stunde umstellen. Falls Ihre Sitzung abläuft, müssen Sie die Integrationsschritte wiederholen.

Gehen Sie folgendermaßen vor, um die AWS-Integration in GravityZone zu erstellen:

1. Melden Sie sich mit Ihren Unternehmensadministrator-Zugangsdaten beim GravityZone Control Center an.
2. Öffnen Sie das Menü oben rechts in der Konsole und klicken Sie auf **Integrationen**.
3. Klicken Sie auf **+ Hinzufügen > Amazon-EC2-Integration hinzufügen**.
4. Das Fenster für die **Amazon-EC2-Integrationseinstellungen** wird mit den folgenden Feldern angezeigt:

Amazon-EC2-Integrationseinstellungen

[More about configuring AWS integration using cross-accounts.](#)

Kontokennung ⓘ

Externe Kennung ⓘ

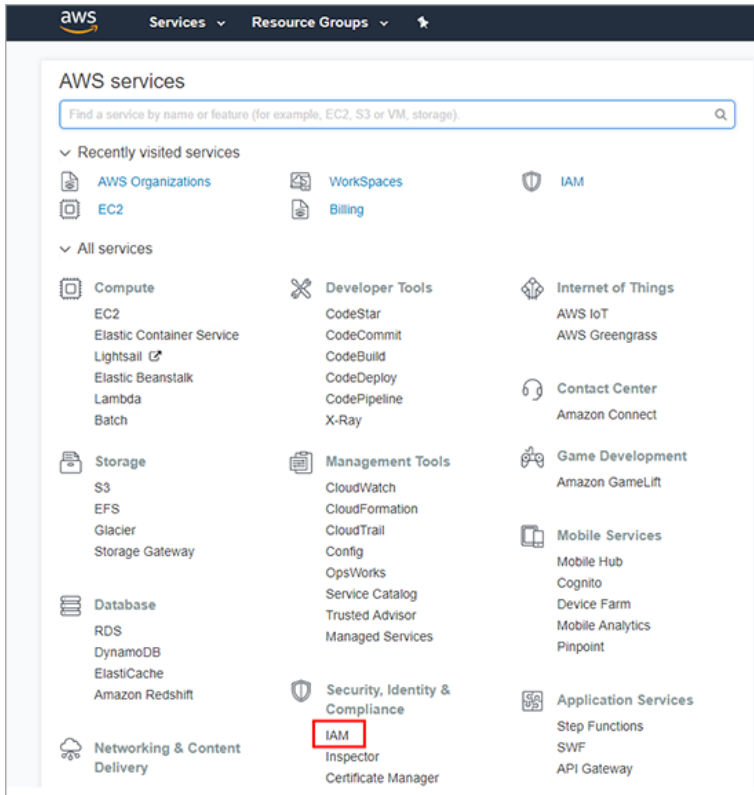
ARN ⓘ

Abbrechen Speichern

GravityZone > Amazon-EC2-Integrationseinstellungen

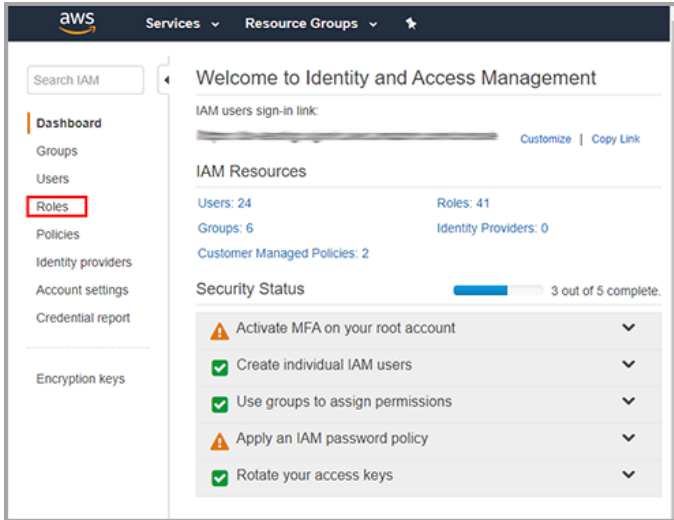
- a. **Account ID:** die eindeutige Kennung für das Bitdefender-AWS-Konto. Das Feld Konto-ID ist bereits ausgefüllt und kann nicht bearbeitet werden.

- b. **External ID** – eine eindeutige Kennung, die mit Ihrem GravityZone-Unternehmen verknüpft ist. Sie wird in Ihrem AWS-Benutzerkonto zur Anlage der GravityZone-spezifischen Rolle für den kontoübergreifenden Zugriff benötigt. Klicken Sie auf die entsprechende **Generate**-Schaltfläche, um den Code zu erhalten und kopieren Sie ihn in die Zwischenablage. Sie benötigen diesen Code in der AWS-Konsole, um den ARN-Code zu erhalten, der zum Abschluss der Integration benötigt wird (sehen Sie hierzu auch Schritt 5-g).
  - c. **ARN**: Der Amazon Resource Name der der in AWS angelegten GravityZone-spezifischen Rolle zugeordnet ist.
5. In diesem Schritt müssen Sie den ARN-Code aus der AWS-Konsole abrufen. Gehen Sie dazu folgendermaßen vor:
  - a. Wechseln Sie zur [AWS-Konsole](#) und melden Sie sich mit Ihrem AWS-Benutzerkonto an.
  - b. Rufen Sie unter AWS Services **Security, Identity & Compliance > IAM** auf.



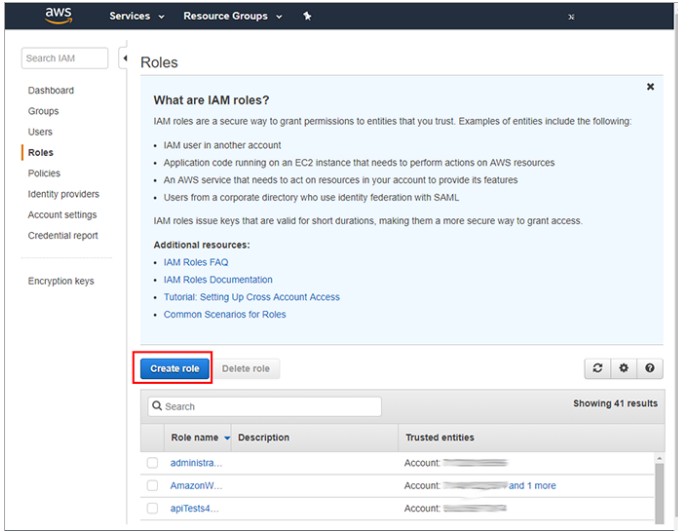
AWS-Konsole > IAM

c. Klicken Sie unter Dashboard auf **Roles**.



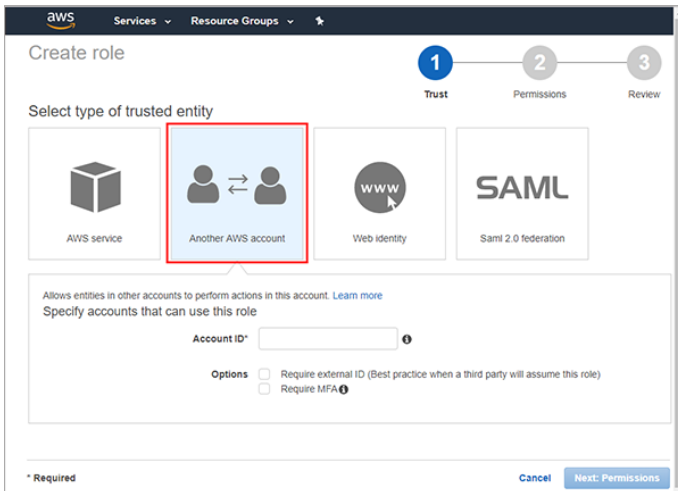
AWS-Konsole > Rollen

d. Klicken Sie auf **Create Role**.



AWS-Konsole > Create roles (Schritt 1)

e. Klicken Sie im nächsten Bildschirm auf **Another AWS Account**.



AWS-Konsole > Create roles (Schritt 2)



- f. Geben Sie im Feld **Account ID**, die Konto-ID ein, die Sie dem GravityZone-Integrationsfenster entnehmen können (sehen Sie dazu Schritt 4).
- g. Wählen Sie im Bereich **Options Require external ID aus (empfohlen, wenn ein Dritter dieser Rolle übernimmt)**. Ein neues Textfeld wird angezeigt. Geben Sie hier die vom GravityZone Control Center im Fenster **Amazon-EC2-Integrationseinstellungen** generierte externe ID ein (sehen Sie dazu Schritt 4).

aws Services Resource Groups

Create role

1 Trust 2 Permissions 3 Review

Allows entities in other accounts to perform actions in this account. [Learn more](#)  
Specify accounts that can use this role

Account ID\*

Options  Require external ID (Best practice when a third party will assume this role)

You can increase the security of your role by requiring an optional external identifier, which prevents "confused deputy" attacks. This is recommended if you do not own or have administrative access to the account that can assume this role. The external ID can include any characters that you choose. To assume this role, users must be in the trusted account and provide this exact external ID. [Learn more](#)

External ID

**Important:** The console does not support using an external ID with the Switch Role feature. If you select this option, entities in the trusted account must use the API, CLI, or a custom federation proxy to make cross-account iam:AssumeRole calls. [Learn more](#)

Require MFA

\* Required Cancel **Next: Permissions**

AWS-Konsole > Create roles (Schritt 3)

- h. Klicken Sie auf **Next: Permissions**.
- i. Im nächsten Bildschirm wird eine Liste mit Berechtigungen für die neue Rolle angezeigt. Prüfen Sie die **AmazonEC2ReadOnlyAccess**-Berechtigung. Nutzen Sie das **Search**-Feld, um die Berechtigung bequem zu finden.

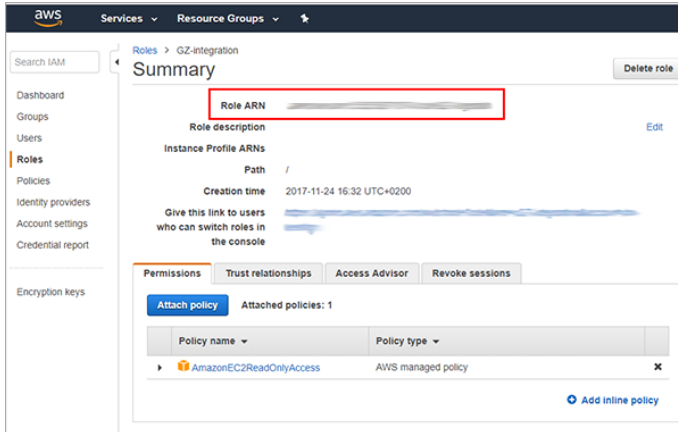
The screenshot shows the AWS IAM console 'Create role' page at step 4, 'Attach permissions policies'. The page has a progress indicator with three steps: 1. Trust, 2. Permissions (current), and 3. Review. Below the progress indicator, there is a section titled 'Attach permissions policies' with the instruction 'Choose one or more policies to attach to your new role.' and buttons for 'Create policy' and 'Refresh'. A search filter is set to 'Policy type' with a search box containing 'ec2readonly', showing 'Showing 1 result'. Below this is a table with the following data:

Policy name	Attachments	Description
<input checked="" type="checkbox"/> AmazonEC2ReadOnlyAccess	32	Provides read only access to Amazon EC2 via the AWS Man...

At the bottom of the page, there are buttons for 'Cancel', 'Previous', and 'Next: Review'.

AWS-Konsole > Create roles (Schritt 4)

- j. Klicken Sie auf **Next: Review**.
- k. Geben Sie einen Namen für die Rolle.
- l. Klicken Sie auf **Create Role**.
- m. Auf der nächsten Seite wird eine Liste mit bestehenden Rollen angezeigt. Suchen Sie die Rolle, die Sie eben angelegt haben und klicken Sie sie an.
- n. Der Rollenübersicht können Sie die ARN der Rolle entnehmen, die im Fenster für die Amazon-EC2-Integrationseinstellungen in der GravityZone Control Center benötigt wird. Kopieren Sie den ARN-Code.



AWS-Konsole > Die ARN der Rolle

6. Wechseln Sie zum GravityZone Control Center und fügen Sie den ARN-Code in das **ARN**-Feld des Integrationsfensters ein.



**Wichtig**

Nach Anlage der Rolle in der AWS-Konsole dauert es ca. eine Minute bis diese Änderung in allen AWS-Regionen verteilt wurde. Die Integration kann nur dann erfolgreich erfolgen, wenn die neue Rolle überall in AWS verteilt wurde. Warten Sie daher eine Minute, bis Sie mit dem nächsten Schritt fortfahren.

7. Klicken Sie auf **Speichern**.
8. Lesen Sie bitte die AWS-Lizenzvereinbarung. Klicken Sie dann auf **Ich stimme zu**.
  - Wurde die Integration erfolgreich durchgeführt, werden die Amazon-EC2-Instanzen in GravityZone importiert und danach unter **Netzwerk > Computer und Gruppen > Amazon EC2** angezeigt. Dort werden Ihre Amazon-EC2-Instanzen nach Amazon-Regionen und den entsprechenden Verfügbarkeitszonen sortiert dargestellt.
  - Ist die Integration fehlgeschlagen, erhalten Sie eine Fehlermeldung mit den möglichen Ursachen. Unter Umständen wurde eine falsche externe ID eingegeben oder die Integration wurde erstellt, bevor die neue AWS-Rolle in allen AWS-Regionen verteilt werden konnte.

Jetzt können Sie Ihre Amazon-Instanzen auf der Seite **Netzwerk** unter **Benutzerdefinierte Gruppen > Amazon EC2** einsehen und verwalten.

### 4.1.2. Bearbeiten der Amazon-EC2-Integration

Sie können Ihre Amazon-EC2-Integration im GravityZone Control Center auf der Seite **Integrationen** jederzeit bearbeiten, indem Sie sie anklicken.

So kann es zum Beispiel notwendig werden, eine neue externe ID in AWS anzugeben. Klicken Sie in diesem Fall auf die **Generate**-Schaltfläche neben dem Feld mit der entsprechenden externen ID. Bitte beachten Sie, dass dadurch die aktuelle externe ID ungültig wird. In diesem Fall wird Ihre Integration ungültig. Zur Wiederherstellung der Integration müssen Sie eine neue externe ID erstellen und die entsprechende Rolle in Ihrem AWS-IAM-Benutzerkonto aktualisieren. Weitere Informationen zum Erstellen einer neuen externen ID finden Sie in diesem [Artikel in der Wissensdatenbank](#).

## 4.2. Installieren des Sicherheitsagenten auf den Instanzen

Um Ihre Amazon-EC2-Instanzen zu schützen, müssen Sie auf jeder Instanz den Bitdefender Endpoint Security Tools-Agenten installieren.

Der Sicherheitsagent übermittelt Scan-Anfragen an den am nächsten gelegenen in Ihren AWS-Regionen gehosteten Sicherheitsserver, der dann den eigentlichen Scan durchführt. Scan-Server kommunizieren zudem mit dem GravityZone Control Center und erhalten so Sicherheitseinstellungen von der Web-Konsole und übermitteln die Ergebnisse ihrer Aktionen. Die Security Server-Maschinen werden von Bitdefender in unterschiedlichen AWS-Regionen gehostet, damit Sie sie nicht in Ihrer eigenen Umgebung bereitstellen müssen.

Bitdefender unterstützt alle öffentlich verfügbaren AWS-Regionen. Weitere Informationen finden Sie in dieser [AWS Regions and Availability Zones](#)-Tabelle.

Bitte beachten Sie bei der Konfiguration der Installationspakete für den Sicherheitsagenten, dass die Scan-Modus-Konfiguration die Amazon-EC2-Instanzen berücksichtigt:

- Automatische (Standard-)Scan-Modi für EC2-Instanzen, die wie folgt eingestellt sind: Zentralisierter Scan mit -Security Server, der in der entsprechenden AWS-Region gehostet ist, mit Ausweichmöglichkeit auf Hybrid-Scan (mit leichten Engines unter Verwendung von Cloud-Scans und, teilweise, lokalen Signaturen).

- Sie können den Scan-Modus auch konfigurieren, indem Sie den benutzerdefinierten Modus und die gewünschten Scan-Modi auswählen.

**Beachten Sie**

Es wird empfohlen, die Standard-Scan-Modi für EC2-Instanzen zu verwenden, da diese speziell auf geringen Ressourcenverbrauch ausgelegt sind. Für EC2-Instanzen mit umfangreichen Ressourcen können Sie auch den folgenden Scan-Modus einstellen: Private Cloud mit -Security Server, der in der entsprechenden AWS-Region gehostet wird, mit Ausweichmöglichkeit auf lokalen Scan (volle Engines unter Verwendung lokal gespeicherter Signaturen und Engines).

Ausführliche Informationen zur Installation von Bitdefender Endpoint Security Tools finden Sie im **Installationshandbuch** unter **Hilfe & Support**.

## 5. ERSTE SCHRITTE MIT BITDEFENDER SECURITY FOR AWS


### 5.1. Verbindung zur GravityZone Control Center

Rufen Sie <https://gravityzone.bitdefender.com/> auf und geben Sie Ihre GravityZone-Zugangsdaten ein.

### 5.2. Verwalten Ihrer EC2-Instanzen

Nach dem erfolgreichen Einrichten der Amazon-EC2-Integration, wird das Amazon-EC2-Inventar im GravityZone Control Center unter **Netzwerk** angezeigt.

Jetzt können Sie mit der Installation des Sicherheitsagenten auf den EC2-Instanzen beginnen, Sicherheitsrichtlinien anwenden und Sicherheitsereignisse über das Dashboard und die verfügbaren Berichte beobachten.

 **Warnung**  
Nur die unterstützten Sicherheitsmodule werden auf den Zielpunkten angewendet. Auf Amazon-EC2-Instanzen werden nur die Module Malware-Schutz, Advanced Therat Control und Gerätesteuerung unterstützt.

GravityZone umfasst eine Reihe von Optionen, die eigens für die Verwaltung von EC2-Instanzen entwickelt wurden. Diese Funktionen werden im Folgenden beschrieben. Informationen zu den weiteren Funktionen im GravityZone Control Center, die dem Sicherheitsmanagement des Netzwerkinventars dienen, finden Sie im **Administrationshandbuch** unter **Hilfe & Support**

#### 5.2.1. Anzeigen des Amazon-EC2-Inventars

Das in GravityZone importierte Amazon-EC2-Inventar wird nach Amazon-Regionen und Verfügbarkeitszonen sortiert dargestellt. Sie finden das Amazon-EC2-Inventar auf der Netzwerkseite im Ordner **Computer und Gruppen**. Die Amazon-EC2-Gruppe wird im linken Bereich der Netzwerkseite angezeigt. Die Instanzen der ausgewählten Gruppe finden Sie im Bereich rechts.

Name	Betriebssystem	IP	Zuletzt gesehen	Bezeichnung
TA-LINUX10_deleted (f-04829e1...		10.10.26.212	N/A	N/A
TA-LINUX10 (f-098fe1fddc766db...		10.10.26.102	N/A	N/A
TA-LINUX11 (f-005dc48ead1148...		10.10.26.251	N/A	N/A
TA-LINUX12 (f-02a4647a837e14...		10.10.26.226	N/A	N/A
TA-LINUX13 (f-01c268c4bac1a3...		10.10.26.135	N/A	N/A
TA-LINUX14_deleted (f-0e7f5f7...		10.10.26.161	N/A	N/A
TA-LINUX14 (f-0cf465c2de5ca25...		10.10.26.103	N/A	N/A
TA-LINUX15 (f-003718bee3a55c...		10.10.26.123	N/A	N/A
TA-LINUX1_deleted (f-09b72ef2...		10.10.26.155	N/A	N/A
TA-LINUX1 (f-0de18a77cb6fbb23...		10.10.26.250	N/A	N/A
TA-LINUX3 (f-0e4324b42405041...		10.10.26.80	N/A	N/A

GravityZone > Netzwerkseite

Beendete Instanzen werden in einem eigenen Ordner im Netzwerkbaum gruppiert. Zuvor verwaltete (geschützte) Instanzen, die von der Amazon-Verwaltungskonsolle aus beendet wurden, werden in der Gruppe **Beendete verwaltete Instanzen** im Ordner **Amazon EC2** gespeichert. Über Berichte können Sie weiterhin Informationen über diese Instanzen erhalten. Wenn sie nicht mehr gebraucht werden, können beendete Instanzen aus dem Netzwerkinventar gelöscht werden.

Sie können Online- und Offline-Instanzen anhand ihres Symbols unterscheiden:

- Offline-Instanzen
- Online-Instanzen

Weitere Einzelheiten zu einer EC2-Instanz können Sie mit einem Klick auf die Instanz auf der **Netzwerkseite** abrufen. Das Informationsfenster mit Informationen wie ID, DNS, IP, Region usw. wird angezeigt.





Informationen
✕

Allgemein   Richtlinie

**Computer**

---

Name: TA-LINUX10 (i-04fc17cfa63d2d659)

Instanz-ID: i-04fc17cfa63d2d659

DNS: N/A

IP: 10.10.26.41

Region: us-east-2

Verfügbarkeitszone: us-east-2c

VPC-ID: vpc-6e176707

Schlüsselname: TA\_Automation\_KeyR2

Instanztyp: t2.micro

Sicherheitsgruppen: TA\_Automation\_SGR2

Speichern
Schließen

GravityZone > EC2-Instanzinformationen

### 5.2.2. Filtern von Amazon-EC2-Instanzen

Um auf die Netzwerkfilteroptionen zuzugreifen, wählen Sie im Bereich links die gewünschte Gruppe aus und klicken Sie auf das **Filter**-Menü oben im Netzwerkbereich.

Im GravityZone Control Center finden Sie eine Reihe von Filteroptionen für das Netzwerkinventar, so auch einige Filter speziell für die Amazon-EC2-Instanzen:

- **Typ:** zeigt nur EC2-Instanzen an.

Typ   Sicherheit   Richtlinie   Tiefe   Betrieb   Tag

**Filtern nach**

Computer

Virtuelle Maschinen

Gruppen/Ordner

Tiefe: in den ausgewählten Ordnern

Speichern
Abbrechen
Zurücksetzen

GravityZone > Netzwerkseite nach Typ filtern


- **Betrieb:** filtert EC2-Instanzen nach Ihrem Betriebsstatus (laufend, angehalten, beendet).

GravityZone > Netzwerkseite nach Betriebsstatus filtern

- **Tag:** filtert Instanzen nach den in Ihrer Amazon-Management-Konsole definierten EC2-Tags.

GravityZone > Netzwerkseite nach Tags filtern

### 5.2.3. Synchronisieren des Amazon-EC2-Inventars

Das Control Center führt alle 15 Minuten automatisch eine Synchronisation mit dem Amazon-EC2-Inventar durch. Sie können diese Synchronisation auch manuell durchführen, indem Sie auf die Schaltfläche  **Mit Amazon EC2 synchronisieren** am oberen Rand der **Netzwerk**-Seite klicken.

## 5.2.4. Erstellen von Amazon-EC2-spezifischen Berichten

Rufen Sie zur Erstellung eines Berichts in der GravityZone Control Center die Seite **Berichte** auf und klicken Sie unten in der Tabelle auf [+](#) **Hinzufügen**. Ein Konfigurationsfenster wird angezeigt. Hier finden Sie verschiedenen Optionen zur Definition des gewünschten Berichts.

GravityZone stellt unterschiedliche Berichtstypen zur Überwachung der Sicherheit auf Ihren Instanzen zur Verfügung. Für EC2-Instanzen steht Ihnen der Berichtstyp **Monatliche Nutzung von Amazon EC2** zur Verfügung:

- Zeigt detaillierte Informationen zur stündlichen Nutzung aller verwalteter Instanzen von Unternehmen die von Ihnen verwaltet sind.
- Die stündliche Nutzungsverteilung pro Instanztyp über alle Ihre verwalteten Unternehmen wird in einem Kuchendiagramm dargestellt.
- In der Tabelle unter dem Diagramm werden Details wie der Name des Unternehmens, der Monat, die gesamten Nutzungsstunden für jedes Unternehmen und die Anzahl verwalteter Instanzen für jedes Unternehmen angezeigt.
- Die Zahl der Nutzungsstunden ist ein Link, der ein neues Fenster öffnet, in dem detaillierte Nutzungsinformationen für jede verwaltete Instanz Ihres Unternehmens aufgeführt sind (Name der Instanz, Instanztyp, IP-Adresse, stündliche Nutzung und übergeordnetes Unternehmen).

## 5.2.5. Überwachen der Benutzeraktivitätsprotokolle

Die Aufzeichnungen zu den Aktivitäten der GravityZone-Benutzerkonten finden Sie auf der Seite **Konten > Benutzeraktivität**.

Das Control Center protokolliert alle von Benutzer ausgeführten Operationen und Aktionen. Die Liste der Benutzeraktivitäten umfasst die folgenden Amazon-EC2-spezifischen Ereignisse:

- Amazon-EC2-Integrationen erstellen, bearbeiten, synchronisieren und löschen
- Bitdefender Security for AWS-Abonnements abschließen und kündigen



Benutzer	Rolle	Aktion	Bereich	Ziel	Erstellt
22222018@btr.com	Company Administrator	Erstellt	Amazon-EC2-Integration	Integrationen	30 Januar 2018, 13:14:05
22222018@btr.com	Company Administrator	Push-Synchron...	Amazon-EC2-Integration	Mit Amazon EC2 synchronisieren	30 Januar 2018, 13:14:05

GravityZone > Benutzerprotokolle

## 5.2.6. Konfigurieren der Amazon-EC2-Control Center-Benachrichtigungen

Das Control Center informiert Sie über den Sicherheitsstatus Ihrer Umgebung, indem es im Bereich **Benachrichtigung** rechts im Control Center entsprechende Benachrichtigungen anzeigt.

**Benachrichtigungen**

Amazon-EC2-Lizenzierungsereignis

Ihr Amazon-EC2-Abonnement ist ab sofort vollständig lizenziert. Ab sofort werden Ihnen am Ende jeden Monats nur die von Ihnen geschätzten Instanzen und nur die tatsächlichen Nutzungsstunden der Bitdefender-Sicherheitsdienste in Rechnung gestellt. Kontaktmöglichkeiten für technische Unterstützung sowie Produktdokumentation finden Sie auf der Hilfe und Support.


Anmeldung von einem ... +

Anmeldung von einem ... +



Amazon-EC2-Lizenzieru... +

Alle Benachrichtigung...

GravityZone > Benachrichtigungen

Sie können die Benachrichtigungen anzeigen, indem Sie auf die Schaltfläche  **Benachrichtigungen** und anschließend auf **Alle Benachrichtigungen anzeigen** klicken. Eine Tabelle mit allen Benachrichtigungen wird angezeigt.

Sie können festlegen, welche Benachrichtigungsarten im Control Center angezeigt werden sollen und welche Sie per E-Mail erhalten möchten. Darüber hinaus gibt es eine Reihe weiterer Optionen. Gehen Sie Konfiguration der Benachrichtigungen wie folgt vor:

- Klicken Sie auf der rechten Seite der Menüleiste auf  **Benachrichtigungen** und danach auf **Alle Benachrichtigungen anzeigen**. Eine Tabelle mit allen Benachrichtigungen wird angezeigt.
- Klicken Sie auf die Schaltfläche  **Konfigurieren** am oberen Rand der Tabelle. Das Fenster **Benachrichtigungsseinstellungen** wird angezeigt.

Im GravityZone Control Center stehen unterschiedliche Amazon-EC2-Benachrichtigungstypen zur Auswahl:

- **Amazon-EC2-Testversion läuft in 7 Tagen ab.** Diese Benachrichtigung informiert Sie darüber, dass Ihr Amazon-EC2-Testabonnement in 7 Tagen abläuft.
- **Amazon-EC2-Testversion läuft morgen ab.** Diese Benachrichtigung wird einen Tag, bevor Ihr Amazon-EC2-Testabonnement ausläuft, ausgegeben.
- **Amazon-EC2-Lizenzierungsereignis.** Diese Benachrichtigung informiert Sie darüber, dass Ihr Amazon-EC2-Abonnement erfolgreich aktiviert wurde.
- **Ungültige Zugangsdaten für Amazon EC2.** Diese Benachrichtigung wird ausgegeben, wenn die AWS-Zugangsdaten nicht mehr gültig sind.
- **Amazon-EC2-Kündigungseignis.** Diese Benachrichtigung wird ausgegeben, wenn das AWS-Abonnement durch den Benutzer gekündigt wird.

## 6. DEINSTALLIEREN VON BITDEFENDER SECURITY FOR AWS

Gehen Sie bitte folgendermaßen vor, wenn Sie die Nutzung von Bitdefender Security for AWS einstellen möchten:

- [Deinstallieren Sie den Sicherheitsagenten von den geschützten EC2-Instanzen](#)
- [Entfernen Sie die Amazon-EC2-Integration aus dem GravityZone Control Center](#)
- [Kündigen Sie das Bitdefender Security for AWS-Dienstabonnement](#)

### 6.1. Deinstallieren des Sicherheitsagenten von den EC2-Instanzen

Wenn Sie die Sicherheit Ihrer EC2-Instanzen nicht mit Bitdefender Endpoint Security Tools verwalten möchten, müssen Sie den Sicherheitsagenten von den Instanzen deinstallieren. Es gibt zwei Möglichkeiten zur Deinstallation von Bitdefender Endpoint Security Tools:

- **Manuell** auf den Zielinstanzen:
  1. Für Windows-Betriebssysteme:
    - a. Melden Sie sich bei der EC2-Instanz an.
    - b. Öffnen Sie die Systemsteuerung und wählen Sie Bitdefender Endpoint Security Tools aus.
    - c. Wählen Sie die Option **Deinstallieren** aus.
    - d. Geben Sie das Bitdefender-Passwort ein, falls es in den Sicherheitsrichtlinien aktiviert ist. Während der Deinstallation können Sie den Prozessfortschritt anzeigen.
  2. Für Linux-Betriebssysteme:
    - a. Terminal öffnen.
    - b. Root-Zugang erhalten Sie über den Befehl `su` oder `sudo su`.
    - c. Mit dem Befehl `cd` gelangen Sie zum folgenden Pfad:

```
/opt/BitDefender/bin
```
    - d. Führen Sie folgendes Script aus:

```
# ./remove-sve-client
```

e. Zum Fortfahren geben Sie das Bitdefender-Passwort ein, sofern dies in den Sicherheitsrichtlinien aktiviert ist.

- **Per Fernzugriff** über das GravityZone Control Center:
  1. Gehen Sie zur Seite **Netzwerk**.
  2. Wählen Sie die verwalteten EC2-Instanzen aus, die sich nicht mehr verwalten möchten. Sie können unter **Computer und Gruppen** auch ganze **Amazon EC2-Gruppen** auswählen.
  3. Klicken Sie auf **Aufgaben** oben in der Tabelle und wählen Sie dann **Client deinstallieren**. Ein Konfigurationsfenster wird geöffnet.
  4. Im Fenster **Agent deinstallieren** können Sie auswählen, ob Sie in Quarantäne befindliche Dateien an den Endpunkten behalten oder löschen wollen.
  5. 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.

## 6.2. Entfernen der Amazon-EC2-Integration

Gehen Sie folgendermaßen vor, um die Amazon-EC2-Integration aus der GravityZone Control Center zu löschen:

1. Öffnen Sie über das Menü in der rechten oberen Ecke der Konsole die Seite **Integrationen**.
2. Markieren Sie das Kästchen für die Lösung, die Sie entfernen möchten.
3. Klicken Sie auf die Schaltfläche **Löschen** am oberen Rand der Tabelle. Im daraufhin angezeigten Fenster müssen Sie das Entfernen noch einmal bestätigen.

Das Löschen der Amazon-EC2-Integration hat die folgenden Auswirkungen:

- Das Amazon-EC2-Inventar wird aus dem Control Center entfernt.
- Alle nicht verwalteten Instanzen werden aus dem GravityZone-Netzwerkinventar gelöscht.
- Die verwalteten Instanzen werden als virtuelle Maschinen in **Computer und Gruppen** verschoben.



- Der Sicherheitsagent auf den verwalteten Maschinen läuft ab, das heißt, dass diese die Kommunikation mit GravityZone und den Bitdefender-Cloud-Diensten einstellen.



### Wichtig

Der abgelaufene Agent wird jedoch auf diesem Maschinen erneut lizenziert, wenn über den GravityZone-Lizenzschlüssel noch Lizenzen verfügbar sind. Es empfiehlt sich daher, Bitdefender Endpoint Security Tools von den verbleibenden verwalteten Maschinen zu deinstallieren und diese dann zu löschen, wenn Sie nicht planen, diese weiterhin zu verwalten.

## 6.3. Kündigen des Bitdefender Security for AWS-Abonnements



### Beachten Sie

Bevor Sie das Abonnement kündigen, empfiehlt es sich, Bitdefender Endpoint Security Tools zunächst von Ihren verwalteten Instanzen zu löschen.

Gehen Sie folgendermaßen vor, um Ihr Bitdefender Security for AWS-Abonnement zu kündigen:

1. Melden Sie sich beim [AWS Marketplace](#) an.

Alternativ können Sie auch das AWS-Marketplace-Widget unter GravityZone Control Center > Benutzermenü > **Mein Unternehmen** verwenden.

2. Wählen Sie im Menü oben rechts den Punkt **Your Marketplace Software** aus. Ein neue Seite wird angezeigt.
3. Rufen Sie unter **Your Software Subscriptions** den Punkt **SaaS** auf.
4. Klicken Sie rechts im Fenster auf **Abonnement kündigen**.
5. Sie werden über eine Pop-up-Meldung zur Bestätigung Ihrer Aktion aufgefordert.

Nach Kündigung des Abonnements:

1. Sie erhalten eine Bestätigungs-E-Mail und eine Benachrichtigung im GravityZone Control Center.
2. Falls Sie über eine Amazon-EC2-Integration mit einer benutzerübergreifenden Rolle verfügen, laufen die Instanzen im GravityZone-Netzwerkinventar ab.

3. Auf der Seite **Mein Unternehmen** zeigt das AWS-Marketplace-Widget den Status **Abgebrochen** an.
4. GravityZone Control Center übermittelt den Nutzungsstatus an AWS. Ihnen wird die Nutzung für den aktuellen Monat in Rechnung gestellt.

Weitere Informationen zur Kündigung des Dienstabonnements finden Sie in diesem [Artikel in der Wissensdatenbank](#).



## A. Anhänge

### A.1. Unterstützte EC2-Instanzen

Größe	Instanztypen nach Erstellung		
	Aktuell	Aktuell (neu hinzugefügt)	Zurück
<b>Klein</b>	t2.micro t2.small	T2.nano	m1.small t1.micro
<b>Mittel</b>	t2.medium m3.medium	-	m1.medium c1.medium
<b>Groß</b>	m3.large c4.large c3.large r3.large	t2.large m4.large r4.large i3.large c5.large	m1.large
<b>xLarge</b>	m3.xlarge c4.xlarge c3.xlarge r3.xlarge i2.xlarge m3.2xlarge c4.2xlarge c3.2xlarge r3.2xlarge i2.2xlarge g2.2xlarge c4.4xlarge c3.4xlarge r3.4xlarge	d2.xlarge m4.xlarge t2.xlarge r4.xlarge i3.xlarge p2.xlarge c5.xlarge d2.2xlarge m4.2xlarge t2.2xlarge r4.2xlarge p3.2xlarge f1.2xlarge i3.2xlarge	m1.xlarge c1.xlarge m2.xlarge m2.2xlarge cg1.4xlarge m2.4xlarge hi1.4xlarge cc1.4xlarge cc2.8xlarge cr1.8xlarge



Größe	Instanztypen nach Erstellung		
	Aktuell	Aktuell (neu hinzugefügt)	Zurück
	i2.4xlarge	c5.2xlarge	
	c4.8xlarge	d2.4xlarge	
	c3.8xlarge	m4.4xlarge	
	r3.8xlarge	r4.4xlarge	
	i2.8xlarge	g3.4xlarge	
	hs1.8xlarge	i3.4xlarge	
		c5.4xlarge	
		d2.8xlarge	
		g2.8xlarge	
		r4.8xlarge	
		p3.8xlarge	
		p2.8xlarge	
		g3.8xlarge	
		i3.8xlarge	
		c5.9xlarge	
		m4.10xlarge	
		x1.16xlarge	
		m4.16xlarge	
		r4.16xlarge	
		p3.16xlarge	
		p2.16xlarge	
		g3.16xlarge	
		f1.16xlarge	
		i3.16xlarge	
		c5.18xlarge	
		x1e.32xlarge	



Größe	Instanztypen nach Erstellung		
	Aktuell	Aktuell (neu hinzugefügt)	Zurück
		x1.32xlarge	

## A.2. Nützliche Links

- [Weitere Informationen zu IAM \(AWS Identity and Access Management\)](#)
- [Informationen zur Erstellung von IAM-Benutzerkonten](#)
- [Informationen zu den AWS-Regionen](#)
- [AWS-Regionen und Verfügbarkeitszonen](#)
- [Anleitung zur Einrichtung der GravityZone-Integration mit Amazon EC2 mit kontoübergreifendem Zugriff](#)
- [Anleitung zum Abschluss eines Bitdefender Security for AWS-Abonnements im AWS Marketplace](#)
- [Best Practices zur Deinstallation von Bitdefender Security for Amazon Web Services](#)