# Stellen Sie einen ExtraHop-Sensor auf der Google Cloud Platform bereit

Veröffentlicht: 2024-11-02

Die folgenden Verfahren erklären, wie Sie ein virtuelles ExtraHop-Paket bereitstellen. Sensor in einer Google Cloud-Umgebung. Sie müssen Erfahrung mit der Bereitstellung virtueller Maschinen in Google Cloud innerhalb Ihrer virtuellen Netzwerkinfrastruktur haben.

Ein virtueller ExtraHop Sensor kann Ihnen helfen, die Leistung Ihrer Anwendungen in internen Netzwerken, im öffentlichen Internet oder einer virtuellen Desktop-Schnittstelle (VDI), einschließlich Datenbank- und Speicherebenen, zu überwachen. Das ExtraHop-System kann die Anwendungsleistung in geografisch verteilten Umgebungen wie Zweigstellen oder virtualisierten Umgebungen über den Verkehr zwischen virtuellen Rechnern überwachen.

Mit dieser Installation können Sie Netzwerkleistungsüberwachung, Netzwerkerkennung und -reaktion sowie Einbruchserkennung auf einem einzigen Gerät ausführen Sensor.

**Wichtig:** Das IDS-Modul benötigt das NDR-Modul. Bevor Sie das IDS-Modul auf diesem Sensor aktivieren können, müssen Sie die Sensor-Firmware auf Version 9.6 oder höher aktualisieren. Wenn das Upgrade abgeschlossen ist, können Sie die neue Lizenz auf den Sensor anwenden.

**Hinweis:** Wenn Sie das IDS-Modul auf diesem Sensor aktiviert haben und Ihr ExtraHop-System keinen direkten Zugang zum Internet und keinen Zugriff auf ExtraHop Cloud Services hat, müssen Sie IDS-Regeln manuell hochladen. Weitere Informationen finden Sie unter Laden Sie die IDS-Regeln über die REST-API in das ExtraHop-System hoch.

Um sicherzustellen, dass die Bereitstellung erfolgreich ist, stellen Sie sicher, dass Sie in der Lage sind, die erforderlichen Ressourcen zu erstellen. Möglicherweise müssen Sie mit anderen Experten in Ihrer Organisation zusammenarbeiten, um sicherzustellen, dass die erforderlichen Ressourcen verfügbar sind.

## Anforderungen an das System

Ihre Umgebung muss die folgenden Anforderungen erfüllen, um einen virtuellen ExtraHop bereitzustellen Sensor in GCP:

- Sie müssen über ein Google Cloud Platform (GCP) -Konto verfügen.
- Sie benötigen die ExtraHop-Bereitstellungsdatei, die auf der ExtraHop Kundenportal.
- Du musst einen ExtraHop haben Sensor Produktschlüssel.
- Sie müssen die Paketspiegelung in GCP aktiviert haben, um den Netzwerkverkehr an das ExtraHop-System weiterzuleiten. Die Paketspiegelung muss so konfiguriert sein, dass Datenverkehr an nic1 (nicht nic0) der ExtraHop-Instanz gesendet wird. Weitere Informationen finden Sie unter https://cloud.google.com/vpc/docs/using-packet-mirroring.

  **Wichtig:** Um die beste Leistung bei der ersten Gerätesynchronisierung zu gewährleisten, schließen Sie alle Sensoren an die Konsole an und konfigurieren Sie dann die Weiterleitung des Netzwerkverkehrs zu den Sensoren.
- Sie müssen Firewallregeln konfiguriert haben, um DNS-, HTTP-, HTTPS- und SSH-Verkehr für die ExtraHop-Verwaltung zuzulassen. Weitere Informationen finden Sie unter https://cloud.google.com/vpc/docs/using-firewalls.

## Anforderungen an virtuelle Maschinen

Sie müssen einen GCP-Instanztyp bereitstellen, der der Größe des virtuellen Sensor am ehesten entspricht und die folgenden Modulanforderungen erfüllt.

| Fühler | Module | Art der Maschine | Bootdisketten | Größe der Startdiskette | Datastore-Festplattentyp | Festplattengröße des Datenspeichers |
|---|---|---|---|---|---|---|
| RevealX Ultra 1 Gbit/s | NDR, NPM, Paketforensik | n1-standard-8 (8 vCPUs, 30 GB Arbeitsspeicher) | NA | NA | Ausgewogener persistenter Speicher | 150 GiB |
| RevealX Ultra 10 Gbit/s | NDR, NPM, Paketforensik | n2-standard-32 (32 vCPUs, 128 GB Arbeitsspeicher) | NA | NA | Ausgewogener persistenter Speicher | 1000 GiB |
| EDA 1100 V | NDR, NPM | n1-standard-4 (4 vCPUs und 15 GB Speicher) | NA | NA | Nichtflüchtiger Standardspeicher | 61 GiB |
| EDA 6320v | NDR, NPM, Intrusion Detection System | n2-standard-32 (32 vCPUs und 128 GB Speicher) | NA | NA | Ausgewogener persistenter Speicher | 1400 GiB |
| EDA 8370v 20 Gbit/s | NDR, NPM, Intrusion Detection System, Paketforensik | n2-standard-80 (80 vCPUs, 320 GB Arbeitsspeicher) | Nichtflüchtiger Standardspeicher | 4 GiB | Ausgewogener persistenter Speicher | 3000 GiB |

**Hinweis:** Durchsatz kann beeinträchtigt werden, wenn mehr als ein Modul auf dem Sensor aktiviert ist.

## Packetstore-Festplattenanforderungen

Sie müssen eine Packetstore-Festplatte für alle RevealX Ultra-Sensoren konfigurieren. Für EDA 8370v-Sensoren müssen Sie Packetstore-Festplatten nur konfigurieren, wenn das Modul Packet Forensics aktiviert ist.

| Sensor | Festplattentyp | Festplattengröße (für jede Festplatte) | Anzahl der Festplatten | Bereitgestellter Durchsatz |
|---|---|---|---|---|
| RevealX Ultra 1 Gbit/s | Nichtflüchtiger Standardspeicher | 4000 GiB | 1 | NA |
| RevealX Ultra 10 Gbit/s | Ausgewogener persistenter Speicher | 32.000 GiB | 1 | NA |
| EDA 8370v 20 Gbit/s | Hyperdisk-Durchsatz<br>Hyperdisk Throughput ist nicht in allen | 13000 GiB | 5 | 600 MiB/s |

| Sensor | Festplattentyp | Festplattengröße (für jede Festplatte) | Anzahl der Festplatten | Bereitgestellter Durchsatz |
|---|---|---|---|---|
| | GCP-Regionen und -Zonen verfügbar. Weitere Informationen finden Sie in der GCP-Dokumentationsseite. | | | |

**Hinweis** Sie müssen den Speicher gleichmäßig auf alle Packetstore-Festplatten verteilen.

## Laden Sie die ExtraHop-Bereitstellungsdatei hoch

1. Melden Sie sich bei Ihrem Google Cloud Platform-Konto an.
2. Klicken Sie im Navigationsmenü auf **Cloud-Speicher** > **Eimer**.
3. Klicken Sie auf den Namen des Speicher-Buckets, in den Sie die ExtraHop-Bereitstellungsdatei hochladen möchten.

   Wenn Sie keinen vorkonfigurierten Speicher-Bucket haben, erstellen Sie jetzt einen.
4. Klicken Sie **Dateien hochladen**.
5. Navigieren Sie zum `extrahop-<module>-gcp-<version>.tar.gz` Datei, die Sie zuvor heruntergeladen haben, und klicken Sie auf **Offen**.

**Nächste Schritte**
Wenn der Datei-Upload abgeschlossen ist, können Sie das Image erstellen.

## Erstellen Sie das Bild

1. Klicken Sie im Navigationsmenü auf **Rechenmaschine** > **Bilder**.
2. klicken **Bild erstellen**.
3. In der Name Feld, geben Sie einen Namen zur Identifizierung des ExtraHop-Sensors ein.
4. Aus dem **Quelle** Dropdownliste, wählen **Cloud-Speicherdatei**.
5. In der Cloud-Speicherdatei Abschnitt, klicken Sie **Durchstöbern**, finde den `extrahop-<module>-gcp-<version>.tar.gz` Datei in Ihrem Speicher-Bucket und klicken Sie dann auf **Wählen**.
6. Konfigurieren Sie alle zusätzlichen Felder, die für Ihre Umgebung erforderlich sind.
7. Schließen Sie die Image-Erstellung ab.

| Option | Description |
|---|---|
| **Für RevealX Ultra 10 Gbit/s, EDA 6320v oder EDA 8370v** | 1. klicken **Gleichwertiger Code**.<br>Auf der rechten Seite öffnet sich ein Fenster.<br>2. In der Gleichwertiger Code Panel, klicken **Kopieren**.<br>3. klicken **In Cloud Shell ausführen**.<br>Der kopierte Text wird an der Eingabeaufforderung angezeigt.<br>4. Fügen Sie diese Option am Ende der Befehlssequenz hinzu: |

| Option | Description |
| --- | --- |
| | `--guest-os-features=GVNIC`<br>5. Drücken Sie die EINGABETASTE.<br>Schließen Sie Cloud Shell, nachdem der Befehl ausgeführt wurde, und klicken Sie dann auf **Stornieren**. Klicken **Stornieren** bricht die Erstellung des Images über Cloud Shell nicht ab. |
| **Für RevealX Ultra 1 Gbit/s** | klicken **Erstellen**. |

## Erstellen Sie die Bootdiskette

**Wichtig:** Erstellen Sie nur eine Bootdiskette für EDA 8370v-Sensoren.

1. Klicken Sie im Navigationsmenü auf **Rechenmaschine** > **Festplatten**.
2. Klicken Sie **Festplatte erstellen**.
3. In der **Name** Feld, geben Sie einen Namen ein, um die Startdiskette zu identifizieren.
4. Aus dem **Typ der Festplattenquelle** Dropdownliste, wählen **Bild**.
5. Aus dem **Quellbild** Wählen Sie in der Dropdownliste das Bild aus , das Sie zuvor erstellt haben.
6. In der **Festplattentyp** Wählen Sie in der Dropdownliste einen Festplattentyp aus.
   Weitere Informationen zur Auswahl eines Festplattentyps finden Sie unter Anforderungen an virtuelle Maschinen.
7. In der **Größe** Feld, geben Sie einen Wert in GiB für die Festplattengröße ein.
   Weitere Informationen zur Auswahl einer Festplattengröße finden Sie unter Anforderungen an virtuelle Maschinen.
8. Konfigurieren Sie alle zusätzlichen Felder, die für Ihre Umgebung erforderlich sind.
9. Klicken Sie **Erstellen**.

## Erstellen Sie die Datenspeicher-Festplatte

1. Klicken Sie im Navigationsmenü auf **Rechenmaschine** > **Festplatten**.
2. Klicken Sie **Festplatte erstellen**.
3. In der Name Feld, geben Sie einen Namen ein, um die ExtraHop-Datenspeicher-Festplatte zu identifizieren.
4. Aus dem **Typ der Festplattenquelle** Dropdownliste, wählen **Bild**.
5. Aus dem **Quellbild** Wählen Sie in der Dropdownliste das Bild aus, das Sie zuvor erstellt haben.
6. In der **Festplattentyp** Wählen Sie in der Dropdownliste einen Festplattentyp aus.
   Weitere Informationen zur Auswahl eines Festplattentyps finden Sie unter Anforderungen an virtuelle Maschinen.
7. In der **Größe** Feld, geben Sie einen Wert in GiB für die Festplattengröße ein.
   Weitere Informationen zur Auswahl einer Festplattengröße finden Sie unter Anforderungen an virtuelle Maschinen.
8. Konfigurieren Sie alle zusätzlichen Felder, die für Ihre Umgebung erforderlich sind.
9. Klicken Sie **Erstellen**.

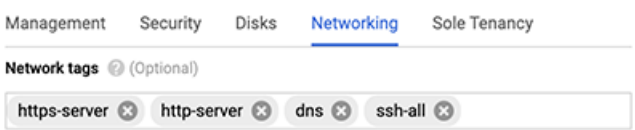
## Erstellen Sie die Packetstore-Diskette

**Hinweis:** Eine Packetstore-Festplatte ist nur für RevealX Ultra 1 Gbps-, RevealX Ultra 10 Gbps- und EDA 8370v-Sensoren erforderlich.

1. Klicken Sie im Navigationsmenü auf **Rechenmaschine** > **Festplatten**.
2. klicken **Festplatte erstellen**.
3. In der **Name** Feld, geben Sie einen Namen zur Identifizierung des Packetstore-Datenträgers ein.
4. Aus dem **Typ der Festplattenquelle** Dropdownliste, wählen **Leere Festplatte**.
5. In der Festplatteneinstellungen Abschnitt, konfigurieren Sie den Festplattentyp und die Größe.
   Weitere Informationen zur Auswahl einer Festplattengröße finden Sie unter Packetstore-Festplattenanforderungen.
6. Konfigurieren Sie alle zusätzlichen Felder, die für Ihre Umgebung erforderlich sind.
7. klicken **Erstellen**.

## Erstellen Sie die VM-Instanz

1. Klicken Sie im Navigationsmenü auf **Rechenmaschine** > **VM-Instanzen**.
2. klicken **Instanz erstellen** und führen Sie die folgenden Schritte aus:
   a) In der **Name** Feld, geben Sie einen Namen ein, um die ExtraHop-Instanz zu identifizieren.
   b) Aus dem **Region** Drop-down-Liste, wählen Sie Ihre geografische Region aus.
   c) Aus dem **Zone** Wählen Sie in der Dropdownliste einen Standort in Ihrer geografischen Zone aus.
   d) In der Konfiguration der Maschine Abschnitt, auswählen **Allgemeiner Zweck** und wählen Sie den Maschinentyp aus , der in der Anforderungen an virtuelle Maschinen.
   e) In der Bootdiskette Abschnitt, klicken Sie **Änderung**.
   f) klicken **Bestehende Festplatten**.
   g) Aus dem **Festplatte** Wählen Sie in der Dropdownliste die Festplatte aus, die Sie zuvor erstellt haben.
   h) Klicken Sie **Wählen**.
3. klicken **Erweiterte Optionen**.
4. klicken **Networking**.
5. Geben Sie im Feld Netzwerk-Tags die folgenden Tag-Namen ein:
   - `https-server`
   - `http-server`
   - `dns`
   - `ssh-alles`




**Wichtig:** Netzwerk-Tags sind erforderlich, um Firewallregeln auf die ExtraHop-Instanz anzuwenden. Wenn Sie keine vorhandenen Firewallregeln haben, die diesen Datenverkehr zulassen, müssen Sie die Regeln erstellen. Weitere Informationen finden Sie unter https://cloud.google.com/vpc/docs/using-firewalls.

6. Wenn Sie einen RevealX Ultra 10-Gbit/s-Sensor konfigurieren, geben Sie die Netzwerkschnittstellenkarte an. In der Konfiguration der Netzwerkleistung Abschnitt, aus dem **Netzwerkschnittstellenkarte** Dropdownliste, wählen **GvNIC**.
7. In der Netzwerkschnittstellen Abschnitt, klicken Sie auf die Verwaltungsoberfläche.
   a) Aus dem Netzwerk Wählen Sie in der Dropdownliste Ihr Verwaltungsnetzwerk aus.
   b) Aus dem **Subnetz** Wählen Sie in der Dropdownliste Ihr Verwaltungsnetzwerk-Subnetz aus.
   c) Konfigurieren Sie alle zusätzlichen Felder, die für Ihre Umgebung erforderlich sind.
   d) Klicken Sie **Erledigt**.
8. klicken **Eine Netzwerkschnittstelle hinzufügen** um die Datenerfassungsschnittstelle zu konfigurieren.

   **Wichtig:** Die Verwaltungsschnittstelle und die Datenerfassungsschnittstelle müssen sich in verschiedenen Virtual Private Cloud (VPC) -Netzwerken befinden.

   a) Aus dem **Netzwerk** Wählen Sie in der Dropdownliste Ihr Netzwerk aus, das den Datenverkehr auf das ExtraHop-System übertragen soll.
   b) Aus dem **Subnetz** Wählen Sie in der Dropdownliste Ihr Netzwerksubnetz aus.
   c) Aus dem **Externe IPv4-Adresse** Dropdownliste, wählen **Keine**.
   d) Konfigurieren Sie alle zusätzlichen Felder, die für Ihre Umgebung erforderlich sind.
   e) Klicken Sie **Erledigt**.
9. Wenn Ihre Konfiguration eine Packetstore-Festplatte enthält, hängen Sie die Festplatte an die Instanz an.
   a) Klicken Sie **Festplatten**.
   b) klicken **Bestehende Festplatte anhängen**.
   c) Fügen Sie den Packetstore-Datenträger hinzu, den Sie zuvor erstellt haben, und klicken Sie dann auf **Speichern**.
10. klicken **Erstellen**.

## Eine Instanzgruppe erstellen

1. Im linken Bereich auf der Rechenmaschine Seite, klicken **Instanzgruppen**.
2. Klicken Sie **Instanzgruppe erstellen**.
3. Klicken Sie **Neue nicht verwaltete Instanzgruppe**.
4. In der **Name** Feld, geben Sie einen Instanzgruppennamen ein.
5. Aus dem **Netzwerk** Wählen Sie in der Dropdownliste das Netzwerk aus, auf das die Instanz zugreifen kann.
6. Aus dem **Subnetz** Wählen Sie in der Dropdownliste Ihr Netzwerksubnetz aus.
7. Aus dem **Wählen Sie VM** Wählen Sie in der Drop-down-Liste Ihren Sensor aus.
8. Klicken Sie **Erstellen**.

## Erstellen Sie einen Load Balancer

1. Klicken Sie im Navigationsmenü auf **Netzwerkdienste** > **Lastenausgleich**.

   **Hinweis:** Wenn der Netzwerkdienste Das Menü befindet sich nicht in Ihrem Navigationsmenü, klicken Sie **Mehr Produkte**.
2. Klicken Sie **Load Balancer erstellen**.
3. In der Network Load Balancer (UDP/mehrere Protokolle) Abschnitt, klicken **Konfiguration starten**.
4. Unter Wählen Sie einen Load Balancer-Typ, klicken **UDP-Loadbalancer**.
5. Unter Internetanschluss oder nur intern, wählen **Nur zwischen meinen VMs**.
6. Unter Backend-Typ, behalte den Standardwert bei (**Backend-Dienst**).

7. Klicken Sie **Fortfahren**.
8. In der **Name des Load Balancers** Feld, geben Sie einen Load Balancer-Namen ein.
9. Aus dem **Region** Drop-down-Liste, wählen Sie Ihre geografische Region aus.
10. Aus dem **Netzwerk** Drop-down-Liste, wählen Sie Ihr Netzwerk aus.
11. In der Backends Abschnitt, aus dem **Instanzgruppe** Wählen Sie in der Dropdownliste Ihre Instanzgruppe aus.
12. Klicken Sie **Gesundheitscheck** und klicken Sie dann **Erstellen Sie einen Gesundheitscheck**.
13. In der **Name** Feld, geben Sie einen Namen für die Integritätsprüfung ein.
14. Aus dem **Protokoll** Dropdownliste, wählen **TCP**.
15. In der **Hafen** Feld, Typ 443.
16. Klicken Sie **Speichern**.

## Erstellen Sie eine Richtlinie zur Datenverkehrsspiegelung

1. Klicken Sie im Navigationsmenü auf **VPC-Netzwerk** > **Paketspiegelung**.
2. Klicken Sie **Richtlinie erstellen**.
3. In der **Name der Richtlinie** Feld, geben Sie einen neuen Richtliniennamen ein.
4. Aus dem Region Drop-down-Liste, wählen Sie Ihre geografische Region aus.
5. Klicken Sie **Weiter**.
6. Wählen **Gespiegelte Quelle und Collector-Ziel befinden sich im selben VPC-Netzwerk** .
7. Aus dem **Netzwerk** Wählen Sie in der Dropdownliste das VPC-Netzwerk aus.
8. Klicken Sie **Weiter**.
9. Wählen Sie die **Wählen Sie ein oder mehrere Subnetzwerke aus** Ankreuzfeld.
10. Aus dem **Subnetz auswählen** Wählen Sie in der Dropdownliste das Kontrollkästchen neben Ihrem Subnetz aus.
11. Klicken Sie **Weiter**.
12. Markieren Sie das Kontrollkästchen neben der VM-Instanz.
13. Klicken Sie **Weiter**.
14. Aus dem **Ziel des Kollektors** Dropdownliste. Wählen Sie den Load Balancer aus, den Sie zuvor erstellt haben.
15. Klicken Sie **Weiter**.
16. Wählen **Gesamten Verkehr spiegeln (Standard)**.
17. Klicken Sie **Einreichen**.

## Den Sensor konfigurieren

**Bevor Sie beginnen**
Bevor Sie den Sensor konfigurieren können, müssen Sie bereits eine Verwaltungs-IP-Adresse konfiguriert haben.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.

   Der Standard-Anmeldename ist `setup` und das Passwort ist die VM-Instanz-ID.
2. Akzeptieren Sie die Lizenzvereinbarung und melden Sie sich dann an.
3. Folgen Sie den Anweisungen, um den Produktschlüssel einzugeben, das Standard-Setup und die Passwörter für das Shell-Benutzerkonto zu ändern, eine Verbindung zu den ExtraHop Cloud Services herzustellen und eine Verbindung zu einer ExtraHop-Konsole herzustellen.

**Nächste Schritte**
Nachdem das System lizenziert ist und Sie sich vergewissert haben, dass Datenverkehr erkannt wird, führen Sie die empfohlenen Verfahren in der Checkliste nach der Bereitstellung.

## L3-Geräteerkennung konfigurieren

Sie müssen das ExtraHop-System so konfigurieren, dass lokale und entfernte Geräte anhand ihrer IP-Adresse erkannt und verfolgt werden (L3 Discovery). Informationen zur Funktionsweise der Gerätesuche im ExtraHop-System finden Sie unter Erkennung von Geräten.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken **Erfassen**.
3. Klicken Sie **Gerätesuche**.
4. In der Lokale Gerätesuche Abschnitt, wählen Sie den **Lokale Geräteerkennung aktivieren** Kontrollkästchen, um L3 Discovery zu aktivieren.
5. In der Geräteerkennung aus der Ferne Abschnitt, geben Sie die IP-Adresse in das **IP-Adressbereiche** Feld.

   Sie können eine IP-Adresse oder eine CIDR-Notation angeben, z. B. `192.168.0.0/24` für ein IPv4-Netzwerk oder `2001:db8::/32` für ein IPv6-Netzwerk.
6. Klicken Sie **Speichern**.