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

Veröffentlicht: 2024-01-22

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

Um sicherzustellen, dass die Bereitstellung erfolgreich ist, stellen Sie sicher, dass Sie Zugriff auf die erforderlichen Ressourcen haben und diese erstellen können. 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 benötigen ein Google Cloud Platform (GCP) -Konto
- Sie benötigen die ExtraHop-Bereitstellungsdatei, die auf der ExtraHop Kundenportal.
- Sie benötigen einen ExtraHop-Produktschlüssel.
- Sie müssen die Paketspiegelung in der GCP aktiviert haben, um Netzwerkverkehr an das ExtraHop-System weiterzuleiten. Die Paketspiegelung muss so konfiguriert sein, dass Datenverkehr an nic1 (nicht nic0) der ExtraHop-Instanz gesendet wird. siehe 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 so konfiguriert haben, dass sie DNS-, HTTP-, HTTPS- und SSH-Verkehr für die ExtraHop-Administration zulassen. siehe https://cloud.google.com/vpc/docs/using-firewalls.
- Sie müssen einen GCP-Instanztyp bereitstellen, der dem virtuellen am ehesten entspricht Sensor Größe, wie folgt:

Fühler	Empfohlener Instanztyp
Reveal (x) EDA 1100v	n1-standard-4 (4 vCPU, 15 GB Speicher)

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** > **Browser**.
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 **Dateien hochladen**.
5. Navigieren Sie zum `extrahop-eda-gcp-<version>.tar.gz` Datei, die Sie zuvor heruntergeladen haben, und klicken Sie **Offen**. Warten Sie, bis die Datei hochgeladen ist, und fahren Sie dann mit dem nächsten Verfahren fort.

Erstellen Sie das Bild

1. Klicken Sie im Navigationsmenü auf **Compute Engine** > **Bilder**.
2. klicken **Bild erstellen** und führen Sie die folgenden Schritte aus:
   a) In der Name Feld, geben Sie einen Namen ein, um den ExtraHop-Sensor zu identifizieren.
   b) Wählen Sie in der Dropdownliste Quelle **Cloud-Speicherdatei**.
   c) In der Cloud-Speicherdatei Abschnitt, klicken **Stöbern**, suchen Sie den `extrahop-eda-gcp-<version>.tar.gz` Datei in Ihrem Speicher-Bucket und klicken Sie dann auf **Wählen**.
   d) Konfigurieren Sie alle zusätzlichen Felder, die für Ihre Umgebung erforderlich sind.
3. klicken **Erstellen**.

Erstellen Sie die Datenspeicherfestplatte

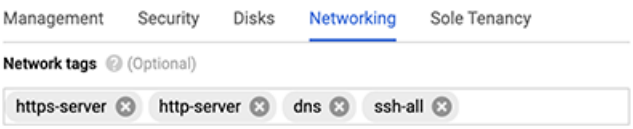
1. Klicken Sie im Navigationsmenü auf **Compute Engine** > **Festplatten**.
2. klicken **Festplatte erstellen** und führen Sie die folgenden Schritte aus:
   a) In der Name Feld, geben Sie einen Namen ein, um die ExtraHop-Festplatte zu identifizieren.
   b) Aus dem Typ Drop-down-Menü, wählen **Nichtflüchtiger Standardspeicher**.
   c) In der Art der Quelle Abschnitt, klicken **Bild**.
   d) Aus dem Quelle Bild-Drop-down-Liste, wählen Sie das Bild aus, das Sie im vorherigen Verfahren erstellt haben.
   e) In der Größe Feld, Typ `61`.
   f) Konfigurieren Sie alle zusätzlichen Felder, die für Ihre Umgebung erforderlich sind.
3. klicken **Erstellen**.

Erstellen Sie die VM-Instanz

1. Klicken Sie im Navigationsmenü auf **Compute Engine** > **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) Wählen Sie in der Drop-down-Liste Region Ihre geografische Region aus.
   c) Wählen Sie in der Dropdownliste Zone einen Standort innerhalb Ihrer geografischen Zone aus.
   d) In der Konfiguration der Maschine Abschnitt, wählen **Allgemeiner Zweck** für die Maschinenfamilie, **N1** für die Serie und **n1-standard-4 (4 vCPU, 15 GB Speicher)** für den Maschinentyp.
   e) In der Startdiskette Abschnitt, klicken **Veränderung**.
   f) klicken **Bestehende Festplatten**.
   g) Aus dem Festplatte Wählen Sie in der Dropdownliste die Festplatte aus, die Sie im vorherigen Verfahren erstellt haben.
   h) klicken **Wählen**.
3. klicken **Erweiterte Optionen**.
4. klicken **Vernetzung**.
5. Geben Sie im Feld Netzwerk-Tags die folgenden Tag-Namen ein:

   Wichtig: Netzwerk-Tags sind erforderlich, um Firewallregeln auf die ExtraHop-Instanz anzuwenden. Wenn Sie nicht über bestehende Firewallregeln verfügen, die diesen Datenverkehr zulassen, müssen Sie die Regeln erstellen. siehe https://cloud.google.com/vpc/docs/using-firewalls.

   - `HTTPS-Server`
   - `http-Server`
   - `dns`
   - `ssh-alles`



6. In der Netzwerkschnittstellen Abschnitt, klicken Sie auf das Bearbeitungssymbol um die Verwaltungsschnittstelle zu bearbeiten.
   a) Aus dem **Netzwerk** Drop-down-Liste, wählen Sie 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 **Erledigt**.
7. klicken **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 spiegeln soll.
   b) Aus dem **Subnetz** Drop-down-Liste, wählen Sie Ihr Netzwerk-Subnetz aus.
   c) Aus dem **Externe IP** Drop-down-Liste, wählen **Keine**.
   d) Konfigurieren Sie alle zusätzlichen Felder, die für Ihre Umgebung erforderlich sind.
   e) klicken **Erledigt**.
8. klicken **Erstellen**.

Eine Instanzgruppe erstellen

1. Im linken Bereich auf der Compute Engine Seite, klick **Instanzgruppen**.
2. klicken **Instanzgruppe erstellen**.
3. klicken **Neue nicht verwaltete Instanzgruppe**.
4. Geben Sie einen Namen für die Instanzgruppe ein in **Name** Feld.
5. In der Netzwerk und Instanzen Abschnitt, wählen Sie das Netzwerk aus, auf das die Instanz zugreifen kann **Netzwerk** Drop-down-Liste.
6. Wählen Sie das Subnetz aus **Subnetz** Drop-down-Liste.
7. Wählen Sie den Sensor aus **Wählen Sie VM** Drop-down-Liste.
8. klicken **Erstellen**.

Erstellen Sie einen Load Balancer

1. Auf dem Netzwerkdienste Seite, klick **Lastenausgleich**.
2. klicken **Load Balancer erstellen**.
3. In der UDP-Lastenausgleich Abschnitt, klicken **Konfiguration starten**.
4. Wählen **Nur zwischen meinen VMs**.
5. klicken **Weiter**.
6. Geben Sie einen Namen für den Load Balancer ein.
7. Wählen Sie Ihre Region aus der **Region** Drop-down-Liste.
8. Wählen Sie Ihr Netzwerk aus der **Netzwerk** Drop-down-Liste.
9. In der Neues Backend Wählen Sie im Abschnitt Ihre Instanzgruppe aus der Drop-down-Liste aus.
10. klicken **Gesundheitscheck** und dann klicken **Erstellen Sie einen Gesundheitscheck**.

11. Geben Sie einen Namen für die Gesundheitsprüfung ein.
12. Wählen **TCP** aus der Dropdownliste Protokoll.
13. Typ 443 im Hafenfeld.
14. klicken **Speichern**.

Erstellen Sie eine Richtlinie zur Verkehrsspiegelung

1. Klicken Sie auf der VPC-Netzwerkseite auf **Spiegelung von Paketen**.
2. klicken **Richtlinie erstellen**.
3. In der Richtlinienübersicht definieren Abschnitt, geben Sie einen neuen Richtliniennamen ein.
4. Wählen Sie Ihre Region aus der **Region** Drop-down-Liste.
5. klicken **Weiter**.
6. Wählen **Die gespiegelte Quelle und das Collector-Ziel befinden sich im selben VPC-Netzwerk** .
7. Wählen Sie das VPC-Netzwerk aus **Netzwerk** Drop-down-Liste.
8. klicken **Weiter**.
9. Wählen Sie den **Wählen Sie ein oder mehrere Subnetze** Checkbox.
10. Aus dem **Subnetz wählen** Wählen Sie in der Dropdownliste das Kontrollkästchen neben Ihrem Subnetz aus.
11. Wählen Sie den **Wählen Sie einzelne Instanzen aus** Checkbox.
12. klicken **Wählen**.
13. Aktivieren Sie das Kontrollkästchen neben der VM-Instanz.
14. klicken **Weiter**.
15. Wählen Sie den Load Balancer, den Sie zuvor erstellt haben, aus der **Ziel des Sammlers** Drop-down-Liste.
16. klicken **Weiter**.
17. Wählen **Gesamten Datenverkehr spiegeln (Standard)**.
18. klicken **Einreichen**.

Den Sensor konfigurieren

Nachdem Sie eine IP-Adresse für die konfiguriert haben Sensor, öffnen Sie einen Webbrowser und navigieren Sie über die konfigurierte IP-Adresse zum ExtraHop-System. Akzeptieren Sie die Lizenzvereinbarung und melden Sie sich an. Der Standard-Anmeldename ist `setup` und das Passwort ist `default`. Folgen Sie den Anweisungen, um den Produktschlüssel einzugeben, die Standard-Setup- und Shell-Benutzerkontokennwörter zu ändern, eine Verbindung zu ExtraHop Cloud Services herzustellen und eine Verbindung zu einer ExtraHop-Konsole herzustellen.

Nachdem das System lizenziert wurde und Sie sich vergewissert haben, dass Datenverkehr erkannt wurde, führen Sie die empfohlenen Verfahren in der Checkliste für die Zeit nach der Bereitstellung.

L3-Geräteerkennung konfigurieren

Sie müssen das ExtraHop-System so konfigurieren, dass es lokale und entfernte Geräte anhand ihrer IP-Adresse erkennt und verfolgt (L3 Discovery). Informationen zur Funktionsweise der Geräteerkennung 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 **Erfassung**.

3. klicken **Geräteerkennung**.
4. In der Lokale Geräteerkennung 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 **Speichern**.