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

Veröffentlicht: 2024-04-09

Die folgenden Verfahren erklären, wie Sie einen virtuellen ExtraHop 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.

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 Zugriff auf die erforderlichen Ressourcen haben und in der Lage sind, diese 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. 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 konfiguriert haben, um DNS-, HTTP-, HTTPS- und SSH-Verkehr für die ExtraHop-Verwaltung zuzulassen. siehe https://cloud.google.com/vpc/docs/using-firewalls.

Anforderungen an virtuelle Maschinen

Sie müssen einen GCP-Instanztyp bereitstellen, der Ihrer virtuellen ExtraHop-Sensorgröße am ehesten entspricht und die folgenden Modulanforderungen erfüllt.

Fühler	Module	Empfohlener Instanztyp	Festplattengröße des Datenspeichers
Enthüllen (x) EDA 1100v	EDA	n1-standard-4 (4 vCPUs und 15 GB Speicher)	61 GB
	DA + Intrusion Detection System	n2-standard-32 (32 vCPUs und 128 GB Speicher)	1400 GB

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 **Öffnen**.

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 Sie **Bild erstellen**.
3. In der Name Feld, geben Sie einen Namen zur Identifizierung des ExtraHop-Sensors ein.
4. Wählen Sie aus der Dropdownliste Quelle **Cloud-Speicherdatei**.
5. In der Cloud-Speicherdatei Abschnitt, klicken **Durchstöbern**, finde den `extrahop-eda-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. Klicken Sie **Gleichwertiger Code**.

   Auf der rechten Seite öffnet sich ein Fenster.
8. Klicken Sie im Bereich Äquivalenzcode auf **Kopieren**.
9. Klicken Sie **In Cloud Shell ausführen**.

   Der kopierte Text wird an der Eingabeaufforderung angezeigt.
10. Fügen Sie diese Option am Ende der Befehlssequenz hinzu:

    ```
    --guest-os-features=GVNIC
    ```
11. Drücken Sie die EINGABETASTE.

Nächste Schritte
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.

Erstellen Sie die Datenspeicher-Festplatte

1. Im linken Bereich auf der Rechenmaschine Seite, klicken **Festplatten**.
2. Klicken Sie **Festplatte erstellen**.

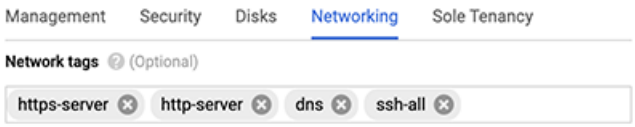
3. In der Name Feld, geben Sie einen Namen zur Identifizierung der ExtraHop-Festplatte ein.
4. Aus dem Typ der Festplattenquelle Dropdownliste, klicken Sie auf **Bild**.
5. Aus dem Festplattentyp Dropdownliste, wählen **Nichtflüchtiger Standardspeicher**.
6. Aus dem Quelle Bild-Dropdownliste, wählen Sie das Bild aus , das Sie zuvor erstellt haben.
7. In der Größe Feld, geben Sie einen Wert in GB 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 **Erstellen**.

Erstellen Sie die VM-Instanz

1. Im linken Bereich auf der Rechenmaschine seite, **VM-Instanzen**.
2. Klicken Sie **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 Dropdownliste Region Ihre geografische Region aus.
   c) Wählen Sie aus der Dropdownliste Zone einen Standort innerhalb Ihrer geografischen Zone aus.
   d) In der Konfiguration der Maschine Abschnitt, auswählen **Allgemeiner Zweck** für die Maschinenfamilie.

      Weitere Informationen zur Auswahl eines Maschinentyps finden Sie unter Anforderungen an virtuelle Maschinen.
   e) In der Bootdiskette Abschnitt, klicken Sie **Änderung**.
   f) Klicken Sie **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 Sie **Erweiterte Optionen**.
4. Klicken Sie **Netzwerke**.
5. Geben Sie im Feld Netzwerk-Tags die folgenden Tag-Namen ein, wobei Sie die einzelnen Namen durch ein Leerzeichen trennen:
   - `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. 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**.

7. Klicken Sie **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 Externes IPv4 Dropdownliste, wählen **Keine**.
   d) Konfigurieren Sie alle zusätzlichen Felder, die für Ihre Umgebung erforderlich sind.
   e) Klicken Sie **Erledigt**.

8. 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 **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 Sie **UDP-Loadbalancer**.
5. Unter Internetanschluss oder nur intern, wählen **Nur zwischen meinen VMs**.
6. Unter Backend-Typ, behalten Sie den Standardwert bei (Backend Service).
7. klicken **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 **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 **Fortfahren**.
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 **Fortfahren**.
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 **Fortfahren**.
12. Markieren Sie das Kontrollkästchen neben der VM-Instanz.
13. klicken **Fortfahren**.
14. Aus dem **Ziel des Kollektors** Dropdownliste. Wählen Sie den Load Balancer aus, den Sie zuvor erstellt haben.
15. klicken **Fortfahren**.
16. Wählen **Gesamten Verkehr spiegeln (Standard)**.
17. klicken **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 **Speichern**.