Stellen Sie den ExtraHop Flow Collector mit VMware bereit

Veröffentlicht: 2024-02-16

In diesem Handbuch wird erklärt, wie die virtuelle ExtraHop Flow Collector-Appliance (EFC 1290v) auf der VMware ESXi/ESX-Plattform bereitgestellt wird.

Der EFC 1290v ist so konzipiert, dass er eine Verbindung zu Reveal (x) 360 herstellt und den flussbasierten Datenverkehr aus Ihrem Netzwerk erfasst. Funktionen, die auf Paketsensoren verfügbar sind, wie maschinelles Lernen, regelbasierte Erkennungen, Bedrohungsinformationen, Paketanalysen und Aktivitätskarten, sind auf dem EFC 1290v nicht verfügbar. Trigger und Open Data Streams werden unterstützt.

Der EFC 1290v unterstützt die folgenden Flow-Technologien: Cisco NetFlow v5 und v9, AppFlow, IPFIX und sFlow. Weitere Informationen zum Erfassen des Datenverkehrs von Netflow- und sFlow-Geräten finden Sie unter Erfassen Sie den Datenverkehr von NetFlow- und sFlow-Geräten.

Anforderungen an virtuelle Maschinen

Ihr Hypervisor muss in der Lage sein, die folgenden Anforderungen an virtuelle Maschinen für die virtuelle Flow Collector-Appliance zu unterstützen.

- Eine vorhandene Installation von VMware ESX oder ESXi Server Version 6.5 oder höher, die die virtuelle Flow Collector-Appliance hosten kann.
- Die virtuelle Flow Collector-Appliance hat die folgenden Ressourcenanforderungen:

Gerät	CPU	RAM	Festplatte
Enthülle (x) EFC 1290v	4 Prozessorkerne mit Hyper-Threading-Unterstützung, VT-x- oder AMD-V-Technologie und 64-Bit-Architektur. Unterstützung für Streaming SIMD Extensions 4.2 (SSE4.2) und POPCNT-Anweisungen.	8 GB	Festplatte mit 46 GB oder mehr zur Datenspeicherung (Thick-Provisioning)

Die folgenden Konfigurationseinstellungen sind erforderlich, um die ordnungsgemäße Funktionalität der virtuellen Appliance sicherzustellen:

- Stellen Sie sicher, dass der VMware ESX/ESXi-Server mit dem richtigen Datum und der richtigen Uhrzeit konfiguriert ist.
- Wählen Sie immer Thick Provisioning. Der ExtraHop-Datenspeicher erfordert Low-Level-Zugriff auf das gesamte Laufwerk und kann mit Thin Provisioning nicht dynamisch wachsen. Thin Provisioning kann zu Messwertverlusten, VM-Blockups und Erfassungsproblemen führen.
- Ändern Sie bei der Erstinstallation nicht die Standardfestplattengröße. Die standardmäßige Festplattengröße gewährleistet das korrekte Lookback für ExtraHop-Metriken und die korrekte Systemfunktionalität. Wenn Ihre Konfiguration eine andere Festplattengröße erfordert, wenden Sie sich an Ihren ExtraHop-Vertreter, bevor Sie Änderungen vornehmen.
- Migrieren Sie die VM nicht. Obwohl eine Migration möglich ist, wenn sich der Datenspeicher auf einem Remote-SAN befindet, empfiehlt ExtraHop diese Konfiguration nicht. Wenn Sie die virtuelle

Maschine auf einen anderen Host migrieren müssen, fahren Sie zuerst die virtuelle Appliance herunter und migrieren Sie dann mit einem Tool wie VMware vMotion. Live-Migration wird nicht unterstützt.

Wichtig: Wenn Sie mehr als eine virtuelle ExtraHop-Appliance bereitstellen möchten, erstellen Sie die neue Instanz mit dem ursprünglichen Bereitstellungspaket oder klonen Sie eine vorhandene Instanz, die noch nie gestartet wurde.

Netzwerkanforderungen

Die folgende Tabelle enthält Anleitungen zur Konfiguration von Netzwerkports für Ihre virtuelle Flow Collector-Appliance.

Gerät	Verwaltung	Flow-Netzwerk
Enthülle (x) EFC 1290v	Ein 1-GbE-Netzwerkanschluss ist erforderlich (für die Verwaltung). Der Management-Port muss über Port 443 zugänglich sein.	Ein 1-GbE-Netzwerkanschluss oder eine virtuelle Schnittstelle ist erforderlich. Die Flow-Zielschnittstelle muss mit der Quelle des NetFlow-Datenverkehrs verbunden sein.

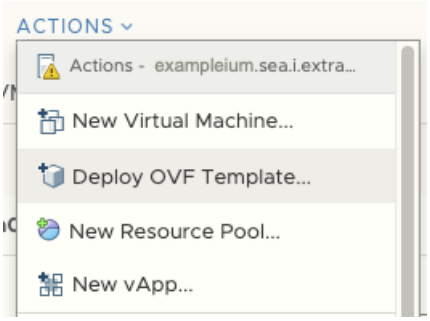
Hinweis: Für Registrierungszwecke benötigt die Flow Collector-Appliance ausgehende Konnektivität auf TCP-Port 443.

Stellen Sie die OVA-Datei über den VMware vSphere-Webclient bereit

ExtraHop verteilt das Paket der virtuellen Flow Collector-Appliance im Format Open Virtual Appliance (OVA).

Bevor Sie beginnen
Laden Sie die OVA-Datei der virtuellen Discover-Appliance 1100v Reveal (x) für VMware herunter von ExtraHop Kundenportal. Die EDA 1100V-Einheit wird automatisch auf die EFC 1290v umgestellt, nachdem Sie die Appliance mit dem 1290V-Produktschlüssel registriert haben.

1. Starten Sie den VMware vSphere Web Client und stellen Sie eine Verbindung zu Ihrem ESX-Server her.
2. Wählen Sie das Rechenzentrum aus, in dem Sie die virtuelle Flow Collector-Appliance bereitstellen möchten.
3. Wählen **OVF-Vorlage bereitstellen...** von der Aktionen Speisekarte.



4. Folgen Sie den Anweisungen des Assistenten, um die virtuelle Maschine bereitzustellen. Für die meisten Bereitstellungen sind die Standardeinstellungen ausreichend.
   a) Wählen **Lokale Datei** und dann klicken **Wählen Sie Dateien**.
   b) Wählen Sie die OVA-Datei auf Ihrem lokalen Computer aus und klicken Sie dann auf **Offen**.

c) klicken **Weiter**.
d) Geben Sie einen Namen und einen Standort für die Appliance an und klicken Sie dann auf **Weiter**.
e) Wählen Sie den Ziel-Computing-Ressourcenstandort aus, vergewissern Sie sich, dass die Kompatibilitätsprüfungen erfolgreich waren, und klicken Sie dann auf **Weiter**.
f) Überprüfen Sie die Vorlagendetails und klicken Sie dann auf **Weiter**.
g) Wählen Sie für Festplattenformat **Thick Provision Lazy Zeroed** und dann klicken **Weiter**.
h) Ordnen Sie die OVF-konfigurierten Netzwerkschnittstellenbezeichnungen den richtigen ESX-konfigurierten Schnittstellenbezeichnungen zu und klicken Sie dann auf **Weiter**.
i) Überprüfen Sie die Konfiguration und klicken Sie dann auf **Fertig stellen** um mit dem Einsatz zu beginnen. Wenn die Bereitstellung abgeschlossen ist, können Sie den eindeutigen Namen, den Sie der ExtraHop-VM-Instanz zugewiesen haben, in der Inventarstruktur für den ESX-Server sehen, auf dem sie bereitgestellt wurde.

5. Die Flow Collector-Appliance enthält eine vorkonfigurierte virtuelle Bridged-Schnittstelle mit dem Netzwerk-Label, VM-Netzwerk. Wenn Ihr ESX eine andere Schnittstellenbezeichnung hat, müssen Sie den Netzwerkadapter auf der virtuellen Flow Collector-Appliance neu konfigurieren, bevor Sie die Appliance starten.
   a) Wählen Sie den **Zusammenfassung** Tabulatur.
   b) klicken **Einstellungen bearbeiten**, wählen **Netzwerkadapter 1**, wählen Sie das richtige Netzwerklabel aus der Netzwerk-Label Dropdownliste, und klicken Sie dann auf **OK**.
6. Wählen Sie die virtuelle Flow Collector-Appliance im ESX-Inventar aus und wählen Sie dann **Konsole öffnen** von der Aktionen Speisekarte.
7. Klicken Sie auf das Konsolenfenster und drücken Sie dann die EINGABETASTE, um die IP-Adresse anzuzeigen.

   Hinweis: DHCP ist standardmäßig auf der virtuellen ExtraHop-Appliance aktiviert. Informationen zur Konfiguration einer statischen IP-Adresse finden Sie in Eine statische IP-Adresse konfigurieren Abschnitt.
8. Konfigurieren Sie in VMware ESXi den virtuellen Switch so, dass er Datenverkehr empfängt, und starten Sie die Appliance neu, um die Änderungen zu sehen.

Konfigurieren Sie eine statische IP-Adresse über die CLI

Das ExtraHop-System wird geliefert mit DHCP aktiviert. Wenn Ihr Netzwerk DHCP nicht unterstützt, wird keine IP-Adresse abgerufen, und Sie müssen eine statische Adresse manuell konfigurieren.

1. Greifen Sie über eine SSH-Verbindung zur konfigurierten IP-Adresse, zur vSphere-Webkonsole oder zur VMware Remote Console auf die CLI zu.
2. Geben Sie in der Anmeldeaufforderung Folgendes ein `Schale`, und drücken Sie dann die EINGABETASTE.
3. Geben Sie an der Passwortaufforderung Folgendes ein `Standard`, und drücken Sie dann die EINGABETASTE.
4. Führen Sie die folgenden Befehle aus, um die statische IP-Adresse zu konfigurieren:
   a) Aktiviere privilegierte Befehle:

   ```
   enable
   ```

   b) Geben Sie an der Passwortaufforderung Folgendes ein `Standard`, und drücken Sie dann die EINGABETASTE.
   c) Rufen Sie den Konfigurationsmodus auf:

   ```
   configure
   ```

d) Rufen Sie den Schnittstellenkonfigurationsmodus auf:

```
interface
```

e) Starte den `ip` Befehl und spezifizieren Sie die IP-Adresse und DNS Einstellungen im folgenden Format:

`ip ipaddr <ip_address> <netmask> <gateway> <dns_server>`

Zum Beispiel:

```
ip ipaddr 10.10.2.14 255.255.0.0 10.10.1.253 10.10.1.254
```

f) Verlassen Sie den Schnittstellenkonfigurationsmodus:

```
exit
```

g) Speichern Sie die laufende Konfigurationsdatei:

```
running_config save
```

h) Typ `y`, und drücken Sie dann die EINGABETASTE.