Stellen Sie den ExtraHop Packetstore mit VMware bereit

Veröffentlicht: 2024-07-17

In diesem Handbuch wird erklärt, wie der virtuelle ExtraHop Packetstore (ETA 1150v und ETA 6150v) auf der VMware ESXi/ESX-Plattform bereitgestellt wird.

Anforderungen an virtuelle Maschinen

Ihre Umgebung muss die folgenden Anforderungen erfüllen, um einen virtuellen Packetstore bereitzustellen:

- Eine bestehende Installation von VMware ESX oder ESXi Server Version 6.5 oder höher, die den virtuellen Packetstore hosten kann. Die virtuellen Paketspeicher haben die folgenden Ressourcenanforderungen:

ETA 1150 v	ETA 6150 v
2 vCPUs	18 vCPUs
16 GB RAM	64 GB RAM
4 GB Systemfestplatte	4 GB Systemfestplatte 250 GB für eine zweite Systemfestplatte
1 TB für eine Packetstore-Festplatte Bei Bedarf können Sie die Festplattengröße vor der Bereitstellung zwischen 50 GB und 4 TB neu konfigurieren.	Packetstore-Diskette Sie müssen zum Zeitpunkt der Bereitstellung manuell ein drittes virtuelles Laufwerk zwischen 1 TB und 25 TB hinzufügen, um Paketdaten zu speichern. Sie können bis zu 16 virtuelle Laufwerke hinzufügen, um die Speicherkapazität und Leistung des Packetstore zu erhöhen. Die Gesamtkapazität aller Festplatten darf 25 TB nicht überschreiten.

  Die Hypervisor-CPU sollte Streaming SIMD Extensions 4.2 (SSE4.2) und POPCNT-Befehle unterstützen.

Folgen Sie diesen Richtlinien, um sicherzustellen, dass der virtuelle Packetstore ordnungsgemäß funktioniert:

- Wenn Sie mehr als einen virtuellen Packetstore bereitstellen möchten, erstellen Sie die neue Instanz mit dem ursprünglichen Bereitstellungspaket oder klonen Sie eine vorhandene Instanz, die noch nie gestartet wurde.
- Wählen Sie immer Thick Provisioning. Der ExtraHop-Packetstore erfordert einen Low-Level-Zugriff auf das gesamte Laufwerk und kann mit Thin Provisioning nicht dynamisch wachsen.
- Ändern Sie die Standardfestplattengröße nicht, nachdem der Packetstore bereitgestellt wurde. Machen Sie das virtuelle Laufwerk vor der Bereitstellung entweder kleiner oder größer als die Standardgröße von 1 TB. Wir unterstützen nicht, die ursprüngliche Festplattengröße zu ändern oder zusätzliche Festplatten hinzuzufügen, nachdem die virtuelle Maschine bereitgestellt wurde.
- Migrieren Sie die virtuelle Maschine nicht von einem Host oder Speicherort zu einem anderen. Obwohl eine Migration möglich ist, wenn sich der Datenspeicher auf einem Remote-SAN befindet, empfiehlt ExtraHop diese Konfiguration nicht. Wenn Sie die VM nach der Bereitstellung auf einen anderen Host

migrieren müssen, fahren Sie zuerst den virtuellen Packetstore herunter und migrieren Sie dann mit einem Tool wie VMware vMotion. Live-Migration wird nicht unterstützt.
- Für maximale Leistung und Kompatibilität setzen Sie Sensoren und Paketspeicher im selben Rechenzentrum.

Überlegungen zur Leistung

Wichtig: Die ETA 6150v ist in der Lage, Pakete mit einem Durchsatz von 10 Gbit/s auf der Festplatte zu erfassen, jedoch nur mit ordnungsgemäß bereitgestellter Netzwerk- und Festplattenbandbreite. Um bei der Erfassung von Datenverkehr von physischen Netzwerkschnittstellen eine Spitzenleistung zu erzielen, müssen Sie sicherstellen, dass für die ETA 6150v eine physische 10-GbE-Netzwerkkarte (oder eine entsprechende verfügbare Bandbreite über mehrere physische 10-GbE-NICs) vorgesehen ist. Ebenso müssen Sie sicherstellen, dass dem ETA 6150v 10 Gbit/s Festplattenbandbreite zugewiesen werden. Bei HDDs erfordert diese Festplattenbandbreite in der Regel die Bereitstellung von 12 oder mehr Festplatten für den virtuellen Packetstore. Bei Speicherkonfigurationen mit einer kleinen Anzahl von Festplatten oder mit einer großen Anzahl von Festplatten, die von mehreren virtuellen Paketspeichern gemeinsam genutzt werden, ist es unwahrscheinlich, dass die PCAP mit 10 Gbit/s aufrechterhalten wird.

Netzwerkanforderungen

Paketshop	Intra-VM	Extern
ETA 1150 v	Für die Verwaltung ist ein 1-Gbit/s-Ethernet-Netzwerkanschluss erforderlich. Ein eigener Port ist nicht erforderlich. Sie können dieselbe physische Netzwerkkarte wie andere VMs in Ihrer Umgebung nutzen. Der Management-Port muss über Port 443 zugänglich sein.	Ein 1-Gbit/s-Ethernet-Netzwerkanschluss für den physischen Port-Mirror. Wir empfehlen Ihnen, den Feed des Datenverkehrs zu duplizieren, der an die Sensor um den ExtraHop-Workflow zu nutzen.
ETA 6150 v	Für die Verwaltung ist ein 1-Gbit/s-Ethernet-Netzwerkanschluss erforderlich. Ein eigener Port ist nicht erforderlich. Sie können dieselbe physische Netzwerkkarte wie andere VMs in Ihrer Umgebung nutzen. Der Management-Port muss über Port 443 zugänglich sein.	Ein 10-Gbit/s-Ethernet-Netzwerkanschluss für den physischen Port-Mirror. Um einen Durchsatz von 10 Gbit/s zu erreichen, benötigen Sie auf Ihrem ESXi-Server mindestens 10 GbE NIC-Ports. Wir empfehlen Ihnen, den Feed des Datenverkehrs zu duplizieren, der an die Sensor um den ExtraHop-Workflow zu nutzen.

Schnittstellenmodi

Jede Schnittstelle kann wie folgt konfiguriert werden:

Schnittstelle	Schnittstellenmodus
Schnittstelle 1	• Deaktiviert • Verwaltung

Schnittstelle	Schnittstellenmodus
	• Geschäftsleitung + RPCAP/ERSPAN/VXLAN/ GENEVE Target
Schnittstelle 2	• Deaktiviert • Überwachung (nur Empfang) • Verwaltung • Geschäftsleitung + RPCAP/ERSPAN/VXLAN/ GENEVE Target • Hochleistungs-ERSPAN-Target (ETA 6150v)
Schnittstelle 3 (ETA 6150v)	• Deaktiviert • Überwachung (nur Empfang) • Verwaltung • Geschäftsleitung + RPCAP/ERSPAN/VXLAN/ GENEVE Target • Leistungsstarkes ERSPAN-Target
Schnittstelle 4 (ETA 6150v)	• Deaktiviert • Überwachung (nur Empfang) • Verwaltung • Geschäftsleitung + RPCAP/ERSPAN/VXLAN/ GENEVE Target • Leistungsstarkes ERSPAN-Target

Das ExtraHop-System unterstützt die folgenden ERSPAN-Implementierungen:

- ERSPAN Typ I
- ERSPAN Typ II
- ERSPAN Typ III
- Transparentes Ethernet-Bridging, eine ERSPAN-ähnliche Kapselung, die häufig in virtuellen Switch-Implementierungen wie VMware VDS und Open vSwitch zu finden ist.

Virtual Extensible LAN (VXLAN) -Pakete werden auf dem UDP-Port 4789 empfangen.

Generic Network Virtualization Encapsulation (GENEVE) -Pakete werden auf dem UDP-Port 6081 empfangen.

Stellen Sie die OVA-Datei über den VMware vSphere Web Client bereit

ExtraHop verteilt das virtuelle Packetstore-Paket im Format Open Virtual Appliance (OVA).

Bevor Sie beginnen
Falls Sie dies noch nicht getan haben, laden Sie die OVA-Datei für VMware von der ExtraHop Kundenportal.

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 den virtuellen Packetstore bereitstellen möchten.
3. Wählen **OVF-Vorlage bereitstellen...** aus dem 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 **Stöbern...**.
   b) Wählen Sie die OVA-Datei auf Ihrem lokalen Computer aus und klicken Sie dann auf **Offen**.

c) klicken **Weiter**.
d) Überprüfen Sie die Details des virtuellen Packetstore und klicken Sie dann auf **Weiter**.
e) Geben Sie einen Namen und einen Speicherort für den Packetstore an und klicken Sie dann auf **Weiter**.
f) Wählen Sie einen Ressourcenstandort aus und klicken Sie dann auf **Weiter**.
g) Wählen Sie für das 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**.

5. Überprüfen Sie die Konfiguration und führen Sie dann die folgenden Schritte aus:

- Für die ETA 1150v

  Wenn Sie die Größe der Packetstore-Festplatte nicht ändern möchten, wählen Sie die Nach der Bereitstellung einschalten Checkbox und dann klicken **Fertig stellen** um mit dem Einsatz zu beginnen.

  Wenn Sie die Größe der Packetstore-Festplatte ändern möchten:

  1. klicken **Fertig stellen** um mit dem Einsatz zu beginnen. Wenn die Bereitstellung abgeschlossen ist, wählen Sie **Einstellungen bearbeiten** von der Aktionen Speisekarte.
  2. Geben Sie eine neue Größe in das Festplatte 2 Feld. Die minimale Festplattengröße beträgt 50 GB und die maximale Größe 4 TB.
  3. Aus dem Aktionen Menü, wählen **Leistung** > **Einschalten**.

- Für die ETA 6150v

  1. Aus dem **Aktionen** Drop-down-Liste, wählen **Einstellungen bearbeiten...** um die Packetstore-Diskette zu konfigurieren.
  2. Aus dem **Neues Gerät** Drop-down-Liste, wählen **Neue Festplatte**, und klicken Sie dann **Hinzufügen**.
  3. Geben Sie eine Größe in das Festplatte 3 Feld. Die minimale Festplattengröße beträgt 1 TB und die maximale Festplattengröße beträgt 25 TB.
  4. Geben Sie einen Datenspeicher für die Packetstore-Festplatte an. Um sicherzustellen, dass die Trace-Appliance Pakete mit maximalem Durchsatz schreiben kann, ohne dass es zu Konflikten durch andere Workloads kommt, empfiehlt ExtraHop, die Festplatte 3 auf einem anderen Datenspeicher als die Festplatten 1 und 2 zu platzieren. Der Datenspeicher muss durch ein Hochleistungsfestplattenvolume gesichert werden, das für die Packetstore-Arbeitslast reserviert ist und nicht mit anderen virtuellen Maschinen gemeinsam genutzt wird.
  5. In der Modus Abschnitt, wählen **Unabhängig** und wählen Sie dann **Hartnäckig**.
  6. Wiederholen Sie die Schritte b bis e, um weitere Packetstore-Festplatten hinzuzufügen.
  7. klicken **Fertig stellen** um mit dem Einsatz zu beginnen.
  8. Suchen Sie die virtuelle ETA 6150v-Maschine im vSphere Web Client-Inventar.
  9. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und klicken Sie **Einstellungen bearbeiten**.
  10. klicken **VM-Optionen** und dann klicken **Fortgeschritten**.
  11. Wählen **Mittel** aus dem Drop-down-Menü Latenzsensitivität.
  12. klicken **OK**.
  13. Wählen Sie im Menü Aktionen **Strom > Einschalten**.

6. Wählen Sie den virtuellen Packetstore 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. DHCP ist standardmäßig im virtuellen Packetstore aktiviert. Informationen zur Konfiguration einer statischen IP-Adresse finden Sie in Konfigurieren Sie eine statische IP-Adresse über die CLI Abschnitt.
8. Beginnen Sie mit dem Senden von Paketen an Ihren oder Ihre Monitoring-Ports. Verbinden Sie entweder einen physischen Ethernet-Port über einen virtuellen Switch mit dem Monitoring-Port, oder

konfigurieren Sie ERSPAN-, RPCAP- oder VXLAN-Quellen, um Datenverkehr an die entsprechende Packetstore-IP-Adresse zu senden.

Konfigurieren Sie eine statische IP-Adresse über die CLI

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

Sie können eine statische IP-Adresse für das ExtraHop-System manuell über die CLI konfigurieren.

Wichtig: Wir empfehlen dringend Konfiguration eines eindeutigen Hostnamens. Wenn sich die System-IP-Adresse ändert, kann die ExtraHop-Konsole die Verbindung zum System einfach über den Hostnamen wiederherstellen.

1. Greifen Sie über eine SSH-Verbindung auf die CLI zu, indem Sie eine USB-Tastatur und einen SVGA-Monitor an die physische ExtraHop-Appliance anschließen, oder über ein serielles RS-232-Kabel (Nullmodem) und ein Terminalemulatorprogramm. Stellen Sie den Terminalemulator auf 115200 Baud mit 8 Datenbits, ohne Parität, 1 Stoppbit (8N1) und deaktivierter Hardware-Flusskontrolle ein.
2. Geben Sie an der Anmeldeaufforderung 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) Geben Sie die IP-Adresse und die DNS-Einstellungen im folgenden Format an:
   `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 ENTER.

Den Packetstore konfigurieren

Öffnen Sie einen Webbrowser, melden Sie sich über die konfigurierte IP-Adresse bei den Administrationseinstellungen im Packetstore an und führen Sie die folgenden Verfahren aus. Der Standard-Anmeldename ist `setup` und das Passwort ist `default`.

- Registrieren Sie Ihr ExtraHop-System
- Sensoren und Konsole mit dem Packetstore verbinden
- Überprüfen Sie die ExtraHop Checkliste nach der Bereitstellung und konfigurieren Sie zusätzliche Packetstore-Einstellungen.

Sensoren und Konsole mit dem Packetstore verbinden

Bevor Sie Pakete abfragen können, müssen Sie die Konsole und alle Sensoren zum Packetstore.

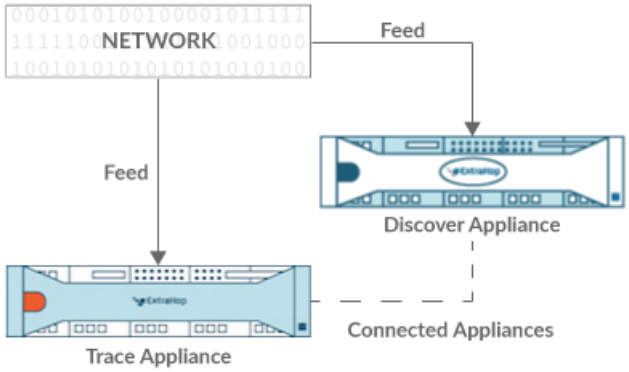

Abbildung 1: An einen Sensor angeschlossen

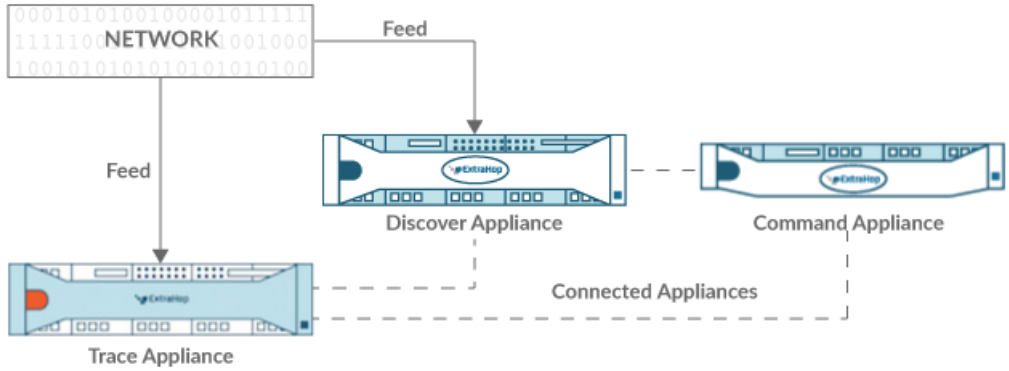

Abbildung 2: Mit Sensor und Konsole verbunden

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Packetstore-Einstellungen Abschnitt, klicken Sie **Synchronisiere Packetstores**.
3. In der Hostname des Paketspeichers Feld, geben Sie den Hostnamen oder die IP-Adresse des Packetstore ein.
4. Klicken Sie **Paar**.
5. Beachten Sie die Informationen in der Fingerabdruck Feld, und überprüfen Sie dann, ob der auf dieser Seite aufgeführte Fingerabdruck mit dem Packetstore-Fingerabdruck auf der Seite Fingerprint in den Administrationseinstellungen des Packetstore übereinstimmt.
6. In der Packetstore-Setup-Passwort Feld, geben Sie das Passwort des Packetstore ein `setup` Nutzer.
7. Klicken Sie **Verbinden**.
8. Um weitere Paketspeicher zu verbinden, wiederholen Sie die Schritte 2 bis 7.

   Hinweis Sie können einen Sensor an zwanzig oder weniger Packetstores anschließen, und Sie können eine Konsole an fünfzig oder weniger Packetstores anschließen.
9. Wenn du eine hast Konsole, melden Sie sich in den Administrationseinstellungen auf der Konsole und wiederholen Sie die Schritte 3 bis 7 für alle Packetstores.

Überprüfen Sie die Konfiguration

Nachdem Sie den Packetstore bereitgestellt und konfiguriert haben, stellen Sie sicher, dass Pakete gesammelt werden .

Bevor Sie beginnen
Sie müssen über ein Mindestbenutzerrecht von verfügen **Pakete ansehen und herunterladen** um dieses Verfahren durchzuführen.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Vergewissern Sie sich, dass **Pakete** Das Menü erscheint im oberen Menü.

3. Klicken Sie **Pakete** um eine neue Paketabfrage zu starten.
   Sie sollten jetzt eine Liste der gesammelten Pakete sehen.

Wenn der Menüpunkt Pakete nicht angezeigt wird, rufen Sie erneut die Sensoren und Konsole mit dem Packetstore verbinden Abschnitt. Wenn bei einer Paketabfrage keine Ergebnisse zurückgegeben werden, überprüfen Sie Ihre Netzwerkeinstellungen. Wenn eines der Probleme weiterhin besteht, wenden Sie sich an ExtraHop-Unterstützung.