Stellen Sie den ExtraHop-Sensor auf VMware bereit

Veröffentlicht: 2024-11-02

In den folgenden Verfahren wird erläutert, wie ein virtueller ExtraHop-Sensor auf einer VMware ESXi/ESX-Plattform bereitgestellt wird. Sie müssen Erfahrung mit der Bereitstellung virtueller Maschinen in vSphere 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: Durchsatz kann beeinträchtigt werden, wenn mehr als ein Modul auf dem Sensor aktiviert ist.

Anforderungen an das System

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

- Sie müssen mit der Verwaltung von VMware vSphere vertraut sein.

  Hinweis: Die Bilder in diesem Handbuch sind nur Beispiele, und einige der Menüoptionen haben sich möglicherweise geändert.
- Sie benötigen die ExtraHop-Bereitstellungsdatei, die auf der ExtraHop Kundenportal
- Du musst einen ExtraHop haben Sensor Produktschlüssel.
- Sie sollten ein Upgrade auf den neuesten Patch für die vSphere-Umgebung durchführen, um bekannte Probleme zu vermeiden.

Anforderungen an virtuelle Maschinen

Sie müssen eine virtuelle VMware vSphere-Maschine bereitstellen, die der Größe des virtuellen ExtraHop-Sensors am ehesten entspricht und die Modulanforderungen erfüllt.

Fühler	Module	CPU	RAM	Festplatte
Enthüllen (x) EDA 1100v	NDR, NPM	4 Prozessorkerne mit Hyper-Threading-Unterstützung, VT-x- oder AMD-V-Technologie und 64-Bit-Architektur. Unterstützung für Streaming	8 GB	Festplatte mit 46 GB oder mehr zur Datenspeicherung (Thick-Provisioning) 250 GB oder weniger Festplatte für

Fühler	Module	CPU	RAM	Festplatte
		SIMD Extensions 4.2 (SSE4.2) und POPCNT-Anweisungen.		Paketerfassungen (Thick-Provisioning)
EDA 6100 v	NDR, NPM	18 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.	64 GB	1 TB oder mehr Festplatte für Datenspeicher (Thick-Provisioning) Festplatte mit 500 GB oder weniger für Paketerfassungen (Thick-Provisioning)
EDA 6320v	NDR, NPM, Intrusion Detection System	32 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.	96 GB	1,4 TB oder größere Festplatte für Datenspeicher (Thick-Provisioning) Festplatte mit 500 GB oder weniger für Paketerfassungen (Thick-Provisioning)
EDA 8320v	NDR, NPM, Intrusion Detection System	64 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.	192 GB	Festplatte mit 2 TB oder mehr für Datenspeicher (Thick-Provisioning) Festplatte mit 500 GB oder weniger für Paketerfassungen (Thick-Provisioning)

Hypervisor-Spezifikationen

Ihr Hypervisor muss in der Lage sein, die folgenden Spezifikationen für den virtuellen Sensor zu unterstützen.

- VMware ESX/ESXi Server Version 6.5 oder höher
- VMware vSphere Client zur Bereitstellung der OVF-Datei und zur Verwaltung der virtuellen Maschine
- (Optional) Wenn Sie Paketerfassungen aktivieren möchten, konfigurieren Sie während der Bereitstellung ein zusätzliches Speicherlaufwerk

Zusätzliche Richtlinien

Um die einwandfreie Funktion des virtuellen Sensor 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 VM auf einen anderen Host migrieren müssen, fahren Sie zuerst den virtuellen Sensor herunter und migrieren Sie dann mit einem Tool wie VMware vMotion. Live-Migration wird nicht unterstützt.

Wichtig: Wenn Sie mehr als einen virtuellen ExtraHop-Sensor 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 Netzwerkanschlüssen für Ihren virtuellen Sensor.

Sensor	Module	Verwaltung	Überwachen
EDA 1100 V	NDR, NPM	Ein 1-GbE-Netzwerkanschluss ist erforderlich (für die Verwaltung). Die Verwaltungsschnittstelle muss über Port 443 zugänglich sein. Die Verwaltungsschnittstelle kann als zusätzliches ERSPAN/RPCAP-Ziel konfiguriert werden.	Für den physischen Port-Mirror wird ein 1-GbE-Netzwerkanschluss empfohlen. Die physische Portspiegelschnittstelle muss mit dem Port-Mirror-Ziel auf dem Switch verbunden sein.
EDA 6100 v	NDR, NPM	Ein 1-GbE-Netzwerkanschluss ist erforderlich (für die Verwaltung). Die Verwaltungsschnittstelle muss über Port 443 zugänglich sein. Die Verwaltungsschnittstelle kann als zusätzliches ERSPAN/RPCAP-Ziel konfiguriert werden.	Für den physischen Port-Mirror wird ein 10-GbE-Netzwerkanschluss empfohlen. Die physische Portspiegelschnittstelle muss mit dem Port-Mirror-Ziel auf dem Switch verbunden sein. Optional können Sie ein bis drei zusätzliche Netzwerkschnittstellen für den Empfang von Paketüberwachungsdatenverkehr konfigurieren. Das Hinzufügen zusätzlicher

Sensor	Module	Verwaltung	Überwachen
			Paketüberwachungsschnittstellen kann die Gesamtleistung beeinträchtigen.
EDA 6320v	NDR, NPM, Intrusion Detection System	Ein 1-GbE-Netzwerkanschluss ist erforderlich (für die Verwaltung). Die Verwaltungsschnittstelle muss über Port 443 zugänglich sein. Die Verwaltungsschnittstelle kann als zusätzliches ERSPAN/RPCAP-Ziel konfiguriert werden.	Für den physischen Port-Mirror wird ein 10-GbE-Netzwerkanschluss empfohlen. Die physische Portspiegelschnittstelle muss mit dem Port-Mirror-Ziel auf dem Switch verbunden sein.
EDA 8320v	NDR, NPM, Intrusion Detection System	Ein 1-GbE-Netzwerkanschluss ist erforderlich (für die Verwaltung). Die Verwaltungsschnittstelle muss über Port 443 zugänglich sein. Die Verwaltungsschnittstelle kann als zusätzliches ERSPAN/RPCAP-Ziel konfiguriert werden.	Für den physischen Port-Mirror wird ein Netzwerkanschluss mit 25 GbE oder höher empfohlen. Die physische Portspiegelschnittstelle muss mit dem Port-Mirror-Ziel auf dem Switch verbunden sein.

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.

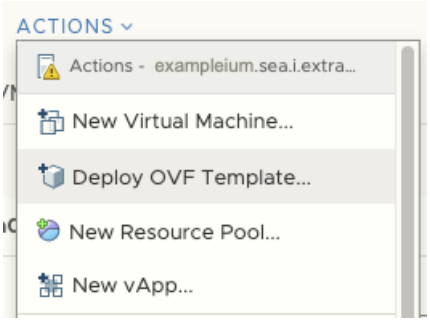
Hinweis: Für Registrierungszwecke benötigt der virtuelle Sensor Outbound DNS Konnektivität auf UDP-Port 53, sofern sie nicht von einer ExtraHop-Konsole verwaltet wird.

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

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

Bevor Sie beginnen
Falls Sie dies noch nicht getan haben, laden Sie die ExtraHop-OVA-Datei für virtuelle Sensor 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 das virtuelle bereitstellen möchten Sensor.
3. Aus dem Aktionen Menü, wählen **OVF-Vorlage bereitstellen...**.



4. Folgen Sie den Anweisungen des Assistenten, um die virtuelle Maschine bereitzustellen.

   Für die meisten Bereitstellungen sind die Standardeinstellungen ausreichend.

   a) Wählen Sie Lokale Datei und klicken Sie dann **Wählen Sie Dateien**.
   b) Wählen Sie die OVA-Datei auf Ihrem lokalen Computer aus und klicken Sie dann auf **Offen**.
   c) Klicken Sie **Als Nächstes**.
   d) Geben Sie einen Namen und einen Speicherort für das Sensor und klicken Sie dann **Als Nächstes**.
   e) Wählen Sie den Zielspeicherort der Rechenressource aus, überprüfen Sie, ob die Kompatibilitätsprüfungen erfolgreich waren, und klicken Sie dann auf **Als Nächstes**.
   f) Überprüfen Sie die Vorlagendetails und klicken Sie dann auf **Als Nächstes**.
   g) Für Festplattenformat, wählen **Thick Provision Lazy Zeroed** und klicken Sie dann **Als Nächstes**.
   h) Ordnen Sie die OVF-konfigurierten Netzwerkschnittstellenbezeichnungen den richtigen ESXi-konfigurierten Schnittstellenbezeichnungen zu und klicken Sie dann auf **Als Nächstes**.
   i) Überprüfen Sie die Konfiguration und klicken Sie dann auf **Fertig stellen** um mit der Bereitstellung zu beginnen.
   Wenn die Bereitstellung abgeschlossen ist, können Sie den eindeutigen Namen, den Sie der ExtraHop-VM-Instanz zugewiesen haben, im Inventarbaum des ESX-Servers sehen, auf dem sie bereitgestellt wurde.
5. Konfigurieren Sie den Netzwerkadapter auf dem virtuellen Sensor, falls erforderlich.

   Das Sensor enthält eine vorkonfigurierte überbrückte virtuelle Schnittstelle mit dem Netzwerklabel, VM-Netzwerk. Wenn Ihr ESX also eine andere Schnittstellenbezeichnung hat, müssen Sie die virtuelle neu konfigurieren Sensor Netzwerkadapter vor dem Start des Sensor.

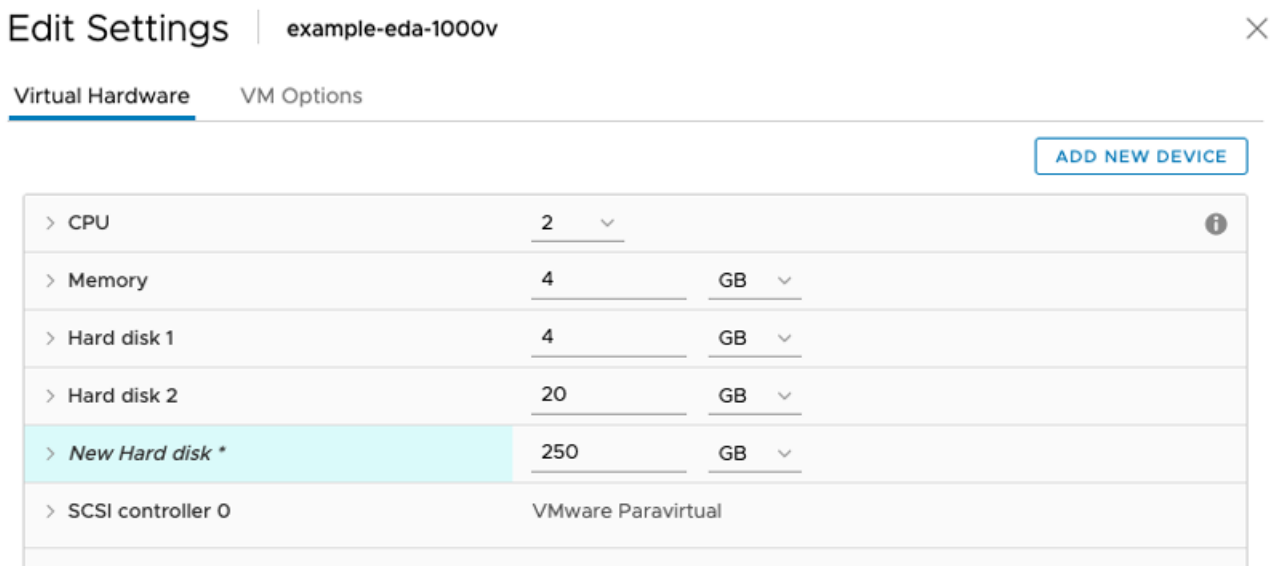
   a) Wählen Sie die Zusammenfassung Tab.
   b) Klicken Sie **Einstellungen bearbeiten** und wähle **Netzwerkadapter 1**.
   c) Aus dem **Netzwerk-Label** Dropdownliste, wählen Sie die richtige Netzwerkbezeichnung aus, und klicken Sie dann auf **OK**.
6. Wählen Sie das virtuelle Sensor im ESX-Inventar und dann aus dem Aktionen Menü, wählen **Konsole öffnen**.
7. Klicken Sie auf das Konsolenfenster und drücken Sie dann die EINGABETASTE, um die IP-Adresse anzuzeigen.

   Hinweis: DHCP ist standardmäßig auf dem virtuellen ExtraHop-Sensor aktiviert. Informationen zum Konfigurieren einer statischen IP-Adresse finden Sie unter Konfigurieren Sie eine statische IP-Adresse über die CLI.
8. Konfigurieren Sie in VMware ESXi den virtuellen Switch so, dass er Datenverkehr empfängt, und starten Sie ihn neu, um die Änderungen zu sehen.

Fügen Sie eine Paketerfassungsfestplatte in VMware vSphere hinzu

Wenn dein Sensor ist für die PCAP lizenziert. Sie müssen eine zusätzliche Festplatte zum Speichern der Paketerfassungsdateien konfigurieren.

1. Wählen Sie Ihre Sensor virtuelle Maschine in der Inventarliste der virtuellen Maschinen.
2. Aus dem **Aktionen** Dropdownliste, wählen **Einstellungen bearbeiten**.
3. Klicken Sie **Neues Gerät hinzufügen** und klicken Sie dann auf **Festplatte**.
4. In der Neue Festplatte Feld, geben Sie eine Festplattengröße ein, die auf dem Sensor basiert, den Sie einsetzen:
   - 250 GB für den EDA 1100v
   - 500 GB für den EDA 6100v
   - 500 GB für den EDA 6320v
   - 500 GB für den EDA 8320v



5. Erweitern Sie die Neue Festplatte Einstellungen und bestätige das **Thick Provision Lazy Zeroed** ist ausgewählt für Festplattenbereitstellung.

   Die übrigen Festplatteneinstellungen müssen nicht geändert werden.
6. Klicken Sie **OK**.

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 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. Der Standard-Anmeldename ist `setup` und das Passwort ist `default`.
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.

Verwandte Dokumentation

Für Informationen zur Konfiguration von RSPAN, ERSPAN und RPCAP Informationen zur Überwachung von Remote-Geräten finden Sie in den folgenden Themen.

- RSPAN mit VMware konfigurieren
- ERSPAN mit VMware konfigurieren
- Konfigurieren Sie ERSPAN mit dem Nexus 1000V

- Paketweiterleitung mit RPCAP

Informationen zur Spiegelung des Datenverkehrs mit VMware finden Sie unter Mirror Wire-Daten mit VMware.