

Stellen Sie den IDS-Sensor mit VMware bereit

Veröffentlicht: 2024-09-25

Veröffentlicht: 2024-09-25

Die Sensoren des Intrusion Detection Systems (Intrusion Detection System) lassen sich in Paketsensoren integrieren, um Erkennungen auf der Grundlage von branchenüblichen IDS-Signaturen zu generieren. In diesem Handbuch wird erklärt, wie der IDS-Sensor mit VMware bereitgestellt wird.

Bevor Sie beginnen

- Sie müssen mit der Verwaltung von VMware vertraut sein. Die Bilder in diesem Handbuch stammen aus VMware Version 6.7, und einige der Menüauswahlen haben sich möglicherweise geändert.
- Wir empfehlen, ein Upgrade auf den neuesten Patch für die vSphere-Umgebung durchzuführen, um bekannte Probleme zu vermeiden.

In diesem Handbuch wird erklärt, wie die folgenden virtuellen ExtraHop-Sensoren auf der VMware ESXi/ESX-Plattform bereitgestellt werden:

- Intrusion Detection System 6280v


Anforderungen an virtuelle Maschinen

Ihr Hypervisor muss die folgenden Spezifikationen für den virtuellen Sensor unterstützen können.

- VMware ESX/ESXi-Server Version 6.5 oder höher
- vSphere-Client zur Bereitstellung der OVF-Datei und zur Verwaltung der virtuellen Maschine
- (Optional) Wenn Sie Paketerfassungen aktivieren möchten, konfigurieren Sie während der Bereitstellung eine zusätzliche Speicherfestplatte
- Die folgende Tabelle enthält die Serverhardwareanforderungen für jedes Discover-Appliance-Modell:

Fühler	CPU	RAM	Festplatte
Intrusion Detection System 1280v	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-Befehle.	8 GB	Festplatte mit 46 GB oder mehr für Datenspeicherung (Thick-Provisioning) 250 GB oder weniger Festplatte für Paket (Thick-Provisioning)
Intrusion Detection System 6280v	16 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-Befehle.	64 GB	Festplatte mit 1 TB oder mehr für Datenspeicherung (Thick-Provisioning) Festplatte mit 500 GB oder weniger für Paketerfassung (Thick-Provisioning)


Um die korrekte Funktionalität 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 einen Low-Level-Zugriff auf das gesamte Laufwerk und kann mit Thin Provisioning nicht dynamisch wachsen. Thin Provisioning kann zum Verlust von Metrik, zum Sperren virtueller Rechner und zu Problemen bei der Erfassung führen.
 - Ändern Sie die Standardfestplattengröße bei der Erstinstallation nicht. Die standardmäßige Festplattengröße gewährleistet den korrekten Lookback für ExtraHop-Metriken und die korrekte Systemfunktionalität. Wenn Ihre Konfiguration eine andere Festplattengröße erfordert, wenden Sie sich an Ihren ExtraHop-Ansprechpartner, 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 den IDS-Sensor.

Fühler	Verwaltung	Überwachen
Intrusion Detection System 680v	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. Der VMware ESX-Server muss Netzwerkschnittstellentreiber unterstützen. Optional können Sie 1–3 1-GbE-Netzwerkanschlüsse für den Empfang von Paketüberwachungsdatenverkehr konfigurieren.

-  **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-Webclient bereit

ExtraShop vertreibt das Virtuelle Sensor Paket im Format Open Virtual Appliance (OVA).

Bevor Sie beginnen

Falls Sie dies noch nicht getan haben, laden Sie die virtuelle ExtraHop-Sensor-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 das virtuelle System bereitstellen möchten Sensor.
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 Speicherort für Sensor und dann klicken **Weiter**.
 - e) Wählen Sie den Speicherort der Ziel-Rechenressource aus, stellen Sie sicher, 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 Sensor enthält eine vorkonfigurierte virtuelle Bridged-Schnittstelle mit dem Netzwerk-Label, VM-Netzwerk. Wenn Ihr ESX eine andere Schnittstellenbezeichnung hat, müssen Sie den Netzwerkadapter auf dem virtuellen Computer neu konfigurieren Sensor vor dem Start des Sensor.
 - 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 das virtuelle Sensor im ESX-Inventar 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 dem virtuellen ExtraHop-Sensor 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 ihn neu, um die Änderungen zu sehen.

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.

Das System konfigurieren

Gehen Sie wie folgt vor, um den IDS-Sensor zu konfigurieren.

1. [Registrieren Sie Ihr ExtraHop-System](#).
2. [Stellen Sie eine Verbindung zu ExtraHop Cloud Services her](#).
3. Verbinden Sie Ihre Konsole mit dem Sensor.
 - Informationen zum Herstellen einer Verbindung zu einer selbstverwalteten Konsole finden Sie unter [Eine ExtraHop-Konsole mit einem ExtraHop-Sensor verbinden](#).
 - Um eine Verbindung zu RevealX 360 herzustellen, siehe [Stellen Sie über selbstverwaltete Sensoren eine Verbindung zu RevealX 360 her](#).
4. Verbinden Sie den IDS-Sensor mit einer Standort.

- Für RevealX Enterprise
 1. Klicken Sie auf der Seite „Verbundene Geräte verwalten“ der Konsole auf **Aktionen** neben dem IDS-Sensor und dann auf **Seite beitreten** von der Appliance-Aktionen Dropdownliste.
 2. Aus dem Verbundene Seite In der Dropdownliste klicken Sie auf den Namen der Standort, der Sie beitreten möchten. Sie müssen einer Standort beitreten, die denselben Netzwerkfeed wie der IDS-Sensor hat.
 3. Klicken Sie **Seite beitreten**.
- Für RevealX 360
 1. Auf dem RevealX 360 **Verwaltung > Sensoren** Seite, wählen Sie das Kontrollkästchen neben dem Namen des IDS-Sensors aus.
 2. Auf dem Angaben zum Sensor Wählen Sie im Bereich den Namen der Standort, der Sie beitreten möchten, aus dem **Verbundene Seite** Dropdownliste. Sie müssen einer Standort beitreten, die denselben Netzwerkfeed wie der IDS-Sensor hat.
 3. Klicken Sie **Seite beitreten**.
- 5. Optional: Wählen Sie die IDS-Erkennungen aus **Tuning-Parameter** [↗](#) um die Erkennung von eingehender Datenverkehr von externen Endpunkten zu ermöglichen.
Standardmäßig generiert das ExtraHop-System nur Erkennungen für internen Verkehr.
- 6. Führen Sie die empfohlenen Verfahren in der **Checkliste nach der Bereitstellung** [↗](#).