Stellen Sie den EDA 10200-Sensor bereit

Veröffentlicht: 2024-10-25

In dieser Anleitung wird die Installation des im Rack montierten EDA 10200 erklärt Sensor.

Mit dieser Installation können Sie die Netzwerkleistungsüberwachung, Netzwerkerkennung und -reaktion sowie die Erkennung von Eindringlingen auf einem einzigen Gerät ausführen Sensor. Durch Hinzufügen des IDS-Moduls können Sie auch IDS-Erkennungen hochladen und anzeigen.

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: 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.

Voraussetzungen für die Installation

Um den Sensor zu installieren, muss Ihre Umgebung die folgenden Anforderungen erfüllen:

Fühler

2 HE Rackfläche und elektrische Anschlüsse für 2 x 1100-W-Stromversorgungen.

Verwaltung

Ein 10/100/1000 BASE-T-Netzwerkanschluss oder ein 10G BASE-SR-Port für die Appliance-Verwaltung.

Überwachung (Erfassung)

Hochleistungsschnittstellen: Ein bis vier Netzwerkanschlüsse für den Anschluss an 100-GbE-, 40-GbE-, 25-GbE- oder 10-GbE-Paketdatenquellen, je nach bestellter Konfiguration.
Management- und Überwachungsschnittstellen: Ein bis drei Netzwerkanschlüsse für den Anschluss an 1-GbE-Paketdatenquellen.

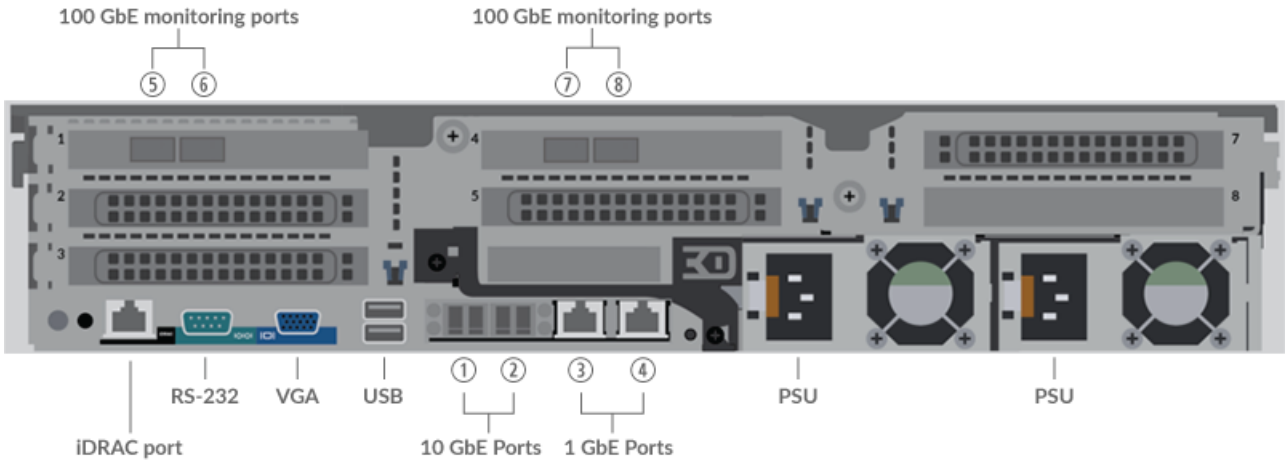
Zugriff auf das Netzwerk

Stellen Sie sicher, dass Administratoren auf die Administrationseinstellungen auf der Sensor über TCP-Port 443.

Weitere Informationen zu den Schnittstellen auf dem ExtraHop-System finden Sie in der Häufig gestellte Fragen zu ExtraHop Hardware.

Anschlüsse auf der Rückseite

VON 10200



- Ein iDRAC-Schnittstellenport
- Ein serieller RS-232-Anschluss zum Anschließen eines Konsolengeräts
- Ein VGA-Anschluss zum Anschluss eines externen Displays
- Zwei USB 3.0-Anschlüsse zum Anschließen von Eingabegeräten wie Tastatur und Maus
- Zwei Stromanschlüsse zum Anschließen der Appliance an eine Wechselstromquelle
- Zwei 10-GbE-Anschlüsse. Die Ports 1 und 2 können als Management-Port, Management- und Flow-Ziel oder Management und RPCAP/ERSPAN/VXLAN/GENEVE-Ziel konfiguriert werden.

  Während die 10-GbE-Management+-Erfassungsschnittstellen auf diesem Sensor Verwaltungsfunktionen mit Geschwindigkeiten von 10 Gbit/s ausführen können, ist die Verarbeitung von Datenverkehr wie ERSPAN, VXLAN und GENEVE auf 1 Gbit/s begrenzt.

  Hinweis In Umgebungen mit asymmetrischem Routing neben den Hochleistungsschnittstellen gelangen Ping-Antworten möglicherweise nicht an den Absender zurück.
- Zwei 10/100/1000 BASE-T-Netzwerkanschlüsse. Port 3 ist der primäre Management-Port. Diese Ports können als Überwachungsport, Management-Port, Management- und Flow-Ziel oder Management und RPCAP/ERSPAN/VXLAN/GENEVE-Ziel konfiguriert werden.
- Vier 100-GbE-fähige Ports an zwei Netzwerkadaptern. Diese Ports sind die leistungsstarken Überwachungs- (Erfassungs-) Schnittstellen.

Unterstützte Paketquellenkonnektivität

Der EDA 10200 kann Pakete über die Ports 1-8 akzeptieren. Die Anschlüsse können gemäß der folgenden Tabelle angeschlossen werden.

EDA 10200 Stecker	Peer-Connector für Paketquelle	Vom Kunden bereitgestellte Verkabelung	Unterstützte Betriebsgeschwindigkeiten
Transceiverbasierte Konnektivität			
100-GbE-QSFP28-SR4-Transceiver	100-GbE-QSFP28-SR4-Transceiver	Multimode-Glasfaser MPO Steckverbinder	100 Gbit/s, 40 Gbit/s
	40-GbE-QSFP+-SR4-Transceiver	Multimode-Glasfaser	40 Gbit/s

EDA 10200 Stecker	Peer-Connector für Paketquelle	Vom Kunden bereitgestellte Verkabelung	Unterstützte Betriebsgeschwindigkeiten
		MPO Steckverbinder	
40-GbE-QSFP SR BiDi-Transceiver (nur vom Kunden bereitgestellter Cisco QSFP-40G-SR-BD)	40GbE QSFP+ SR BiDi-Transceiver	Duplex-Multimode-Glasfaser-LC-Steckverbinder	40 Gbit/s
25-GbE-SFP28-SR-Transceiver (mit QSFP28-zu-SFP28-Adapter)	2,5-GbE-SFP28-SR-Transceiver	Multimode-Glasfaser LC-Stecker	25 Gbit/s, 10 Gbit/s
	10GbE SFP+ SR-Transceiver	Multimode-Glasfaser LC-Stecker	10 Gbit/s
Direct Attach-Konnektivität			
Vom Kunden bereitgestelltes QSFP28-DAC-Kabel, z. B. die MELLANOX MCP1600-Cxxx-Serie			100 Gbit/s
QSFP28-zu-SFP28-Adapter mit vom Kunden bereitgestelltem SFP28-DAC-Kabel, z. B. die Mellanox MCP2M00-Axxx-Serie			25 Gbit/s
Vom Kunden bereitgestelltes RJ45-Ethernet-Kabel 1 Gbit/s			1 Gbit/s

Hinweis Die Paketverarbeitungsfähigkeit des Sensor beträgt 100 Gbit/s. Es ist zwar möglich, dass der Sensor überlastet wird, indem mehr als 100 Gbit/s an Paketdaten über die vier 100-GbE-fähigen Ports gesendet werden, aber eingehende Workloads, die 100 Gbit/s überschreiten, führen dazu, dass Pakete verloren gehen.

Richtlinien zur Verkehrsverteilung

- Pakete aus demselben Fluss sollten auf derselben Schnittstelle oder auf Schnittstellen derselben Netzwerkschnittstellenkarte (NIC) empfangen werden.
- Die Aufnahme auf jeder Netzwerkkarte sollte 75% des bewerteten Analysedurchsatzes für die Sensor um sicherzustellen, dass der Datenverkehr auf die Systemressourcen verteilt ist.
- Wenn Ihr Datenfeed nicht beide Schnittstellen auf der NIC benötigt, deaktivieren Sie die unkonfigurierten Schnittstellen in den Administrationseinstellungen. Konfigurieren Sie den Sensor beispielsweise mit einer einzigen Schnittstelle, um 50 Gbit/s auf jeder Netzwerkkarte aufzunehmen. Deaktivieren Sie die externen Ports auf jeder Netzwerkkarte. Diese Konfiguration optimiert die Leistung für 100 Gbit/s.
- Es wird erwartet, dass ein einzelnes Hochleistungs-ERSPAN-Target 20 bis 30 Gbit/s verarbeitet. Auf einem größeren Sensoren, verteilen Sie den ERSPAN-Verkehr auf mehr Schnittstellen, um die Datenaufnahme zu skalieren.

Richten Sie den Sensor ein

1. Rackmontage des Sensor.

   Installiere das Sensor in Ihrem Rechenzentrum mit dem mitgelieferten Rackmontage-Kit. Das Montageset unterstützt die meisten Racks mit vier Pfosten mit runden oder quadratischen Löchern.

   Richten Sie die Hardware so aus, dass ein ordnungsgemäßer Luftstrom gewährleistet ist. Der Kaltlufteinlass erfolgt durch die Vorderseite des Sensor.
2. Verbinden Sie Port 3 mit Ihrem Verwaltungsnetzwerk.

Die EDA 10200 Sensor hat zwei 10/100/1000 BASE-T-Netzwerkanschlüsse. Verbinden Sie mit einem Netzwerk-Patchkabel den Management-Port am Sensor zu Ihrem Management-Netzwerk. Port 3 ist der Standard-Management-Port auf dem EDA 10200.

3. Schließen Sie den Monitoring-Port an.

   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.

   Verbinden Sie mit dem entsprechenden Netzwerkkabel Port 7 an der Sensor zu einem Netzwerk-Tap- oder Mirror-Port am Switch. Stellen Sie bei der Konfiguration mehrerer Monitoring-Ports sicher, dass die Transceiver auf die Adapter verteilt sind. Schließen Sie beispielsweise bei zwei Transceivern das Kabel an den Transceivern an Port 5 und Port 7 an.

   Hinweis: Die Verbindungsleuchten an den Anschlüssen der Überwachungsschnittstelle leuchten erst auf, wenn Sie den ExtraHop-Sensor, den Recordstore oder den Packetstore mit Ihrem Produktschlüssel registriert haben.

4. Optional: Schließen Sie den iDRAC-Port an.

   Um die Remoteverwaltung des zu ermöglichen Sensor, verbinden Sie Ihr Verwaltungsnetzwerk mit einem Netzwerk-Patchkabel mit dem iDRAC-Port.

5. Die Frontverkleidung einbauen.

   Sie müssen die Frontblende installieren, wenn Sie das konfigurieren möchten Sensor durch das LCD-Display.

   Stecken Sie den USB-Anschluss auf der rechten Seite der Blende in den USB-Anschluss an der Vorderseite des Sensor. Halten Sie die Entriegelungstaste am linken Ende der Blende gedrückt und drücken Sie die Blende bündig mit dem Sensor bis es einrastet.

6. Schließen Sie die Netzkabel an.

   Verbinden Sie die beiden mitgelieferten Netzkabel mit den Netzteilen auf der Rückseite des Sensor, und stecken Sie dann die Kabel in eine Steckdose. Wenn der Sensor schaltet sich nicht automatisch ein, drücken Sie den Netzschalter ⏻ auf der rechten Vorderseite des Sensor.

Konfigurieren Sie die Verwaltungs-IP-Adresse

DHCP ist auf dem ExtraHop-System standardmäßig aktiviert. Wenn Sie das System einschalten, versucht Interface 3, eine IP-Adresse über DHCP abzurufen. Bei Erfolg wird die IP-Adresse auf dem Startbildschirm der LCD-Anzeige angezeigt.

Wenn Ihr Netzwerk DHCP nicht unterstützt, können Sie eine statische IP-Adresse über das LCD-Menü auf der Vorderseite oder über die Befehlszeilenschnittstelle (CLI) konfigurieren.

Konfigurieren Sie eine statische IP-Adresse über das LCD

Gehen Sie wie folgt vor, um eine IP-Adresse manuell über die LCD-Bedienelemente auf der Vorderseite zu konfigurieren.

1. Stellen Sie sicher, dass die Standard-Verwaltungsschnittstelle mit dem Netzwerk verbunden ist und der Verbindungsstatus aktiv ist.
2. Drücken Sie die Auswahltaste (✓), um zu beginnen.
3. Drücken Sie die Abwärtspfeiltaste, um auszuwählen `Network`, und drücken Sie dann die Auswahltaste.
4. Drücken Sie den Abwärtspfeil, um auszuwählen `Set static IP`, und drücken Sie dann die Auswahltaste.
5. Drücken Sie die Links- oder Rechtspfeile, um die erste Ziffer auszuwählen, die geändert werden soll, und drücken Sie dann die Aufwärts- oder Abwärtspfeile, um die Ziffer in die gewünschte Zahl zu ändern.

Wiederholen Sie diesen Schritt für jede Ziffer, die Sie ändern müssen. Nachdem Sie die gewünschte IP-Adresse konfiguriert haben, drücken Sie die Auswahltaste.

6. Auf dem `Network mask` Bildschirm, drücken Sie die Links- oder Rechtspfeile, um die erste Ziffer auszuwählen, die geändert werden soll, und drücken Sie dann die Aufwärts- oder Abwärtspfeile, um die Ziffer in die gewünschte Zahl zu ändern.

   Wiederholen Sie diesen Schritt für jede Ziffer, die Sie ändern müssen. Nachdem Sie die gewünschte Netzwerkmaske konfiguriert haben, drücken Sie die Auswahltaste.
7. Auf dem `Default gateway` Bildschirm, drücken Sie die Links- oder Rechtspfeile, um die erste Ziffer auszuwählen, die geändert werden soll, und drücken Sie dann die Aufwärts- oder Abwärtspfeile, um die Ziffer in die gewünschte Zahl zu ändern.

   Wiederholen Sie diesen Schritt für jede Ziffer, die Sie ändern müssen. Nachdem Sie das gewünschte Standard-Gateway konfiguriert haben, drücken Sie die Auswahltaste.
8. Bestätigen Sie Ihre geänderten Netzwerkeinstellungen auf der `Settings saved` Bildschirm, und drücken Sie dann eine beliebige Taste, um zum `Network Menu`.

   Hinweis: Jeder Adresse ist ein Buchstabe vorangestellt, der angibt, ob es sich um die System-IP-Adresse (I), die Gateway-Adresse (G) oder die Netzmaske (N) handelt.
9. Drücken Sie den Abwärtspfeil und scrollen Sie zu `Set DNS servers`, und drücken Sie dann die Auswahltaste.
10. Drücken Sie die Links- oder Rechtspfeile auf der `DNS1` Bildschirm, um die erste Ziffer auszuwählen, die geändert werden soll, und drücken Sie dann die Aufwärts- oder Abwärtspfeile, um die Ziffer auf die gewünschte Zahl zu ändern.

    Wiederholen Sie diesen Schritt für jede Ziffer, die Sie ändern müssen, und drücken Sie dann die Auswahltaste, um mit der `DNS2` Bildschirm.
11. Konfigurieren Sie einen zweiten DNS-Server.
12. Bestätigen Sie die DNS-Einstellungen auf der `Settings saved` Bildschirm, und drücken Sie dann eine beliebige Taste, um zum `Network Menu`.
13. Drücken Sie zweimal den Abwärtspfeil bis ← `Back` erscheint, und drücken Sie dann die Auswahltaste.
14. Drücken Sie zweimal den Abwärtspfeil, um iDRAC auszuwählen.
15. Konfigurieren Sie iDRAC DHCP, IP, Maske, Gateway und DNS auf die gleiche Weise wie die IP-Adresse.
16. Drücken Sie die `X` Taste, um zum Hauptmenü zurückzukehren.

Konfigurieren Sie eine IP-Adresse über die CLI

Bevor Sie beginnen
Sie können auf die CLI zugreifen, indem Sie eine USB-Tastatur und einen SVGA-Monitor an die 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.
Führen Sie die folgenden Schritte aus, um eine IP-Adresse manuell über die CLI zu konfigurieren.

1. Stellen Sie eine Verbindung zum ExtraHop-System her.
2. Geben Sie an der Anmeldeaufforderung ein `Schale` und drücken Sie dann ENTER.
3. Geben Sie in der Passwortabfrage die Seriennummer des Systems ein, und drücken Sie dann die EINGABETASTE.

   Die Seriennummer befindet sich auf einem Etikett auf der Rückseite des Sensor. Die Seriennummer finden Sie auch auf dem LCD-Display auf der Vorderseite des Sensor in der `Info` Abschnitt.
4. Aktiviere privilegierte Befehle:

   ```
   enable
   ```
5. Geben Sie in der Passwortabfrage die Seriennummer ein, und drücken Sie dann die EINGABETASTE.

6. Rufen Sie den Konfigurationsmodus auf:

```
configure
```

7. Rufen Sie den Schnittstellenkonfigurationsmodus auf:

```
interface
```

8. Geben Sie die IP-Adresse und die DNS-Einstellungen im folgenden Format an:
   `ip ipaddr <ip_adresse> <Netzmaske> <Tor> <DNS-Server>`
   Zum Beispiel:

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

9. Verlassen Sie den Konfigurationsmodus:

```
exit
```

10. Speichern Sie die laufende Konfiguration:

```
running_config save
```

11. Typ y und drücken Sie dann ENTER.

Hinweis: Das System aktualisiert die laufende Konfigurationsdatei und wendet die neuen Einstellungen an, wenn eine Verbindung auf der Schnittstelle erkannt wird.

(Optional) Konfigurieren Sie die 10-GbE-Verwaltungsschnittstelle

Sie können einen 10-GbE-Anschluss (Port 1 oder Port 2) konfigurieren, um das System zu verwalten. Mit den folgenden Befehlen werden die Einstellungen von Port 3 auf Port 1 verschoben und dann Port 3 deaktiviert. Alternativ können Sie die 10-GbE-Verwaltungsschnittstelle in den Administrationseinstellungen konfigurieren.

1. Stellen Sie sicher, dass der Port 1 mit dem 10-GbE-Netzwerk verbunden ist.
2. Stellen Sie eine SSH-Verbindung zum ExtraHop-System her.
3. Geben Sie an der Anmeldeaufforderung ein `shell` und drücken Sie dann ENTER.
4. Geben Sie in der Passwortabfrage die Seriennummer des Systems ein, und drücken Sie dann die EINGABETASTE.
   Die Seriennummer befindet sich auf einem Etikett auf der Rückseite des Sensor. Die Seriennummer finden Sie auch auf dem LCD-Display auf der Vorderseite des Sensor in der `Info` Abschnitt.
5. Aktiviere privilegierte Befehle:

```
enable
```

6. Geben Sie in der Passwortabfrage die Seriennummer ein, und drücken Sie dann die EINGABETASTE.
7. Rufen Sie den Konfigurationsmodus auf:

```
configure
```

8. Rufen Sie den Schnittstellenkonfigurationsmodus auf:

```
interface 1
```

9. Verschieben Sie die Schnittstelleneinstellungen:

Warnung: Dieser Befehl überschreibt die Einstellungen für Interface 1 mit den Einstellungen von Interface 3. Die aktuellen Einstellungen für Interface 1 gehen verloren und Interface 3 wird deaktiviert.

```
take_settings 3
```

10. Typ `Y` um fortzufahren, 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`. Das Passwort ist die Seriennummer des Systems , die in der `Info` Abschnitt des LCD-Displays und auf dem Etikett auf der Rückseite des Sensor.
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.