

Stellen Sie einen ExtraHop-Sensor mit Hyper-V bereit

Veröffentlicht: 2024-02-12

In den folgenden Verfahren wird erklärt, wie der virtuelle ExtraHop EDA 1100v bereitgestellt wird. Sensoren auf der Microsoft Hyper-V-Plattform. Sie müssen Erfahrung mit der Verwaltung Ihres Hypervisor-Produkts haben, um diese Verfahren durchführen zu können.

Anforderungen an virtuelle Maschinen

Ihr Hypervisor muss in der Lage sein, die folgenden Spezifikationen für das virtuelle Sensor.

- Hyper-V unter Windows Server 2012 (oder höher), das den virtuellen Sensor hosten kann
- Hyper-V Manager zur Verwaltung der virtuellen Maschine
- (Optional) Wenn Sie Paketerfassungen aktivieren möchten, konfigurieren Sie während der Bereitstellung ein zusätzliches Speicherlaufwerk. Informationen zum Hinzufügen einer Festplatte finden Sie in der Dokumentation Ihres Anbieters.
- Die folgende Tabelle enthält die Serverhardwareanforderungen für jedes Sensormodell:

Fühler	CPU	RAM	Festplatte
Enthülle (x) EDA 1100v	4 Prozessorkerne mit Hyperthreading-Unterstützung, VT-x- oder AMD-V-Technologie und 64-Bit-Architektur. Unterstützung für Streaming-SIMD-Erweiterungen 4.2 (SSE4.2) und POPCNT-Befehle.	8 GB	Festplatte mit 46 GB oder höher (Thick-Provisioning) 250 GB oder weniger Festplatte für Paketerfassungen (Thick-Provisioning)

Um die korrekte Funktionalität der virtuellen Sensor:

- Ändern Sie nicht die Standardfestplattengröße bei der Erstinstallation. Die Beibehaltung der Standardfestplattengröße gewährleistet ein korrektes Lookback für ExtraHop-Metriken und eine einwandfreie Systemfunktionalität. Wenn Ihre Konfiguration eine andere Festplattengröße erfordert, wenden Sie sich vor der Änderung an Ihren ExtraHop-Vertreter.
- Migrieren Sie die VM nicht. Obwohl es möglich ist, zu migrieren, wenn sich der Datenspeicher auf einem Remote-SAN befindet, empfiehlt ExtraHop diese Konfiguration nicht.


! **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

Sie können den internen oder externen Datenverkehr überwachen.

- **Intra-VM:** Ein 1-Gbit/s-Ethernet-Netzwerkanschluss ist erforderlich (für die Verwaltung). Der Management-Port muss über Port 443 zugänglich sein.

- **Extern:** Zwei 1-Gbit/s-Ethernet-Netzwerkanschlüsse sind erforderlich. Eine für den physischen Port-Mirror und eine für die Verwaltung. Die physische Port-Mirror-Schnittstelle muss mit der Port-Mirror-Schnittstelle des Switches verbunden sein. Es ist zwar möglich, einen 10-Gbit/s-Ethernet-Netzwerkanschluss für die Port-Mirror-Schnittstelle zu konfigurieren, dies wird jedoch nicht empfohlen, da der virtuelle Sensor nicht mehr als 1 Gbit/s Datenverkehr verarbeiten kann.

 **Hinweis:** Alle virtuellen NICs sind standardmäßig im Trunk-Modus konfiguriert. Wenn Sie Ihrer Verwaltungsschnittstelle ein bestimmtes VLAN zuweisen müssen, müssen Sie die Schnittstelle über PowerShell ändern, um die Verwaltungsschnittstelle in den Zugriffsmodus zu ändern.

 **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.

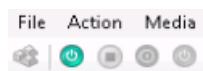
Für Registrierungszwecke benötigt der virtuelle Sensor eine ausgehende Verbindung DNS Konnektivität auf UDP-Port 53, sofern sie nicht von einer ExtraHop-Konsole verwaltet wird.

Installieren Sie die Dateien für Hyper-V

Bevor Sie beginnen

Falls Sie dies noch nicht getan haben, laden Sie die ExtraHop-Sensor-Firmware-Datei für Hyper-V von der [ExtraHop Kundenportal](#) und extrahiere den Inhalt aus dem `.zip` Datei auf Ihren Windows Server-Computer.

1. Gehen Sie auf Ihrem Windows Server-Computer zu **Start** Menü und öffnen Sie den Hyper-V-Manager.
2. Klicken Sie im rechten Bereich des Hyper-V-Managers auf **Neu** und wähle **Virtuelle Maschine importieren...**
3. Wenn der Bevor du anfängst Bildschirm erscheint, klicken **Weiter**. Fahren Sie andernfalls mit dem nächsten Schritt fort.
4. Suchen Sie nach dem Ordner mit den entpackten Dateien und klicken Sie auf **Weiter**.
5. Wählen Sie die zu importierende virtuelle Maschine aus und klicken Sie auf **Weiter**.
6. Wählen **Kopieren Sie die virtuelle Maschine** und klicken **Weiter**.
7. Auf Ordner für Dateien virtueller Maschinen auswählen, wählen Sie den Speicherort für die Konfiguration der VM aus und klicken Sie auf **Weiter**.
8. Auf Wählen Sie Speicherordner zum Speichern virtueller Festplatten, wählen Sie einen Speicherort für die virtuellen Festplatten aus und klicken Sie auf **Weiter**.
9. Überprüfen Sie auf dem Übersichtsbildschirm Ihre Auswahl und klicken Sie dann auf **Fertig stellen**.
10. Warten Sie einige Minuten, bis die Dateien kopiert sind.
11. Klicken Sie in der Liste Virtuelle Maschinen mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Start**.
12. Klicken Sie erneut mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Verbinde**.
13. Klicken Sie oben auf dem Bildschirm auf die grüne Startschaltfläche und warten Sie auf die Anmeldeaufforderung.




14. Geben Sie an der Anmeldeaufforderung Folgendes ein `schale` und drücken Sie dann die EINGABETASTE.
15. Geben Sie an der Passworteingabeaufforderung Folgendes ein `standard`, und drücken Sie dann die EINGABETASTE.
16. Führen Sie das aus `ipaddr anzeigen` Befehl zur Anzeige der IP-Adresse und Netzmaske des Sensor. Sie benötigen die IP-Adresse, um die ExtraHop-Lizenz im nächsten Verfahren anzuwenden.

 **Hinweis** Wenn Ihr Netzwerk dies nicht unterstützt DHCP, siehe [Eine statische IP-Adresse konfigurieren](#) um eine statische IP-Adresse festzulegen.

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.

 **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 in der Anmeldeaufforderung Folgendes ein `schale` und drücken Sie dann ENTER.
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 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 die EINGABETASTE.

Den Sensor konfigurieren

Nachdem Sie eine IP-Adresse für die konfiguriert haben Sensor, öffnen Sie einen Webbrowser und navigieren Sie über die konfigurierte IP-Adresse zum ExtraHop-System. Akzeptieren Sie die Lizenzvereinbarung und melden Sie sich an. Der Standard-Anmeldename ist `setup` und das Passwort ist

default. Folgen Sie den Anweisungen, um den Produktschlüssel einzugeben, die Standard-Setup- und Shell-Benutzerkontokennwörter zu ändern, eine Verbindung zu ExtraHop Cloud Services herzustellen und eine Verbindung zu einer ExtraHop-Konsole herzustellen.

Nachdem das System lizenziert wurde und Sie sich vergewissert haben, dass Datenverkehr erkannt wurde, führen Sie die empfohlenen Verfahren in der [Checkliste für die Zeit nach der Bereitstellung](#) .

Mirror Wire-Daten

Dieser Abschnitt enthält Verfahren zum Spiegeln von Daten auf Ihre virtuelle ExtraHop-Appliance.

Spiegelung von internem und externem Verkehr

Der virtuelle ExtraHop-Sensor kann in den folgenden Netzwerkkonfigurationsbeispielen für die Überwachung des Netzwerkverkehrs konfiguriert werden. Jedes Beispiel erfordert eine Änderung der Netzwerkkonfiguration seines Hypervisor-Hosts und gibt Netzwerkadapter 1 als Verwaltungsschnittstelle an.



Hinweis Für die Überwachung des externen Netzwerkdatenverkehrs mit Spiegelung sind eine externe Netzwerkkarte und ein zugehöriger virtueller Switch erforderlich.

Überwachung des VM-internen Datenverkehrs

Die Sensor kann so konfiguriert werden, dass der Netzwerkverkehr einer anderen VM auf demselben Host überwacht wird, indem Sie wählen **Port-Spiegelung** Modus im Hyper-V-Manager. Eine virtuelle ExtraHop-Maschine, die im Port-Mirroring-Modus ausgeführt wird, kann nur eine andere virtuelle Maschine überwachen, die auf demselben virtuellen Switch läuft.

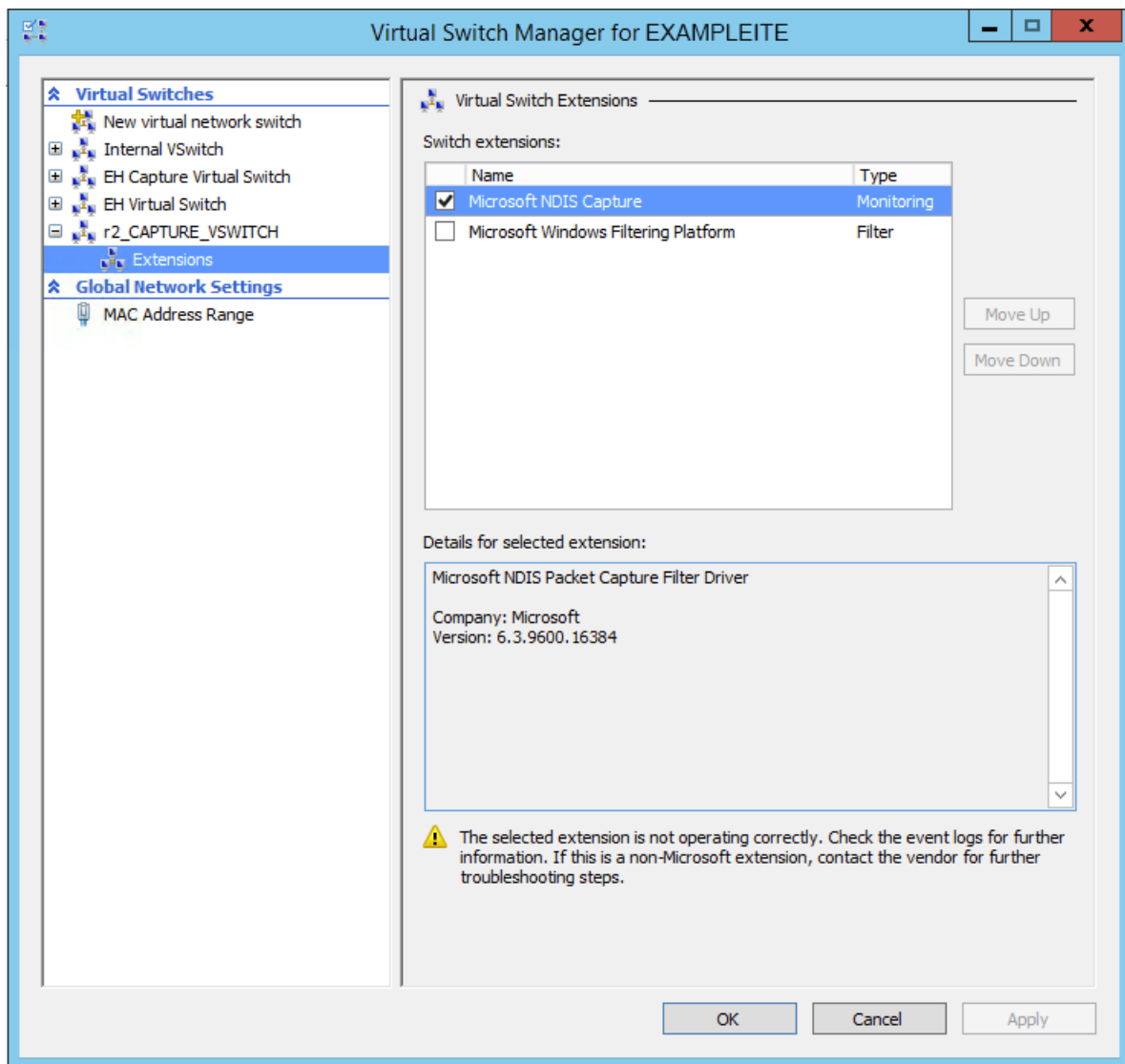
Aktivieren Sie den Port-Spiegelungsmodus im Hyper-V-Manager

1. Klicken Sie mit der rechten Maustaste auf ExtraHop Sensor VM und wählen **Einstellungen**.
2. expandieren **Netzwerkadapter** und klicken **Erweiterte Funktionen**.
3. In der Port-Spiegelung klicken Sie im Abschnitt auf die Dropdownliste Spiegelungsmodus und wählen Sie **Quelle**.
4. Notieren Sie sich das Quellnetzwerk und stellen Sie sicher, dass sich die Capture-Schnittstelle auf der ExtraHop-VM im selben Netzwerk befindet.
5. klicken **Bewerben**.
6. klicken **OK**.
7. Wiederholen Sie diese Schritte für alle VMs, die Sie überwachen möchten, mit Ausnahme der ersten VM, die Sie in diesem Verfahren erstellt haben.

Überwachung des externen gespiegelten Datenverkehrs zur VM

Dieses Szenario erfordert eine zweite physische Netzwerkschnittstelle und die Erstellung eines zweiten vSwitches, der dieser NIC zugeordnet ist. Diese NIC stellt dann eine Verbindung zu einem Mirror, Tap oder Aggregator her, der den Datenverkehr von einem Switch kopiert. Dieses Setup ist nützlich für die Überwachung des Intranets eines Büros.

1. Klicken Sie mit der rechten Maustaste auf die ExtraHop-Sensor-VM und wählen Sie **Einstellungen**.
2. expandieren **Netzwerkadapter** und klicken **Fortgeschrittene Funktionen**.
3. Klicken Sie im Abschnitt Port-Mirroring auf **Spiegelungsmodus** Drop-down-Liste und wählen **Reiseziel**.
4. klicken **Bewerben**.
5. klicken **OK**.
6. Erweitern Sie den virtuellen Switch, der dem externen Datenfeed zugeordnet ist, und aktivieren Sie den **Microsoft NDIS-Erfassung** Schalter. Sie können die Warnung ignorieren, dass die ausgewählte Erweiterung nicht ordnungsgemäß funktioniert.



7. klicken **Bewerben**, und klicken Sie dann **OK**.
8. Starten Sie Windows PowerShell mit Administratorrechte.
9. Konfigurieren Sie den externen Port des virtuellen Switches, indem Sie die folgenden Befehle ausführen:

a) Speichern Sie die FeatureName Parameter in einer Variablen:

```
$portFeature=Get-VMSystemSwitchExtensionPortFeature -FeatureName
"Ethernet Switch Port Security Settings"
```

b) Ändern Sie den Monitormodus des virtuellen Switches auf Quelle:

```
$portFeature.SettingData.MonitorMode = 2
```

c) Fügen Sie dem virtuellen Switch einen externen Port hinzu, der den FeatureName in Schritt 9a spezifizierter Parameter:

```
add-VMSwitchExtensionPortFeature -ExternalPort -SwitchName
<name_of_switch> -VMSwitchExtensionFeature $portFeature
```

Wo <name_of_switch> ist der Name des virtuellen Switches.

10. Optional: Um gespiegelten Datenverkehr von mehreren VLANs zu empfangen, setzen Sie die VM-NIC in den Trunk-Modus und geben Sie eine Liste der zulässigen VLAN-IDs an, indem Sie den folgenden Befehl ausführen:

```
Set-VMNetworkAdapterVlan -VMName <destination_vm> -Trunk -
AllowedVlanIdList <id_list> -NativeVlanId <vlan_id>
```

Wo *<destination_vm>* ist der Name der ExtraHop VM, *<id_list>* ist die Liste der erlaubten VLAN-IDs und *<vlan_id>* ist die ID des Standard-VLAN.

Zum Beispiel:

```
Set-VMNetworkAdapterVlan -VMName EDA1100v -Trunk -AllowedVlanIdList 1-100
-NativeVlanId 10
```

Paketweiterleitung

Ein Paket Forwarder leitet den Verkehr von einem beliebigen Host an das ExtraHop-System weiter. Ein Paket Forwarder ähnelt konzeptionell einem physischen Netzwerk-Tap, ist jedoch in Software implementiert. In diesen Themen und in der Branche wird diese Software abwechselnd als Software Tap oder manchmal als RPCAP bezeichnet, was für Remote Packet Capture steht.

Um den Paket Forwarder zu implementieren, stellen Sie Folgendes sicher:

- Sie haben administrativer Zugriff Server, die Sie überwachen möchten.
- Sie verwenden ein 64-Bit-Linux- oder Windows-Betriebssystem (Windows Server 2008 R2 oder 2012).

Gehen Sie wie folgt vor, um die korrekte Funktionalität der virtuellen ExtraHop-Appliance sicherzustellen:

- Stellen Sie sicher, dass RPCAP auf der virtuellen ExtraHop-Appliance aktiviert ist. Sehen Sie die [Konfiguration zusätzlicher RPCAP-Einstellungen](#) Abschnitt für optionale Einstellungen.
- Installieren Sie den Paket Forwarder auf den Servern, die Datenverkehr senden.
- Analysieren Sie den Verkehr im ExtraHop-System.

Installieren Sie den Paket Forwarder auf einem Linux-Server

Sie müssen die Paketweiterleitungssoftware auf jedem Server installieren, der überwacht werden soll, um Pakete an das ExtraHop-System weiterzuleiten.

RPCAP-Installationsdateien und Anweisungen finden Sie unter [ExtraHop Downloads und Ressourcen](#) [Webseite](#).

Downloaden und auf Debian-basierten Systemen installieren

Um den Paket Forwarder auf Debian-basierten Systemen herunterzuladen und zu installieren:

1. Laden Sie die RPCAP-Installationsdatei vom ExtraHop herunter [Downloads und Ressourcen](#) [Webseite](#).
2. Installieren Sie die Software auf dem Server, indem Sie den folgenden Befehl ausführen:

```
sudo dpkg -i rpcapd_<extrahop_firmware_version>_amd64.deb
```

3. Geben Sie an der Eingabeaufforderung die IP-Adresse des ExtraHop-Systems ein, bestätigen Sie die Standardverbindung zu Port 2003 und drücken Sie die EINGABETASTE.
4. Optional: Stellen Sie sicher, dass das ExtraHop-System Datenverkehr empfängt, indem Sie die folgenden Befehle ausführen:

```
sudo dpkg --get-selections | grep rpcapd
```

```
sudo service rpcapd status
```

- Optional: Führen Sie den folgenden Befehl aus, um die IP-Adresse, die Portnummer oder die Argumente des ExtraHop-Systems für den Dienst zu ändern.

```
sudo dpkg-reconfigure rpcapd
```

Herunterladen und auf RPM-basierten Systemen installieren

- Laden Sie die RPCAP-Installationsdatei vom ExtraHop herunter [Downloads und Ressourcen](#) Webseite.
- Installieren Sie die Software auf dem Server, indem Sie den folgenden Befehl ausführen:

```
sudo rpm -i rpcapd-<extrahop_firmware_version>.x86_64.rpm
```

- Öffnen und bearbeiten Sie das `rpcapd.ini` Datei in einem Texteditor, indem Sie einen der folgenden Befehle ausführen:

```
vim /opt/extrahop/etc/rpcapd.ini
```

```
nano /opt/extrahop/etc/rpcapd.ini
```

Beispielausgabe:

```
#ActiveClient = <TARGETIP>,<TARGETPORT>  
NullAuthPermit = YES
```

Ersetzen `<TARGETIP>` mit der IP-Adresse des ExtraHop-Systems und `<TARGETPORT>` mit 2003. Kommentieren Sie die Zeile zusätzlich aus, indem Sie das Nummernzeichen löschen (#) am Anfang der Zeile.

Zum Beispiel:

```
ActiveClient = 10.10.10.10,2003  
NullAuthPermit = YES
```

- Starten Sie das Senden von Traffic an das ExtraHop-System, indem Sie den folgenden Befehl ausführen:

```
sudo /etc/init.d/rpcapd start
```

- Optional: Stellen Sie sicher, dass das ExtraHop-System Datenverkehr empfängt, indem Sie den folgenden Befehl ausführen:

```
sudo service rpcapd status
```

Downloaden und auf anderen Linux-Systemen installieren

- Laden Sie die RPCAP-Installationsdatei vom ExtraHop herunter [Downloads und Ressourcen](#) Webseite.
- Installieren Sie die Software auf dem Server, indem Sie die folgenden Befehle ausführen:
 - Extrahieren Sie die Paket Forwarder-Dateien aus der Archivdatei:

```
tar xf rpcapd-<extrahop_firmware_version>.tar.gz
```

- Wechseln Sie zu `rpcapd` Verzeichnis:

```
cd rpcapd
```

- c) Führen Sie das Installationskript aus:

```
sudo ./install.sh <extrahop_ip> 2003
```

3. Optional: Stellen Sie sicher, dass das ExtraHop-System Datenverkehr empfängt, indem Sie den folgenden Befehl ausführen:

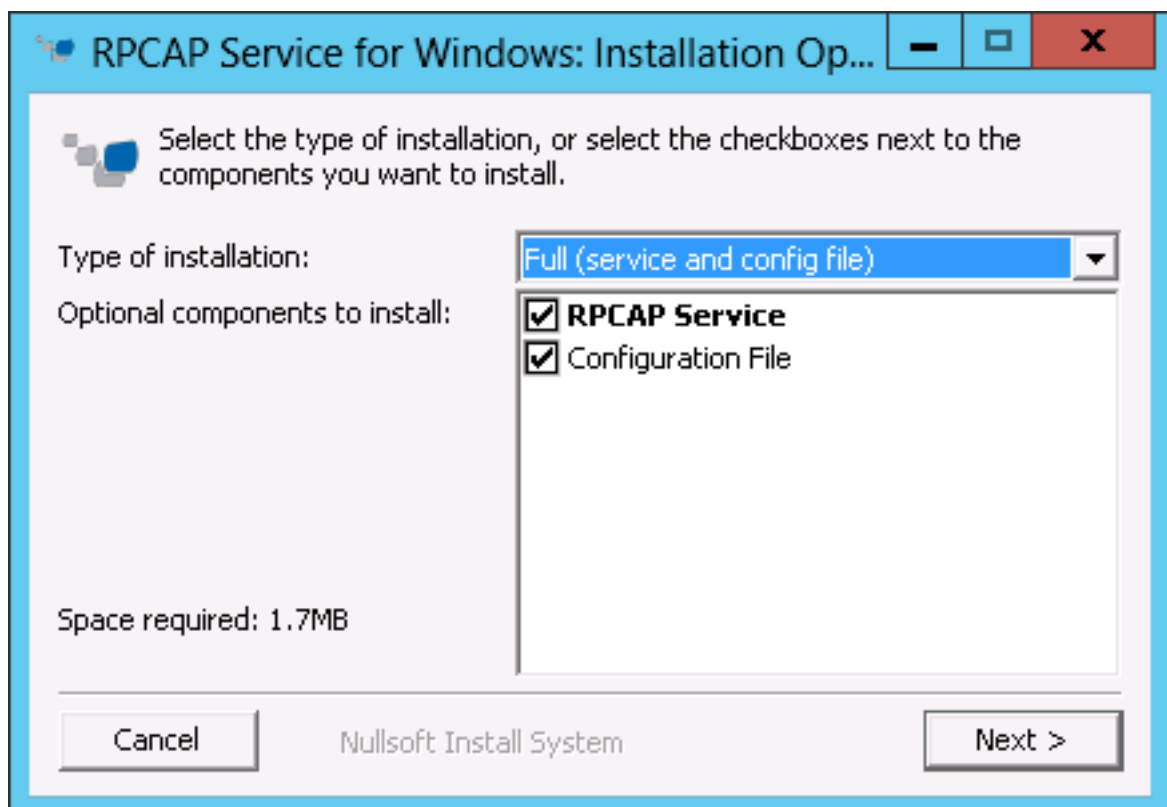
```
sudo /etc/init.d/rpcapd status
```

Informationen zum Ausführen der Software auf Servern mit mehreren Schnittstellen finden Sie unter [Überwachung mehrerer Schnittstellen auf einem Linux-Server](#).

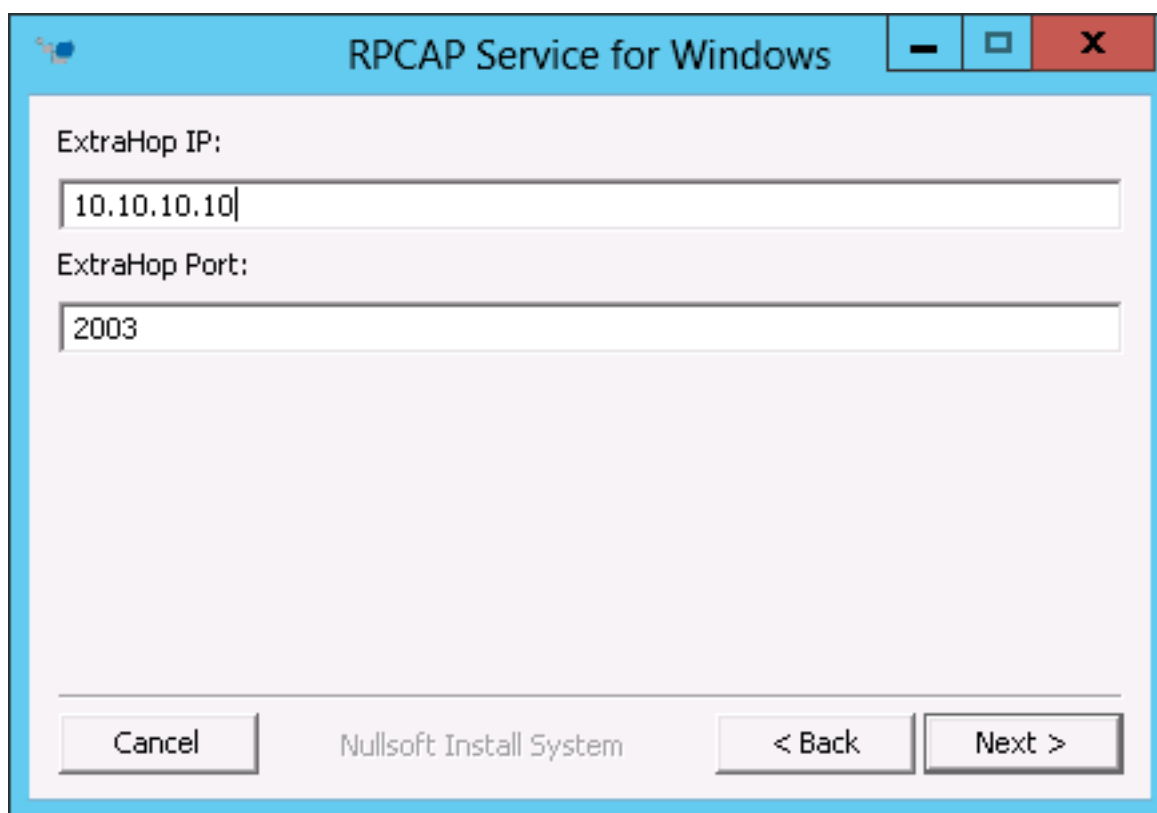
Installieren Sie den Paket Forwarder auf einem Windows-Server

Sie müssen die Paketweiterleitungssoftware auf jedem zu überwachenden Server installieren, um Pakete an das ExtraHop-System weiterzuleiten.

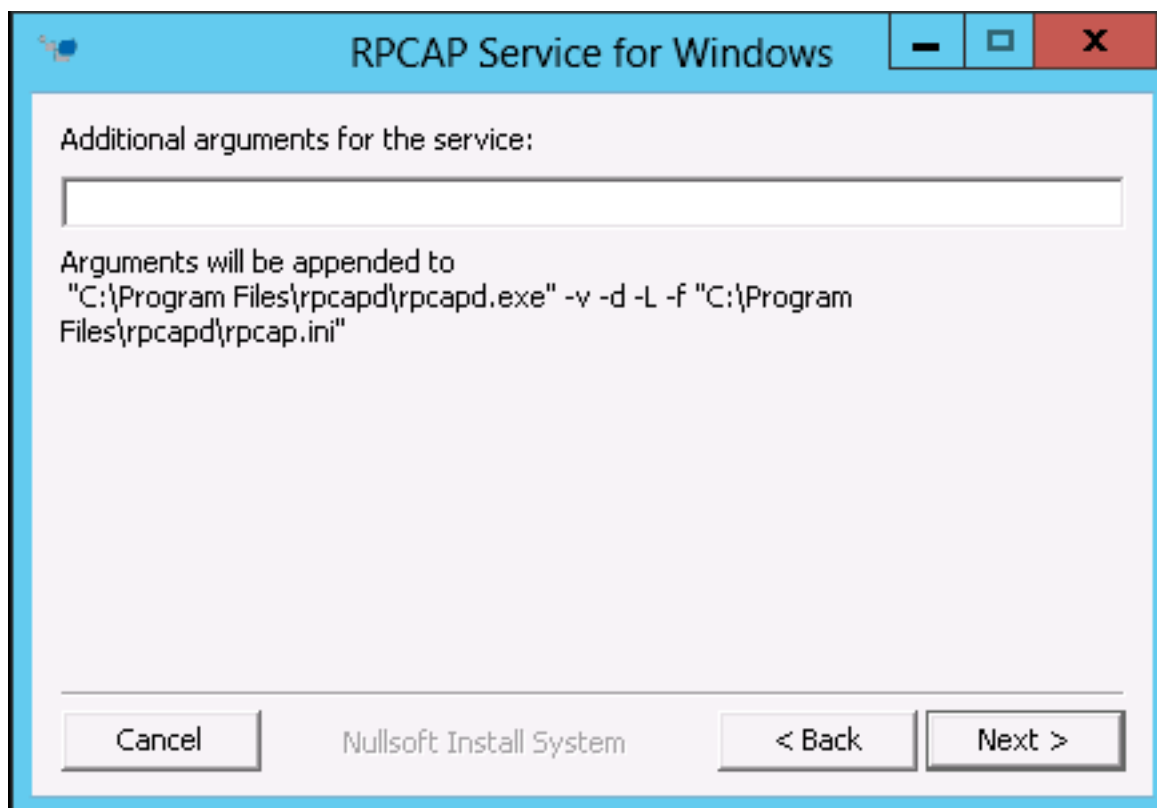
1. Laden Sie die Installationsdatei für RPCAP Service für Windows vom ExtraHop herunter [Downloads und Ressourcen](#) [Webseite](#).
2. Doppelklicken Sie auf die Datei, um das Installationsprogramm zu starten.
3. Wählen Sie im Assistenten die zu installierenden Komponenten aus.



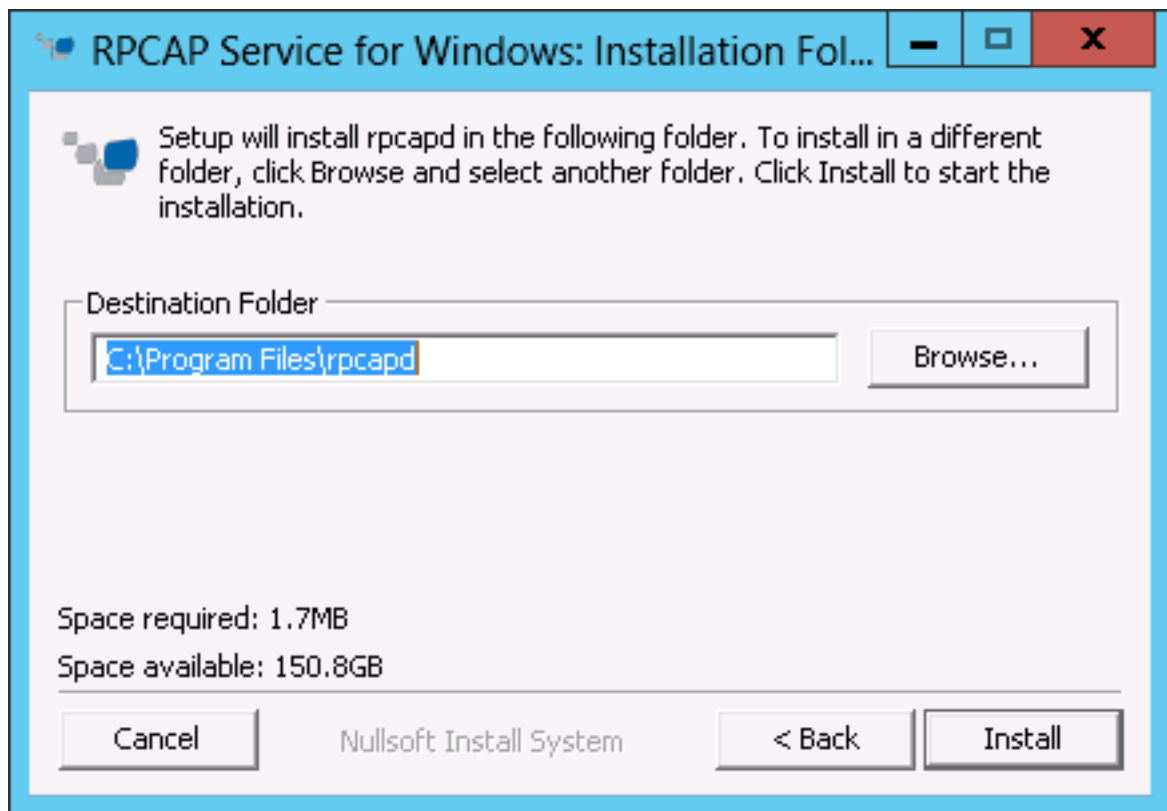
4. Schließen Sie das ab **ExtraHop-IP** und **ExtraHop-Anschluss** Felder und klicken Sie auf **Weiter**. Der Standardport ist 2003.



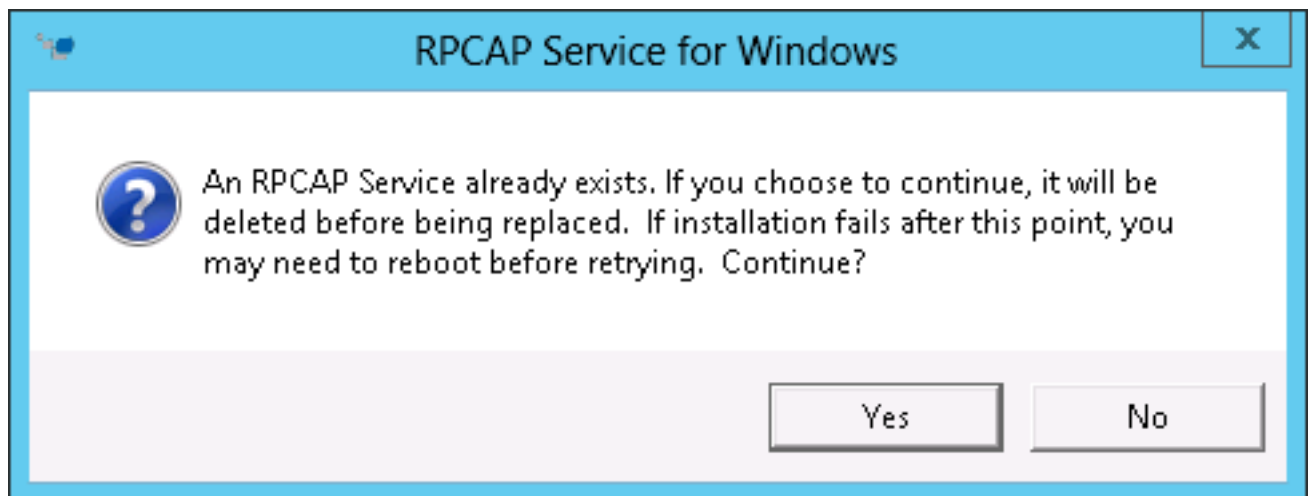
5. Optional: Geben Sie zusätzliche Argumente in das Textfeld ein und klicken Sie auf **Weiter**.



6. Suchen Sie den Zielordner für die Installation des RPCAP-Dienstes und wählen Sie ihn aus.



7. Wenn der RPCAP-Dienst zuvor installiert war, klicken Sie auf **Ja** um den vorherigen Dienst zu löschen.



8. Wenn die Installation abgeschlossen ist, klicken Sie **Schliessen**.

Überwachung mehrerer Schnittstellen auf einem Linux-Server

Bei Servern mit mehreren Schnittstellen können Sie die Paketweiterleitung so konfigurieren, dass Pakete von einer bestimmten Schnittstelle oder von mehreren Schnittstellen weitergeleitet werden, indem Sie die zugehörige Konfigurationsdatei auf dem Server bearbeiten.

Gehen Sie wie folgt vor, um die Konfigurationsdatei zu bearbeiten.

1. Öffnen Sie nach der Installation des Paket Forwarders die Konfigurationsdatei. `/opt/extrahop/etc/rpcapd.ini`.

Die Konfigurationsdatei enthält diesen Text oder einen ähnlichen Text:

```
ActiveClient = 10.0.0.100,2003
```

```
NullAuthPermit = YES
```

- Ändern Sie das Bestehende `ActiveClient` Linie und erstelle eine `ActiveClient` Leitung für jede weitere zu überwachende Schnittstelle. Geben Sie jede Schnittstelle anhand ihres Schnittstellennamens oder ihrer IP-Adresse an.

```
ActiveClient = <extrahop_ip>, <extrahop_port>, ifname=<interface_name>
```

oder

```
ActiveClient = <extrahop_ip>, <extrahop_port>, ifaddr=<interface_address>
```

Wo `<interface_name>` ist der Name der Schnittstelle, von der aus Sie Pakete weiterleiten möchten, und `<interface_address>` ist die IP-Adresse der Schnittstelle, von der die Pakete weitergeleitet werden. Die `<interface_address>` Variable kann entweder die IP-Adresse selbst sein, z. B. 10.10.1.100, oder eine CIDR-Spezifikation (Netzwerk-IP-Adresse/Subnetzpräfixlänge), die die IP-Adresse enthält, z. B. 10.10.1.0/24.

Für jeden `ActiveClient` Leitung, der Paketweiterleiter leitet unabhängig Pakete von der in der Zeile angegebenen Schnittstelle weiter.

Das Folgende ist ein Beispiel für die Konfigurationsdatei, die zwei Schnittstellen anhand des Schnittstellennamens spezifiziert:

```
ActiveClient = 10.10.6.45, 2003, ifname=eth0
ActiveClient = 10.10.6.45, 2003, ifname=eth1
NullAuthPermit = YES
```

Das Folgende ist ein Beispiel für die Konfigurationsdatei, die zwei Schnittstellen anhand der Schnittstellen-IP-Adresse spezifiziert:

```
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.1.100
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.2.100
NullAuthPermit = YES
```

Im Folgenden finden Sie ein Beispiel für die Konfigurationsdatei, die zwei Schnittstellen mithilfe von CIDR-Spezifikationen spezifiziert, die die Schnittstellen-IP-Adresse enthalten:

```
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.1.0/24
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.2.0/24
NullAuthPermit = YES
```

- Speichern Sie die Konfigurationsdatei. Achten Sie darauf, die Datei im ASCII-Format zu speichern, um Fehler zu vermeiden.
- Starten Sie den Paket Forwarder neu, indem Sie den folgenden Befehl ausführen:

```
sudo /etc/init.d/rpcapd restart
```



Hinweis Um den Paket Forwarder nach dem Ändern der Konfigurationsdatei erneut zu installieren, führen Sie den Installationsbefehl aus und ersetzen Sie `<extrahop_ip>` und `<extrahop_port>` mit dem `-k` Flag, um die geänderte Konfigurationsdatei beizubehalten. Zum Beispiel:

```
sudo sh ./install-rpcapd.sh -k
```

Überwachung mehrerer Schnittstellen auf einem Windows-Server

Bei Servern mit mehreren Schnittstellen können Sie die Paketweiterleitung so konfigurieren, dass Pakete von einer bestimmten Schnittstelle oder von mehreren Schnittstellen weitergeleitet werden, indem Sie die zugehörige Konfigurationsdatei auf dem Server bearbeiten.

Gehen Sie wie folgt vor, um die Konfigurationsdatei zu bearbeiten.

1. Öffnen Sie nach der Installation des Paket Forwarders auf dem Server die Konfigurationsdatei: C:\Program Files\rpcapd\rpcapd.ini

Die Konfigurationsdatei enthält diesen Text oder einen ähnlichen Text:

```
ActiveClient = 10.0.0.100,2003
NullAuthPermit = YES
```

2. Ändern Sie die bestehende ActiveClient-Zeile und erstellen Sie eine ActiveClient-Zeile für jede weitere zu überwachende Schnittstelle. Geben Sie jede Schnittstelle anhand ihres Schnittstellennamens oder ihrer IP-Adresse an.

```
ActiveClient = <extrahop_ip>, <extrahop_port>, ifname=<interface_address>
```

Wo *<interface_address>* ist die IP-Adresse der Schnittstelle, von der die Pakete weitergeleitet werden und *<interface_address>* kann entweder die IP-Adresse selbst sein, z. B. 10.10.1.100, oder eine CIDR-Spezifikation (Netzwerk-IP-Adresse/Subnetzpräfixlänge), die die IP-Adresse enthält, z. B. 10.10.1.0/24.

oder

```
ActiveClient = <extrahop_ip>, <extrahop_port>, ifaddr=<interface_name>
```

Wo *<interface_name>* ist der Name der Schnittstelle, von der aus die Pakete weitergeleitet werden. Der Name ist formatiert als \Device\NPF_{<GUID>}, wo *<GUID>* ist der global eindeutige Bezeichner (GUID) der Schnittstelle. Wenn die Schnittstellen-GUID beispielsweise 2C2FC212-701D-42E6-9EAE-BEE969FEFB3F, der Schnittstellename ist \Device\NPF_{2C2FC212-701D-42E6-9EAE-BEE969FEFB3F}.

Das Folgende ist ein Beispiel für die Konfigurationsdatei, die zwei Schnittstellen mit der Schnittstellen-IP-Adresse spezifiziert:

```
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.1.100
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.2.100
NullAuthPermit = YES
```

Im Folgenden finden Sie ein Beispiel für die Konfigurationsdatei, die zwei Schnittstellen mit CIDR-Spezifikationen spezifiziert, die die Schnittstellen-IP-Adresse enthalten:


```
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.1.0/24
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.2.0/24
NullAuthPermit = YES
```

Das Folgende ist ein Beispiel für die Konfigurationsdatei, die zwei Schnittstellen mit dem Schnittstellennamen spezifiziert:

```
ActiveClient = 10.10.6.45, 2003, ifname=\Device
\NPF_{2C2FC212-701D-42E6-9EAE-BEE969FEFB3F}
ActiveClient = 10.10.6.45, 2003, ifname=\Device
\NPF_{3C2FC212-701D-42E6-9EAE-BEE969FEFB3F}
NullAuthPermit = YES
```

3. Speichern Sie die Konfigurationsdatei (.ini). Achten Sie darauf, die Datei im ASCII-Format zu speichern, um Fehler zu vermeiden.
4. Starten Sie den Paket Forwarder neu, indem Sie den folgenden Befehl ausführen:

```
restart-service rpcapd
```

 **Hinweis** Um die Paket Forwarder-Software nach dem Ändern der Konfigurationsdatei erneut zu installieren, führen Sie den Installationsbefehl aus und ersetzen Sie `-RpcapIp` und `-RpcapPort` mit dem `-KeepConfig` Markierung , um die geänderte Konfigurationsdatei beizubehalten. Zum Beispiel:

```
.\install-rpcapd.ps1 -MgmtIp <extrahop_ip> -KeepConfig
```

oder

```
.\install-rpcapd.ps1 -InputDir . -KeepConfig
```

Konfiguration zusätzlicher RPCAP-Einstellungen

Standardmäßig akzeptiert das ExtraHop-System weitergeleitete Pakete auf Port 2003. Die Server, die den Software-Tap verwenden, werden angewiesen, den gesamten Datenverkehr weiterzuleiten, wie durch den Platzhalter (*) in der Schnittstellenadresse Spalte.

Gehen Sie wie folgt vor, um einen anderen Port anzugeben.

1. Gehen Sie zum Abschnitt RPCAP-Einstellungen und klicken Sie auf **2003**.
2. Ändern und modifizieren Sie die Einstellungen auf der Seite RPCAP-Portdefinition hinzufügen.

Hafen

Gibt den Listening-Port auf dem ExtraHop-System an. Jeder Port muss für jedes Schnittstellensubnetz auf demselben Server eindeutig sein. Serverübergreifend können unterschiedliche Subnetze für denselben Port konfiguriert werden.

Schnittstellenadresse

Gibt ein Subnetz auf dem Paketweiterleitungsserver an. Wenn der Server über mehrere Schnittstellen verfügt, die der Schnittstellenadresse entsprechen, sendet die erste Schnittstelle auf dem Server Datenverkehr an das ExtraHop-System, sofern der Schnittstellename nicht angegeben ist.

Name der Schnittstelle

Gibt die Schnittstelle auf dem Paketweiterleitungsserver an, von der Pakete weitergeleitet werden sollen.

 **Hinweis** Sie müssen eine Schnittstellenadresse oder einen Schnittstellennamen angeben. Wenn Sie beide angeben, gelten beide Kriterien.

Filter

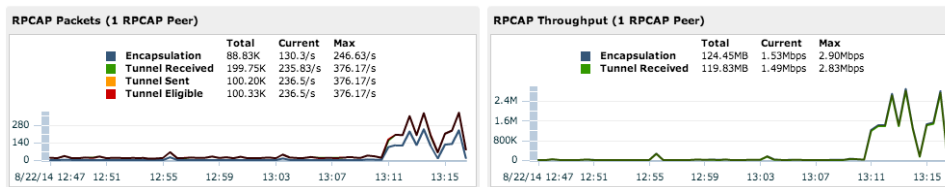
Gibt den Verkehr an, der mithilfe der Berkeley-Paketfilter-Syntax weitergeleitet werden soll. Zum Beispiel `TCP port 80` leitet nur TCP-Verkehr auf Port 80 weiter und `not TCP port 80` leitet nur Nicht-TCP-Verkehr auf Port 80 weiter.

3. klicken **Speichern**.

Analysieren von wire data von einer Paketweiterleitung

Um herauszufinden, wie viele wire data das ExtraHop-System vom Paket Forwarder empfängt, gehen Sie wie folgt vor:

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>` und klicken Sie auf **Systemeinstellungen** Symbol.
2. klicken **Gesundheit des Systems** um mehr Informationen über den weitergeleiteten Verkehr zu erhalten. Auf dieser Seite wird für jeden Software-Tap, der mit dem ExtraHop-System verbunden ist, ein Diagramm mit Paketen und Durchsatz angezeigt.



Die RPCAP Pakete und Durchsatzdiagramme enthalten vier Metriken:

Verkapselung

Die Gesamtzahl der vom ExtraHop-System empfangenen RPCAP-Kapselungspakete.

Geeignet für Tunnel

Gesamtzahl der Pakete, die an das ExtraHop-System weitergeleitet werden können.

Tunnel gesendet

Gesamtzahl der RPCAP-Tunnelpakete, die an das ExtraHop-System weitergeleitet wurden.

Tunnel empfangen

Gesamtzahl der RPCAP-Tunnelpakete, die vom ExtraHop-System empfangen wurden.

Die Werte Tunnelberechtigt, Tunnel gesendet und Tunnel empfangen sind identisch, wenn das ExtraHop-System alle vom Server gesendeten Pakete empfängt und verarbeitet. Wenn die Werte nicht identisch sind, ziehen Sie die folgenden Optionen zur Fehlerbehebung in Betracht:

- Wenn `Tunnel Sent` ist weniger als `Tunnel Eligible`, der Server ist nicht in der Lage, den gesamten Verkehr weiterzuleiten. Dieses Verhalten kann darauf hindeuten, dass die Paketweiterleitung mehr Verarbeitungs- oder ausgehende Bandbreitenressourcen auf dem Server erfordert. Erwägen Sie, den Weiterleitungsprozess auf eine separate CPU zu trennen oder eine dedizierte Schnittstelle für die Weiterleitung des Datenverkehrs zuzuweisen.
- Wenn `Tunnel Received` ist weniger als `Tunnel Sent`, das ExtraHop-System empfängt nicht den gesamten vom Server weitergeleiteten Datenverkehr. Dieses Verhalten kann auf eine Netzwerküberlastung oder unzureichende Ressourcen auf dem ExtraHop-System zurückzuführen sein. Wenn Sie vermuten, dass es sich um Letzteres handelt, wenden Sie sich an den ExtraHop-Support.

3. Nachdem Sie sich vergewissert haben, dass das ExtraHop-System Datenverkehr empfängt, beenden Sie den Gesundheit des Systems Seiten- und Anzeigemetriken in der ExtraHop Web UI.

Den Paket Forwarder von einem Linux-Server entfernen

Führen Sie die folgenden Befehle aus:

- Um die Software zu beenden und von einem Debian-basierten Linux-Server zu entfernen, führen Sie die folgenden Befehle aus:

```
sudo service rpcapd stop
sudo dpkg -r rpcapd
sudo dpkg --get-selections | grep rpcapd
```

Sie können auch das einstellen `-P` markieren, um das Paket vollständig von Ihrem System zu entfernen.

- Führen Sie die folgenden Befehle aus, um die Software zu beenden und von einem RPM-basierten Linux-Server zu entfernen:

```
service rpcapd stop
rpm -e rpcapd-<extrahop_firmware_version>.x86_64
```

- Führen Sie die folgenden Befehle aus, um den Software-Tap zu beenden und von einem anderen Linux-Server zu entfernen:

```
sudo /etc/init.d/rpcapd stop
sudo update-rc.d -f rpcapd remove
sudo rm -rf /opt/extrahop
sudo rm -f /etc/init.d/rpcapd
```

Den Paket Forwarder von einem Windows-Server entfernen

Um die Software von einem Windows-Server oder Ihrem Windows-Desktop zu entfernen:

1. Gehe zum **Startmenü** und wähle **Schalttafel**.
2. Wählen **Programm deinstallieren**.
3. Wählen **RPCAP-Dienst für Windows**.
4. Klicken Sie im Popup-Dialogfeld auf **entfernen**.
5. Wenn das Entfernen abgeschlossen ist, klicken Sie auf **Schliessen**.