

Systemintegritäts-Dashboard

Veröffentlicht: 2023-09-14

Das Systemstatus-Dashboard bietet eine große Sammlung von Diagrammen, mit denen Sie sicherstellen können, dass Ihr ExtraHop-System wie erwartet läuft, Probleme beheben und Bereiche bewerten können, die die Leistung beeinträchtigen. Sie können beispielsweise die Anzahl der vom ExtraHop-System verarbeiteten Pakete überwachen, um sicherzustellen, dass Pakete kontinuierlich erfasst werden.


Jedes Diagramm im Network Performance Dashboard enthält Visualisierungen von Systemleistungsdaten, die über die [ausgewähltes Zeitintervall](#), nach Region organisiert.

Das Systemintegritäts-Dashboard ist ein integriertes System-Dashboard, das Sie nicht bearbeiten, löschen oder zu einer gemeinsamen Sammlung hinzufügen können. Sie können jedoch [ein Diagramm kopieren](#) aus dem System Health Dashboard und füge es zu einem [benutzerdefiniertes Dashboard](#), oder du kannst [eine Kopie des Dashboard erstellen](#) und bearbeiten Sie es, um für Sie relevante Kennzahlen zu überwachen.



Hinweis Die Seite mit den Administrationseinstellungen bietet auch [Statusinformationen und Diagnosetools](#) für alle ExtraHop-Systeme.

Navigieren Sie im Systemstatus-Dashboard

Rufen Sie die Seite Systemstatus auf, indem Sie auf das Symbol Systemeinstellungen klicken  oder durch Anklicken **Armaturenbrett** von oben auf der Seite. Das Systemstatus-Dashboard zeigt automatisch Informationen über das ExtraHop-System an, mit dem Sie verbunden sind. Wenn Sie das Systemintegritäts-Dashboard von einer Konsole aus aufrufen, können Sie oben auf der Seite auf die Seitenauswahl klicken, um Daten für eine bestimmte Standort oder für alle Sites in Ihrer Umgebung anzuzeigen.

Die Diagramme im Systemstatus-Dashboard sind in die folgenden Abschnitte unterteilt:

Geräteerkennung

Sehen Sie sich die Gesamtanzahl der Geräte in Ihrem Netzwerk an. Sehen Sie, welche Geräte entdeckt wurden und wie viele dieser Geräte derzeit aktiv sind.

Datenfeed

Beurteilen Sie die Effizienz der Kabeldatenerfassung anhand von Diagrammen zu Durchsatz, Paketrate, Desynchronisierung und Erfassungsverlusten.

Rekorde

Zeigt die Gesamtanzahl der Datensätze an, die an einen angehängten Recordstore gesendet werden.

Auslöser

Überwachen Sie die Auswirkungen von Triggern auf Ihr ExtraHop-System. Sehen Sie, wie oft Trigger ausgeführt werden, wie oft sie ausfallen und welche Trigger Ihre CPU am stärksten belasten.

Öffnen Sie Data Stream und Recordstore

Verfolgen Sie die Aktivitäten von Open Data Stream (ODS) -Übertragungen zu und von Ihrem System. Zeigen Sie die Gesamtzahl der Remoteverbindungen, den Nachrichtendurchsatz und Details zu bestimmten Remote-Zielen an.

SSL Zertifikate

Überprüfen Sie die Statusinformationen für alle SSL-Zertifikate auf Ihrem ExtraHop-System.

Paketerfassung aus der Ferne (RPCAP)

Zeigen Sie die Anzahl der Pakete und Frames an, die von RPCAP-Peers gesendet und empfangen werden.

Fortgeschrittene Gesundheitsmetriken

Verfolgen Sie die Heap-Zuweisung im Zusammenhang mit der Datenerfassung, dem Systemdatenspeicher, Triggern und Fernübertragungen. Überwachen Sie den Schreibdurchsatz, die Größe des Arbeitssets und die Triggeraktivität im Systemdatenspeicher.

Geräteerkennung

Die Geräteerkennung Ein Abschnitt des Systemstatus-Dashboards bietet einen Überblick über die Gesamtzahl der Geräte in Ihrem Netzwerk. Sehen Sie, welche Arten von Geräten angeschlossen sind und wie viele dieser Geräte derzeit aktiv sind.

Die Geräteerkennung Dieser Abschnitt enthält die folgenden Diagramme:

- [Aktive Geräte](#)
- [Geräte insgesamt](#)

Aktive Geräte

Ein Flächendiagramm, das die Anzahl der L2-, L3-, Gateway- und benutzerdefinierten Geräte anzeigt, die während des ausgewählten Zeitintervalls aktiv im Netzwerk kommuniziert haben. Neben dem Flächendiagramm zeigt ein Wertdiagramm die Anzahl der L2-, L3-, Gateway- und benutzerdefinierten Geräte an, die im ausgewählten Zeitintervall aktiv waren.

Wie diese Informationen Ihnen helfen können

Überwachen Sie dieses Diagramm, nachdem Sie Änderungen an der SPAN-Konfiguration vorgenommen haben, um sicherzustellen, dass keine unbeabsichtigten Folgen auftreten, die das ExtraHop-System in einen schlechten Zustand versetzen könnten. Beispielsweise kann die versehentliche Einbindung eines Netzwerk die Kapazität der ExtraHop-Systemfunktionen belasten, da mehr Ressourcen verbraucht und mehr Paketverarbeitung erforderlich ist, was zu einer schlechten Leistung führt. Vergewissern Sie sich, dass das ExtraHop-System die erwartete Anzahl aktiver Geräte überwacht.

Geräte insgesamt

Ein Liniendiagramm, das die Gesamtzahl der vom ExtraHop-System überwachten L3- und benutzerdefinierten Geräte anzeigt, unabhängig davon, ob sie aktiv oder inaktiv sind, im ausgewählten Zeitintervall. Neben dem Flächendiagramm wird in einem Wertdiagramm die Gesamtzahl der L3- und benutzerdefinierten Geräte angezeigt, die derzeit vom ExtraHop-System überwacht werden.

Wie diese Informationen Ihnen helfen können

Überwachen Sie dieses Diagramm, nachdem Sie Änderungen an der SPAN-Konfiguration vorgenommen haben, um sicherzustellen, dass keine unbeabsichtigten Folgen auftreten, die das ExtraHop-System in einen schlechten Zustand versetzen könnten. Beispielsweise kann die versehentliche Einbindung eines Netzwerk die Kapazität der ExtraHop-Systemfunktionen belasten, da mehr Ressourcen verbraucht und mehr Paketverarbeitung erforderlich ist, was zu einer schlechten Leistung führt. Vergewissern Sie sich, dass das ExtraHop-System die erwartete Gesamtanzahl an Geräten enthält.

Datenfeed

Die Datenfeed In einem Bereich des Systemstatus-Dashboards können Sie die Effizienz der Kabeldatenerfassung anhand von Diagrammen zu Durchsatz, Paketrate, Desynchronisierung und Erfassungsausfällen beobachten.

Die Datenfeed Dieser Abschnitt enthält die folgenden Diagramme:

- [Durchsatz](#)
- [Paket-Rate](#)
- [Analysierte Ströme](#)
- [Desynchronisierungen](#)
- [Drop-Rate erfassen](#)
- [Auf die Festplatte geschriebene Metriken \(Log-Skala\)](#)

- [Lookback-Schätzungen für metrische Daten](#)

Durchsatz

Ein Flächendiagramm, das den Durchsatz eingehender Pakete im ausgewählten Zeitintervall darstellt, ausgedrückt in Byte pro Sekunde. Das Diagramm zeigt Durchsatzinformationen für analysierte und gefilterte Pakete sowie L2- und L3-Duplikate an.

Wie diese Informationen Ihnen helfen können

Das Überschreiten der Produktgrenzwerte kann zu Datenverlust führen. Eine hohe Durchsatzrate kann beispielsweise dazu führen, dass Pakete an der Span-Quelle oder an einem Span-Aggregator verworfen werden. In ähnlicher Weise kann eine große Anzahl von L2- oder L3-Duplikaten auch auf ein Problem an der Span-Quelle oder dem Span-Aggregator hinweisen und zu verzerrten oder falschen Metriken führen.

Die akzeptable Rate von Byte pro Sekunde hängt von Ihrem Produkt ab. Beziehen Sie sich auf die [Datenblatt für ExtraHop-Sensoren](#) um herauszufinden, welche Grenzwerte für Ihr ExtraHop-System gelten, und um festzustellen, ob die Byte-Rate pro Sekunde zu hoch ist.

Paket-Rate

Ein Flächendiagramm, das die Rate eingehender Pakete, ausgedrückt in Paketen pro Sekunde, anzeigt. In der Tabelle werden Informationen zur Paketrate für analysierte und gefilterte Pakete sowie für L2- und L3-Duplikate angezeigt.

Wie diese Informationen Ihnen helfen können

Das Überschreiten der Produktgrenzwerte kann zu Datenverlust führen. Eine hohe Paketrate kann beispielsweise dazu führen, dass Pakete an der Span-Quelle oder an einem Span-Aggregator verworfen werden. In ähnlicher Weise können große Mengen von L2- oder L3-Duplikaten auch auf ein Problem an der Span-Quelle oder dem Span-Aggregator hinweisen und zu verzerrten oder falschen Metriken führen.

Die akzeptable Paketrate pro Sekunde hängt von Ihrem Produkt ab. Weitere Informationen finden Sie in [Datenblatt für ExtraHop-Sensoren](#) um herauszufinden, welche Grenzwerte für Ihr ExtraHop-System gelten, und um festzustellen, ob die Rate der Pakete pro Sekunde zu hoch ist.

Analysierte Ströme

Ein Liniendiagramm, das die Anzahl der Flows anzeigt, die das ExtraHop-System im ausgewählten Zeitintervall analysiert hat. Das Diagramm zeigt auch, wie viele unidirektionale Flüsse im gleichen Zeitraum aufgetreten sind. Neben dem Liniendiagramm wird in einem Wertdiagramm die Gesamtzahl der analysierten und unidirektionalen Flüsse angezeigt, die im ausgewählten Zeitintervall aufgetreten sind. Ein Fluss ist ein Satz von Paketen, die Teil einer Transaktion zwischen zwei Endpunkten über ein Protokoll wie TCP, UDP oder ICMP sind.

Wie diese Informationen Ihnen helfen können

Das Überschreiten der Produktgrenzwerte kann zu Datenverlust führen. Beispielsweise könnte eine hohe Anzahl analysierter Datenflüsse dazu führen, dass Pakete an der Span-Quelle oder an einem Span-Aggregator verworfen werden.

Desynchronisierungen

Ein Liniendiagramm, das das Auftreten systemweiter Desynchronisierungen auf dem ExtraHop-System im ausgewählten Zeitintervall anzeigt. Neben dem Liniendiagramm wird in einem Wertdiagramm die Gesamtzahl der Desynchronisierungen angezeigt, die im ausgewählten Zeitintervall aufgetreten sind. Eine Desynchronisierung liegt vor, wenn der ExtraHop-Datenfeed ein TCP-Paket verwirft und daher nicht mehr mit einer TCP-Verbindung synchronisiert wird.

Wie diese Informationen Ihnen helfen können

Eine große Anzahl von Desynchronisierungen kann auf verworfene Pakete auf der Überwachungsschnittstelle, dem SPAN oder dem Netzwerk-Tap hinweisen.

Wenn Anpassungen an Ihrem SPAN eine große Anzahl von Desynchronisierungen nicht reduzieren, wenden Sie sich an [ExtraHop-Unterstützung](#).

Verkürzte Pakete

Ein Liniendiagramm, das das Auftreten von gekürzten Paketen auf dem ExtraHop-System im ausgewählten Zeitintervall anzeigt. Neben dem Liniendiagramm wird in einem Wertdiagramm die Gesamtzahl der gekürzten Pakete angezeigt, die im ausgewählten Zeitintervall aufgetreten sind. Ein abgeschnittenes Paket liegt vor, wenn die tatsächliche Gesamtlänge des Paket geringer ist als die Gesamtlänge, die im IP-Header angegeben ist.

Wie diese Informationen Ihnen helfen können

Verkürzte Pakete deuten möglicherweise auf Paket Slicing hin. Ein Sensor verwirft alle abgeschnittenen Pakete, die er empfängt, was dazu führen kann [Desynchronisierungen](#) auftreten.

Drop-Rate erfassen

Ein Liniendiagramm, das den Prozentsatz der Pakete anzeigt, die während des ausgewählten Zeitintervalls an der Netzwerkkartenschnittstelle eines ExtraHop-Systems verworfen wurden.

Wie diese Informationen Ihnen helfen können

Paketverluste treten häufig auf, wenn Sensorschwellenwerte überschritten werden. Beziehen Sie sich auf die [Datenblatt für ExtraHop-Sensoren](#) um herauszufinden, wo die Grenzen Ihres ExtraHop-Systems liegen.

Ladung erfassen

Ein Liniendiagramm, das den Prozentsatz der Zyklen auf dem ExtraHop-System anzeigt, die von aktiven Capture-Threads im ausgewählten Zeitintervall verbraucht wurden, basierend auf der gesamten Capture-Thread-Zeit. Klicken Sie auf das zugehörige Durchschnittliche Aufnahmelast Diagramm, um nach Threads aufzuschlüsseln und festzustellen, welche Threads die meisten Ressourcen verbrauchen.

Wie diese Informationen Ihnen helfen können

Achten Sie auf Spitzen oder ein steigendes Wachstum der Fanglast, um zu überwachen, ob Sie sich den Sensorgrenzwerten nähern. Beziehen Sie sich auf die [Datenblatt für ExtraHop-Sensoren](#) um die Grenzen Ihres ExtraHop-Systems zu entdecken.

Auf die Festplatte geschriebene Metriken (Log-Skala)

Ein Liniendiagramm, das den Speicherverbrauch von Messwerten, die während des ausgewählten Zeitintervalls auf die Festplatte geschrieben wurden, in Byte pro Sekunde anzeigt. Da zwischen den Datenpunkten ein großer Bereich besteht, wird die Festplattennutzung in logarithmischer Skala angezeigt.

Wie diese Informationen Ihnen helfen können

Es ist wichtig, dass Sie sich darüber im Klaren sind, wie viel Speicherplatz die Metriken in Ihrem Datenspeicher beanspruchen. Die Größe des Speicherplatzes in Ihrem Datenspeicher wirkt sich auf die Menge des verfügbaren Lookbacks aus. Wenn einige Metriken zu viel Speicherplatz beanspruchen, können Sie die zugehörigen Trigger untersuchen, um zu sehen, ob Sie den Auslöser ändern können, um ihn effizienter zu gestalten.

Lookback-Schätzungen für metrische Daten

Zeigt die geschätzten Datenspeicher-Lookback-Metriken auf dem ExtraHop-System an. Lookback-Metriken sind in Zeitintervallen von 24 Stunden, 1 Stunde, 5 Minuten und 30 Sekunden verfügbar, basierend auf der Schreibdurchsatzrate, die in Byte pro Sekunde ausgedrückt wird.

Wie diese Informationen Ihnen helfen können

Anhand dieser Tabelle können Sie ermitteln, wie weit Sie historische Daten für bestimmte Zeitintervalle zurückverfolgen können. Beispielsweise können Sie Daten in Intervallen von 1 Stunde bis zu 9 Tagen nachschlagen.

Rekorde

Die Rekorde In einem Bereich des Systemstatus-Dashboards können Sie die Effizienz der Kabeldatenerfassung anhand von Diagrammen zur Anzahl der Datensätze und zum Durchsatz beobachten.

Die Datenfeed Dieser Abschnitt enthält die folgenden Diagramme:

- [Anzahl der Datensätze](#)
- [Durchsatz aufzeichnen](#)

Anzahl der Datensätze

Ein Liniendiagramm, das die Anzahl der Datensätze anzeigt, die im ausgewählten Zeitintervall an einen Recordstore gesendet wurden. Neben dem Liniendiagramm wird in einem Wertdiagramm die Gesamtzahl der im ausgewählten Zeitintervall gesendeten Datensätze angezeigt.

Wie diese Informationen Ihnen helfen können

Eine extrem hohe Anzahl von Datensätzen, die an einen Recordstore gesendet werden, kann zu langen Nachrichtenwarteschlangen und verworfenen Nachrichten im Recordstore führen. Sehen Sie sich Diagramme in der [Öffnen Sie Data Stream und Recordstore](#) Im Abschnitt Systemintegritäts-Dashboard finden Sie weitere Informationen zu Recordstore-Übertragungen.

Durchsatz aufzeichnen

Ein Liniendiagramm, das die Anzahl der Datensätze in Byte anzeigt, die an einen Recordstore gesendet wurden. Neben dem Liniendiagramm wird in einem Wertdiagramm die Gesamtmenge der im ausgewählten Zeitintervall gesendeten Datensätze in Byte angezeigt.

Wie diese Informationen Ihnen helfen können

Dieses Diagramm spiegelt keine Größenanpassungen auf der Grundlage von Komprimierung oder Datenduplikation wider und sollte nicht zur Schätzung der Recordstore-Kosten verwendet werden. Ein extrem hoher Datensatzdurchsatz kann zu langen Warteschlangenlängen und verworfenen Nachrichten im Recordstore führen. Sehen Sie sich Diagramme in der [Öffnen Sie Data Stream und Recordstore](#) Im Abschnitt Systemintegritäts-Dashboard finden Sie weitere Informationen zu Recordstore-Übertragungen.

Auslöser

Die Auslöser In einem Bereich des Systemstatus-Dashboards können Sie die Auswirkungen von Triggern auf Ihr System überwachen. Sehen Sie, wie oft Trigger ausgeführt werden, wie oft sie ausfallen und welche Trigger Ihre CPU am stärksten belasten.

Die Auslöser Dieser Abschnitt enthält die folgenden Diagramme:

- [Last auslösen](#)
- [Triggerverzögerung](#)
- [Trigger wird ausgeführt und gelöscht](#)
- [Einzelheiten zum Auslöser](#)
- [Laden nach Trigger auslösen](#)
- [Trigger wird von Trigger ausgeführt](#)
- [Ausnahmen nach Trigger auslösen](#)

- [Zyklen nach Thread auslösen](#)

Last auslösen

Ein Liniendiagramm, das den Prozentsatz der CPU-Zyklen anzeigt, die Triggerprozessen zugewiesen wurden und während des ausgewählten Zeitintervalls von Triggern verbraucht wurden.

Wie diese Informationen Ihnen helfen können

Achten Sie auf Spitzen oder ein steigendes Wachstum der Triggerlast, insbesondere nach dem Erstellen eines neuen Auslöser oder dem Ändern eines vorhandenen Auslöser. Wenn Sie eine der beiden Bedingungen bemerken, sehen Sie sich die [Laden nach Trigger auslösen](#) Diagramm, um zu sehen, welche Trigger die meisten Ressourcen verbrauchen.

Triggerverzögerung

Ein Säulendiagramm, das die maximalen Triggerverzögerungen, die während des ausgewählten Zeitintervalls aufgetreten sind, in Millisekunden anzeigt. Neben dem Säulendiagramm wird in einem Wertdiagramm die längste Triggerverzögerung angezeigt, die im ausgewählten Zeitintervall aufgetreten ist. Eine Triggerverzögerung ist die Zeitspanne zwischen der Erfassung eines Triggerereignisses und der Erstellung eines Trigger-Threads für das Ereignis.

Wie diese Informationen Ihnen helfen können

Lange Auslöseverzögerungen können auf Verarbeitungsprobleme hinweisen. Sehen Sie sich die [Ausnahmen nach Trigger auslösen](#) und [Laden nach Trigger auslösen](#) Diagramme, um zu sehen, welcher Auslöser die meisten unbehandelten Ausnahmen auslöst und welcher die meisten Ressourcen verbraucht.

Trigger wird ausgeführt und gelöscht

Ein Linien- und Säulendiagramm, in dem das Liniendiagramm anzeigt, wie oft Trigger ausgeführt wurden, und das dazugehörige Säulendiagramm zeigt, wie oft Trigger im ausgewählten Zeitintervall gelöscht wurden. Neben dem Linien- und Säulendiagramm zeigt ein Wertdiagramm die Gesamtzahl der Triggerausführungen und Drops an, die im ausgewählten Zeitintervall aufgetreten sind. Diese Diagramme bieten einen allgemeinen Überblick über alle Trigger, die derzeit auf dem ExtraHop-System ausgeführt werden.

Wie diese Informationen Ihnen helfen können

Suchen Sie im Linien- und Säulendiagramm nach Spitzen und untersuchen Sie alle Auslöser, die zu dem Anstieg geführt haben. Möglicherweise stellen Sie beispielsweise eine erhöhte Aktivität fest, wenn ein Auslöser geändert oder ein neuer Auslöser aktiviert wurde. Sehen Sie sich das [Trigger wird von Trigger ausgeführt](#) Diagramm, um zu sehen, welche Trigger am häufigsten ausgeführt werden.

Einzelheiten zum Auslöser

Ein Listendiagramm, das einzelne Trigger und die Anzahl der Zyklen, Ausführungen und Ausnahmen anzeigt, die den einzelnen Triggern im ausgewählten Zeitintervall zugewiesen wurden. Standardmäßig ist die Liste der Trigger in absteigender Reihenfolge nach Triggerzyklen sortiert.

Wie diese Informationen Ihnen helfen können

Identifizieren Sie, welche Auslöser die meisten Zyklen verbrauchen. Trigger, die zu häufig ausgeführt werden oder auf andere Weise mehr Zyklen verbrauchen, als sie sollten, können mehr Quellen als nötig zugewiesen werden. Stellen Sie sicher, dass jeder überaktive Auslöser nur der spezifischen Quelle zugewiesen ist, aus der Sie Daten sammeln müssen.

Laden nach Trigger auslösen

Ein Liniendiagramm, das den Prozentsatz der CPU-Zyklen anzeigt, die Triggerprozessen zugewiesen sind und während des ausgewählten Zeitintervalls von Triggern verbraucht wurden, aufgelistet nach Triggernamen.

Wie diese Informationen Ihnen helfen können

Identifizieren Sie, welche Auslöser die meisten Zyklen verbrauchen. Trigger, die mehr Zyklen verbrauchen, als sie sollten, können mehr Quellen als nötig zugewiesen werden. Stellen Sie sicher, dass jeder überaktive Auslöser nur der spezifischen Quelle zugewiesen ist, aus der Sie Daten sammeln müssen.

Trigger wird von Trigger ausgeführt

Ein Liniendiagramm, das anzeigt, wie oft jeder aktive Auslöser im ausgewählten Zeitintervall ausgeführt wurde.

Wie diese Informationen Ihnen helfen können

Suchen Sie nach Triggern, die häufiger als erwartet ausgeführt werden, was darauf hindeuten könnte, dass der Auslöser zu breit zugewiesen ist. Ein Auslöser, der allen Anwendungen oder allen Geräten zugewiesen ist, kann hohe Leistungseinbußen nach sich ziehen. Ein Auslöser, der einer erweiterten Gerätegruppe zugewiesen ist, sammelt möglicherweise Messwerte, die Sie nicht möchten. Um die Auswirkungen auf die Leistung zu minimieren, sollte ein Auslöser nur den spezifischen Quellen zugewiesen werden, aus denen Sie Daten sammeln müssen.

Eine hohe Aktivität kann auch darauf hindeuten, dass ein Auslöser härter arbeitet, als er muss. Beispielsweise kann ein Auslöser bei mehreren Ereignissen ausgeführt werden, bei denen es effizienter wäre, separate Trigger zu erstellen, oder ein Trigger-Skript entspricht möglicherweise nicht den empfohlenen Skriptrichtlinien, wie in der [Leitfaden mit bewährten Methoden für Trigger](#).

Ausnahmen nach Trigger auslösen

Ein Liniendiagramm, das die Anzahl der unbehandelten Ausnahmen, sortiert nach Auslöser, anzeigt, die im ausgewählten Zeitintervall auf dem ExtraHop-System aufgetreten sind.

Wie diese Informationen Ihnen helfen können

Trigger-Ausnahmen sind die Hauptursache für Leistungsprobleme bei Triggern. Wenn dieses Diagramm darauf hinweist, dass eine Trigger-Ausnahme aufgetreten ist, sollten Sie den Auslöser sofort untersuchen.

Zyklen nach Thread auslösen

Ein Liniendiagramm, das die Anzahl der Triggerzyklen anzeigt, die von Triggern für einen Thread verbraucht wurden.

Wie diese Informationen Ihnen helfen können

Triggerverluste können auftreten, wenn der Verbrauch eines Threads erheblich höher ist als der der anderen, auch wenn der Thread-Verbrauch gering ist. Achten Sie auf einen gleichmäßigen Zyklusverbrauch zwischen den Threads.

Öffnen Sie Data Stream und Recordstore

Im Bereich Open Data Stream (ODS) und Recordstore des Systems Health Dashboard können Sie die Aktivitäten von ODS- und Recordstore-Übertragungen zu und von Ihrem System verfolgen. Sie können auch die Gesamtzahl der Remoteverbindungen, den Nachrichtendurchsatz und Details zu bestimmten Remote-Zielen anzeigen.

Die Open Data Stream (ODS) und Recordstore Dieser Abschnitt enthält die folgenden Diagramme:

- [Nachrichtendurchsatz](#)
- [Gesendete Nachrichten](#)
- [Nach Remotetyp verworfene Nachrichten](#)
- [Fehler beim Senden von Nachrichten](#)
- [Verbindungen](#)
- [Länge der Exremote-Nachrichtenwarteschlange nach Ziel](#)

- [Länge der Nachrichtenwarteschlange nach Remote-Typ ausschließen](#)
- [Einzelheiten zum Ziel](#)

Nachrichtendurchsatz

Ein Liniendiagramm, das den Durchsatz von Fernmeldungsdaten in Byte anzeigt. Neben dem Liniendiagramm zeigt ein Wertdiagramm die durchschnittliche Durchsatzrate von Fernmeldungsdaten über das ausgewählte Zeitintervall an. Fernnachrichten sind Übertragungen, die vom ExtraHop-System über einen offenen Datenstrom (ODS) an einen Recordstore oder an Systeme von Drittanbietern gesendet werden.

Wie diese Informationen Ihnen helfen können

Überwachen Sie dieses Diagramm, um sicherzustellen, dass die Byte wie erwartet übertragen werden. Wenn Sie niedrige Durchsatzraten feststellen, liegt möglicherweise ein Problem mit der Konfiguration eines ODS oder eines angeschlossenen Recordstore vor. Signifikante Durchsatzeinbrüche können auf Probleme mit Ihren Datenströmen hinweisen.

Gesendete Nachrichten

Ein Liniendiagramm, das die durchschnittliche Rate anzeigt, mit der Remote-Nachrichten vom ExtraHop-System an ein Recordstore- oder ODS-Ziel (Open Data Stream) gesendet wurden. Neben dem Liniendiagramm zeigt ein Wertdiagramm die Gesamtzahl der Nachrichten an, die im ausgewählten Zeitintervall gesendet wurden.

Wie diese Informationen Ihnen helfen können

Überwachen Sie dieses Diagramm, um sicherzustellen, dass Pakete wie erwartet gesendet werden. Wenn keine Pakete gesendet werden, liegt möglicherweise ein Problem mit der Konfiguration eines ODS oder eines angehängten Recordstore vor.

Nach Remotetyp verworfene Nachrichten

Ein Liniendiagramm, das die durchschnittliche Rate von Remotenachrichten anzeigt, die gelöscht wurden, bevor sie einen Recordstore oder ein ODS-Ziel erreichten.

Wie diese Informationen Ihnen helfen können

Verworfene Nachrichten weisen auf Verbindungsprobleme mit dem Remote-Ziel hin. Eine hohe Anzahl von Drops könnte auch darauf hinweisen, dass der Nachrichtendurchsatz zu hoch ist, um vom ExtraHop-System oder dem Zielsystem verarbeitet zu werden.

Fehler beim Senden von Nachrichten

Ein Liniendiagramm, das die Anzahl der Fehler anzeigt, die beim Senden einer Remote-Nachricht an einen Recordstore oder ein ODS-Ziel aufgetreten sind. Überwachen Sie dieses Diagramm, um sicherzustellen, dass Pakete wie erwartet gesendet werden. Übertragungsfehler können Folgendes beinhalten:

Fehler auf dem Zielsystem

Die Anzahl der Fehler, die von Recordstores oder ODS-Zielen an das ExtraHop-System zurückgegeben werden. Diese Fehler sind auf dem Zielsystem aufgetreten und deuten nicht auf ein Problem mit dem ExtraHop-System hin.

Verworfene Nachrichten in voller Warteschlange

Die Anzahl der an Datensatzspeicher und ODS-Ziele gesendeten Nachrichten, die gelöscht wurden, weil die Nachrichtenwarteschlange auf dem Zielsystem voll war. Eine hohe Anzahl verworfener Nachrichten kann darauf hindeuten, dass der Nachrichtendurchsatz zu hoch ist, um vom ExtraHop-System oder dem Zielsystem verarbeitet zu werden. Schau dir das an [Länge der Exremote-Nachrichtenwarteschlange nach Ziel](#) und der [Einzelheiten zum Ziel](#) Diagramme, um festzustellen, ob Ihre Übertragungsfehler möglicherweise auf eine lange Nachrichtenwarteschlange zurückzuführen sind.

Nicht übereinstimmende Zielmeldungen

Die Anzahl der gelöschten Remote-Nachrichten, weil das im Open Data Stream (ODS) -Triggerskript angegebene Remotesystem nicht mit dem Namen übereinstimmt, der auf der Seite Open Data Streams in den Administrationseinstellungen konfiguriert wurde. Stellen Sie sicher, dass die Namen der Remotesysteme in den Triggerskripten und den Administrationseinstellungen konsistent sind.

Fehler beim Dekodieren gelöschter Nachrichten

Die Anzahl der Nachrichten, die aufgrund interner Kodierungsprobleme zwischen ExtraHop Capture (excap) und ExtraHop Remote (exremote) verloren gegangen sind.

Verbindungen

Ein Linien- und Säulendiagramm, in dem das Liniendiagramm die Anzahl der Versuche anzeigt, die das System unternommen hat, eine Verbindung zu einem Remote-Zielserver herzustellen, und das dazugehörige Säulendiagramm die Anzahl der Fehler anzeigt, die als Ergebnis dieser Versuche aufgetreten sind. Neben dem Linien- und Säulendiagramm zeigt ein Wertdiagramm die Gesamtzahl der Verbindungsversuche und Verbindungsfehler an, die im ausgewählten Zeitintervall aufgetreten sind.

Wie diese Informationen Ihnen helfen können

Identifizieren Sie Zielserver, die ungewöhnlich viele Verbindungsversuche erfordern oder unverhältnismäßig viele Verbindungsfehler verursachen. Ein Anstieg der Verbindungsversuche könnte darauf hindeuten, dass der Zielserver nicht verfügbar ist.

Länge der Exremote-Nachrichtenwarteschlange nach Ziel

Ein Liniendiagramm, das die Anzahl der Nachrichten in der ExtraHop Remote (exremote) -Warteschlange anzeigt, die darauf warten, vom ExtraHop-System verarbeitet zu werden.

Wie diese Informationen Ihnen helfen können

Eine hohe Anzahl von Nachrichten in der Warteschlange kann darauf hindeuten, dass der Nachrichtendurchsatz zu hoch ist, um vom ExtraHop-System oder dem Zielserver verarbeitet zu werden. Beziehen Sie sich auf den Wert Exremote Full Queue Dropped Messages in der [Fehler beim Senden von Nachrichten](#) Diagramm, um festzustellen, ob Nachrichtenabbrüche aufgetreten sind.

Länge der Nachrichtenwarteschlange nach Remote-Typ ausschließen

Ein Liniendiagramm, das die Anzahl der Remote-Zielnachrichten in der ExtraHop Capture (Excap) -Warteschlange anzeigt, die darauf warten, vom ExtraHop-System verarbeitet zu werden.

Wie diese Informationen Ihnen helfen können

Eine hohe Anzahl von Nachrichten in der Warteschlange kann darauf hindeuten, dass der Nachrichtendurchsatz zu hoch ist, um vom ExtraHop-System oder dem Zielserver verarbeitet zu werden.

Beziehen Sie sich auf die [Nach Remotetyp verworfene Nachrichten](#) Diagramm, um festzustellen, ob Nachrichtenabbrüche aufgetreten sind.

Einzelheiten zum Ziel

Ein Listendiagramm, das die folgenden Metriken zu Recordstore- oder ODS-Remote-Zielen im ausgewählten Zeitintervall anzeigt: Zielname, Zielnachrichten-Bytes out, gesendete Zielnachrichten, Zielserverfehler, gelöschte Nachrichten in voller Warteschlange, Dekodierungsfehler, gelöschte Nachrichten, Zielserver-Verbindungsversuche und Zielserver-Verbindungsfehler.

Wie diese Informationen Ihnen helfen können

Wenn Sie Nachrichtenfehler sehen, die in der [Gesendete Nachrichten](#) Diagramm, die Details in diesem Diagramm können Ihnen helfen, die Hauptursache von Fernmeldungsfehlern zu ermitteln.

SSL Zertifikate

Im Bereich SSL-Zertifikate des Systemstatus-Dashboards können Sie die Statusinformationen für alle SSL-Zertifikate auf Ihrem System überprüfen.

Die SSL Zertifikate Dieser Abschnitt enthält die folgende Tabelle:

- [Einzelheiten zum Zertifikat](#)

Einzelheiten zum Zertifikat

Ein Listendiagramm, das die folgenden Informationen für jedes Zertifikat anzeigt:

Entschlüsselte Sitzungen

Die Anzahl der Sitzungen, die erfolgreich entschlüsselt wurden.

Nicht unterstützte Sitzungen

Die Anzahl der Sitzungen, die mit passiver Analyse nicht entschlüsselt werden konnten, z. B. beim DHE-Schlüsselaustausch.

Getrennte Sitzungen

Die Anzahl der Sitzungen, die aufgrund von Desynchronisierungen nicht oder nur teilweise entschlüsselt wurden.

Passthrough-Sitzungen

Die Anzahl der Sitzungen, die aufgrund von Hardwarefehlern nicht entschlüsselt wurden, z. B. aufgrund von Fehlern, die durch Überschreitung der Spezifikationen der SSL-Beschleunigungshardware verursacht wurden.

Mit Shared Secret entschlüsselte Sitzungen

Die Anzahl der Sitzungen, die mit einem gemeinsamen geheimen Schlüssel entschlüsselt wurden.

Wie diese Informationen Ihnen helfen können

Überwachen Sie dieses Diagramm, um sicherzustellen, dass die richtigen SSL-Zertifikate auf dem ExtraHop-System installiert sind und die Entschlüsselung wie erwartet durchgeführt wird.

Paketerfassung aus der Ferne (RPCAP)

Im Bereich Remote Packet Capture (RPCAP) des Systemstatus-Dashboards können Sie die Anzahl der Pakete und Frames anzeigen, die von RPCAP-Peers gesendet und vom ExtraHop-System empfangen wurden.

Die Paketerfassung aus der Ferne (RPCAP) Dieser Abschnitt enthält die folgenden Diagramme:

- [Weitergeleitet von Peer](#)
- [Vom ExtraHop-System empfangen](#)

Weitergeleitet von Peer

Ein Listendiagramm, das die folgenden Informationen zu Paketen und Frames anzeigt, die von einem RPCAP-Peer weitergeleitet werden:

Weitergeleitete Pakete

Die Anzahl der Pakete, die ein RPCAP-Peer versucht hat, an ein ExtraHop-System weiterzuleiten.

Forwarder-Schnittstellenpakete

Die Gesamtzahl der Pakete, die vom Forwarder angesehen wurden. Forwarder auf RPCAP-Geräten koordinieren sich miteinander, um zu verhindern, dass mehrere Geräte dasselbe Paket senden. Dies ist die Anzahl der Pakete, die angesehen wurden, bevor Frames entfernt wurden, um den

weitergeleiteten Verkehr zu reduzieren, und bevor Frames durch benutzerdefinierte Filter entfernt wurden.

Forwarder-Kernel-Frame-Drops

Die Anzahl der Frames, die gelöscht wurden, weil der Kernel des RPCAP-Peers mit dem Stream ungefilterter Frames überlastet war. Ungefilterte Frames wurden vom Kernel nicht gefiltert, um doppelte Pakete oder Pakete zu entfernen, die aufgrund benutzerdefinierter Regeln nicht weitergeleitet werden sollten.

Die Forwarder-Schnittstelle wird unterbrochen

Die Anzahl der Pakete, die verworfen wurden, weil der RPCAP-Forwarder mit dem Stream ungefilterter Frames überlastet war. Ungefilterte Frames wurden nicht gefiltert, um doppelte Pakete oder Pakete zu entfernen, die aufgrund benutzerdefinierter Regeln nicht weitergeleitet werden sollten.

Wie diese Informationen Ihnen helfen können

Jedes Mal, wenn Sie Pakete sehen, die vom RPCAP-Peer verworfen wurden, deutet dies darauf hin, dass ein Problem mit der RPCAP-Software vorliegt.

Vom ExtraHop-System empfangen

Ein Listendiagramm, das die folgenden Informationen zu Paketen und Frames anzeigt, die von einem ExtraHop-System von einem Remote Packet Capture (RPCAP) -Peer empfangen werden:

Gekapselte Bytes

Die Gesamtgröße aller Pakete, die sich auf den UDP-Fluss vom RPCAP-Gerät zum ExtraHop-System beziehen, in Byte. Diese Information zeigt Ihnen, wie viel Traffic der RPCAP-Forwarder Ihrem Netzwerk hinzufügt.

Gekapselte Pakete

Die Anzahl der Pakete, die sich auf den UDP-Fluss vom RPCAP-Gerät zum ExtraHop-System beziehen.

Tunnel-Bytes

Die Gesamtgröße der Pakete, ohne Kapselungsheader, die das ExtraHop-System von einem RPCAP-Gerät empfangen hat, in Byte.

Tunnel-Pakete

Die Anzahl der Pakete, die das ExtraHop-System von einem RPCAP-Peer empfangen hat. Diese Zahl sollte der Zahl der weitergeleiteten Pakete in der Tabelle Vom Remote-Gerät gesendet sehr ähnlich sein. Wenn zwischen diesen beiden Zahlen eine große Lücke besteht, fallen Pakete zwischen dem RPCAP-Gerät und dem ExtraHop-System ab.

Wie diese Informationen Ihnen helfen können

Die Verfolgung der gekapselten Pakete und Bytes ist eine gute Methode, um sicherzustellen, dass RPCAP-Forwarder Ihr Netzwerk nicht unnötig belasten. Sie können Tunnelpakete und Bytes überwachen, um sicherzustellen, dass das ExtraHop-System alles empfängt, was das RPCAP-Gerät sendet.

Fortgeschrittene Gesundheitsmetriken

Im Bereich Advanced Health Metrics des Systems Health Dashboard können Sie die Heap-Zuweisung im Zusammenhang mit der Datenerfassung, dem Systemdatenspeicher, Triggern und Fernübertragungen verfolgen. Überwachen Sie den Schreibdurchsatz, die Größe des Arbeitssets und die Triggeraktivität im Systemdatenspeicher.

Die Fortgeschrittene Gesundheitsmetriken Dieser Abschnitt enthält die folgenden Diagramme:

- [Erfassung und Datenspeicher-Heap-Zuweisung](#)

- [Trigger- und Remote-Heap-Zuweisung](#)
- [Schreibdurchsatz speichern](#)
- [Größe des Arbeitssets](#)
- [Laden des Datenspeicher-Triggers](#)
- [Der Datenspeicher-Trigger wird ausgeführt und gelöscht](#)
- [Datenspeicherauslöserausnahmen nach Trigger](#)

Erfassung und Datenspeicher-Heap-Zuweisung

Ein Liniendiagramm, das die Speichermenge anzeigt, die das ExtraHop-System für die Erfassung von Netzwerkpaketen und für den Datenspeicher reserviert.

Wie diese Informationen Ihnen helfen können

Die Daten in dieser Tabelle dienen internen Zwecken und können angefordert werden von [ExtraHop-Unterstützung](#) [↗](#) um Ihnen bei der Diagnose eines Problems zu helfen.

Trigger- und Remote-Heap-Zuweisung

Ein Liniendiagramm, das die Speichermenge, ausgedrückt in Byte, anzeigt, die das ExtraHop-System der Verarbeitung von Capture-Trigger und Open Data Streams (ODS) widmet.

Wie diese Informationen Ihnen helfen können

Die Daten in dieser Tabelle dienen internen Zwecken und können angefordert werden von [ExtraHop-Unterstützung](#) [↗](#) um Ihnen bei der Diagnose eines Problems zu helfen.

Schreibdurchsatz speichern

Ein Flächendiagramm, das den Datenspeicher-Schreibdurchsatz, ausgedrückt in Byte, auf dem ExtraHop-System anzeigt. Das Diagramm zeigt Daten für das ausgewählte Zeitintervall und für Intervalle von 24 Stunden, 1 Stunde, 5 Minuten und 30 Sekunden an.

Wie diese Informationen Ihnen helfen können

Die Daten in dieser Tabelle dienen internen Zwecken und können angefordert werden von [ExtraHop-Unterstützung](#) [↗](#) um Ihnen bei der Diagnose eines Problems zu helfen.

Größe des Arbeitssets

Ein Flächendiagramm, das die Größe des Schreib-Cache-Arbeitssets für Metriken auf dem ExtraHop-System anzeigt. Die Größe des Arbeitssets gibt an, wie viele Metriken für das ausgewählte Zeitintervall und für Intervalle von 24 Stunden, 1 Stunde, 5 Minuten und 30 Sekunden in den Cache geschrieben werden können.

Wie diese Informationen Ihnen helfen können

Die Daten in diesem Diagramm können nach der Erstellung oder Änderung des Auslöser stark ansteigen, wenn das Trigger-Skript Metriken nicht effizient sammelt.

Laden des Datenspeicher-Triggers

Ein Liniendiagramm, das den Prozentsatz der Zyklen anzeigt, die von datenspeicherspezifischen Triggern auf dem ExtraHop-System verbraucht wurden, basierend auf der gesamten Capture-Thread-Zeit.

Wie diese Informationen Ihnen helfen können

Achten Sie auf Spitzen oder ein steigendes Wachstum der Datenspeicher-Triggerlast, insbesondere nach dem Erstellen eines neuen Datenspeicher-Triggers oder dem Ändern eines vorhandenen Datenspeicher-Triggers. Wenn Sie beides bemerken, klicken Sie auf **Last auslösen** Metriklabel, um eine Aufschlüsselung durchzuführen und zu sehen, welche Datenspeicher-Trigger die meisten Ressourcen verbrauchen.

Der Datenspeicher-Trigger wird ausgeführt und gelöscht

Ein Linien- und Säulendiagramm, in dem das Liniendiagramm anzeigt, wie oft datenspeicherspezifische Trigger auf dem ExtraHop-System während des ausgewählten Zeitintervalls ausgeführt wurden, und das dazugehörige Säulendiagramm die Anzahl der datenspeicherspezifischen Trigger anzeigt, die während des ausgewählten Zeitintervalls aus der Warteschlange der Trigger gelöscht wurden, die darauf warten, auf dem ExtraHop-System ausgeführt zu werden.

Wie diese Informationen Ihnen helfen können

Ein einzelner Datenspeicher-Trigger, der häufig ausgeführt wird, kann darauf hinweisen, dass der Auslöser allen Quellen zugewiesen wurde, z. B. Anwendungen oder Geräten. Um die Auswirkungen auf die Leistung zu minimieren, sollte ein Auslöser nur den spezifischen Quellen zugewiesen werden, aus denen Sie Daten sammeln müssen.

Aus dem [Laden des Datenspeicher-Triggers](#) Diagramm, klicken Sie auf **Last auslösen** Metriklabel, um eine Aufschlüsselung durchzuführen und zu sehen, welche Datenspeicher-Trigger am häufigsten ausgeführt werden.

Alle Drop-Daten, die im Säulendiagramm angezeigt werden, weisen darauf hin, dass es zu Drops von Datenspeicher-Trigger kommt und dass Trigger-Warteschlangen gesichert werden .

Das System stellt Triggeroperationen in die Warteschlange, wenn ein Trigger-Thread überlastet ist. Wenn die Datenspeicher-Trigger-Warteschlange zu lang wird, beendet das System das Hinzufügen von Trigger-Vorgängen zur Warteschlange und löscht die Trigger. Aktuell ausgeführte Trigger sind davon nicht betroffen.

Die Hauptursache für lange Warteschlangen und nachfolgende Triggerausfälle ist ein Trigger mit langer Laufzeit im Datenspeicher.

Datenspeicherauslöserausnahmen nach Trigger

Ein Listendiagramm, das die Anzahl der unbehandelten Ausnahmen anzeigt, die durch datenspeicherspezifische Trigger im ExtraHop-System verursacht wurden.

Wie diese Informationen Ihnen helfen können

Ausnahmen für Datenspeicher-Trigger sind die Hauptursache für Leistungsprobleme bei Auslöser. Wenn dieses Diagramm darauf hinweist, dass eine Trigger-Ausnahme aufgetreten ist, sollte der Datenspeicher-Trigger sofort korrigiert werden.

Status- und Diagnosetools in den Administrationseinstellungen

Die Administrationseinstellungen sind eine weitere Quelle für Systeminformationen und Diagnosen.

Für weitere Messwerte zum allgemeinen Zustand des ExtraHop-Systems und für Diagnosetools, die [ExtraHop-Unterstützung](#) um Systemfehler zu beheben, schauen Sie sich die [Status und Diagnose](#) Abschnitt der Administrationseinstellungen.