Häufig gestellte Fragen zur Systemintegrität

Veröffentlicht: 2024-09-26

Hier finden Sie einige Antworten auf häufig gestellte Fragen zu System Health.

Wie überprüfe ich einen möglichen Datenverlust?

Die besten Indikatoren für Datenverlust sind verworfene Pakete, TCP-Desynchronisierungen und zu hohe Paket- oder Durchsatzraten.

- Überprüfe die Drop-Rate erfassen Diagramm für Pakete, die an der Netzwerkkartenschnittstelle, dem SPAN oder dem Netzwerk-Tap verloren gegangen sind
- Überprüfe die Desynchronisierungen Diagramm für systemweite Desynchronisierungen, die darauf hinweisen, dass die Synchronisation bei der Verarbeitung einer TCP-Verbindung verloren gegangen ist.
- Überwachen Sie die folgenden Diagramme, um sicherzustellen, dass das ExtraHop-System die Sensorschwellenwerte nicht überschreitet:
  - Durchsatz
  - Paket-Rate

  Eine hohe Paket- oder Durchsatzrate kann dazu führen, dass Pakete an der Span-Quelle oder an einem Span-Aggregator verloren gehen. Beziehen Sie sich auf die Datenblatt für ExtraHop-Sensoren um mehr über Sensorraten und Grenzwerte zu erfahren.

Wie überwache ich den Ressourcenverbrauch?

Das Gerät entdecken weist Speicherressourcen zum Erfassen von Paketen, Ausführen von Triggern, Übertragen von Daten an Remoteserver und Aufzeichnen im Datenspeicher zu.

In den folgenden Tabellen finden Sie die Speichermenge, die Gerät entdecken widmet sich jedem Ressourcenbereich über einen bestimmten Zeitraum:

- Erfassung und Datenspeicher-Heap-Zuweisung
- Trigger- und Remote-Heap-Zuweisung
- Laden des Datenspeicher-Triggers

Wie überprüfe ich die Leistung meiner RPCAP-Bereitstellungen?

Nach der ersten Einrichtung einer RPCAP-Bereitstellung (RPCAP) sollten Sie sicherstellen, dass Ihre Bereitstellung wie erwartet funktioniert.

- Überprüfe die Weitergeleitet von Peer Diagramm, um sicherzustellen , dass das Volumen der an das ExtraHop-System gesendeten Pakete den für Ihre RPCAP-Peer-Geräte angegebenen Filterregeln entspricht.

- Überwachen Sie die Vom ExtraHop-System empfangen Diagramm, um sicherzustellen, dass ExtraHop-Systeme effizient Pakete von RPCAP-Peers empfangen.

Laufen meine Trigger richtig?

Um das Beste aus Ihren Triggern herauszuholen, stellen Sie sicher, dass neue und geänderte Trigger genaue Daten liefern, ohne die Systemleistung zu beeinträchtigen.

- Sehen Sie sich das an Trigger wird ausgeführt und gelöscht Diagramm, um sicherzustellen, dass das Ausmaß der Triggeraktivität Ihren Erwartungen entspricht. Halten Sie Ausschau nach Ausbrüchen von Triggeraktivitäten, die auf ein ineffizientes Verhalten eines oder mehrerer Auslöser hinweisen könnten. Mit diesem Diagramm können Sie auch die Anzahl der Trigger verfolgen, die aus der Trigger-Warteschlange entfernt wurden . Das ExtraHop-System löst möglicherweise einen lang andauernden Auslöser, der den Ressourcenverbrauch dominiert.
- Sehen Sie sich das an Trigger wird von Trigger ausgeführt Diagramm, nachdem Sie einen neuen Auslöser erstellt oder einen vorhandenen geändert haben, um sicherzustellen, dass der Auslöser ausgeführt wird. Jeder Auslöser, der überdurchschnittlich viele Ressourcen verbraucht, hat möglicherweise ein schlecht optimiertes Skript, das die Leistung beeinträchtigt.
- Überprüfe die Ausnahmen nach Trigger auslösen Diagramm zur Anzeige aller unbehandelten Trigger-Ausnahmen. Ausnahmen tragen maßgeblich zu Problemen mit der Systemleistung bei und sollten sofort behoben werden.

Anhand der folgenden Diagramme können Sie überwachen, ob Ihre Datenspeicher-Trigger, auch als Bridge-Trigger bezeichnet, ordnungsgemäß ausgeführt werden:

- Der Datenspeicher-Trigger wird ausgeführt und gelöscht
- Datenspeicherauslöserausnahmen nach Trigger

Wie wirken sich Trigger auf mein ExtraHop-System aus?

Neben der Überwachung, wie gut Ihre Trigger laufen, enthält die Seite Systemzustand Diagramme, mit denen Sie die Auswirkungen laufender Trigger auf Ihr ExtraHop-System überwachen und beurteilen können.

- Sehen Sie sich das an Last auslösen Diagramm zur Anzeige mehrerer Messungen des Ressourcenverbrauchs durch alle laufenden Trigger. Achten Sie auf Verbrauchsspitzen, die darauf hinweisen können, dass ein neuer Auslöser eingeführt wurde oder dass ein vorhandener Auslöser Probleme hat.
- Überprüfe die Laden nach Trigger auslösen Diagramm, um die Anzahl der Zyklen anzuzeigen, die von jedem laufenden Auslöser verbraucht wurden. Ein Auslöser, der selten ausgeführt wird, aber mehr Zyklen als der Durchschnitt benötigt, kann dazu führen, dass andere Trigger aus der Warteschlange entfernt werden.
- Überprüfe die Zyklen nach Thread auslösen Diagramm, um die Anzahl der Zyklen anzuzeigen, die jeder Thread Triggeroperationen zugewiesen hat. Achten Sie auf einen gleichmäßigen Verbrauch zwischen mehreren Threads. Triggerverluste können auftreten, wenn der Verbrauch eines Threads erheblich höher ist als bei den anderen.

Sie können die Auswirkungen von Datenspeicher-Triggern, auch als Bridge-Trigger bezeichnet, die auf Ihrem ExtraHop-System ausgeführt werden, anhand der folgenden Diagramme überwachen:

- Laden des Datenspeicher-Triggers
- Der Datenspeicher-Trigger wird ausgeführt und gelöscht

Wie schneiden meine offenen Datenströme ab?

Sie können Diagramme überwachen, die sich auf den Zustand und die Leistung von ODS-Übertragungen (Open Data Stream) an ein Syslog, eine Datenbank oder einen Server eines Drittanbieters beziehen.

- Klicken Sie auf Gesendete Nachrichten Diagramm zur Anzeige der Gesamtzahl der von allen aktiven Datenströmen übertragenen Nachrichten und der Anzahl der Fehler, die bei diesen Übertragungen

aufgetreten sind. Überwachen Sie dieses Diagramm, um sicherzustellen, dass Nachrichten wie erwartet übertragen werden. Wenn keine Byte gesendet werden, liegt möglicherweise ein Problem mit der Konfiguration eines offenen Datenstroms oder eines ODS-Triggers vor.

- Klicken Sie auf Nachrichtendurchsatz Diagramm, um die Gesamtzahl der von allen aktiven Datenströmen übertragenen Byte anzuzeigen. Überwachen Sie dieses Diagramm, um sicherzustellen , dass Byte wie erwartet übertragen werden. Wenn keine Byte gesendet werden, liegt möglicherweise ein Problem mit der Konfiguration eines offenen Datenstroms oder eines ODS-Triggers vor.
- Überprüfe die Verbindungen Ein Diagramm, das auf einen Blick die Versuche, eine Verbindung zu ODS-Zielen herzustellen, und die während der Versuche aufgetretenen Fehler zeigt.
- Überwachen Sie die Nach Remotetyp verworfene Nachrichten Diagramm , um die Rate anzuzeigen, mit der Nachrichten gelöscht werden, bevor sie ein Recordstore- oder ODS-Ziel erreichen. Eine hohe Anzahl von Drops kann darauf hinweisen, dass der Nachrichtendurchsatz zu hoch ist, um vom ExtraHop-System oder dem Zielserver verarbeitet zu werden.
- Überwachen Sie die Länge der Exremote-Nachrichtenwarteschlange und Länge der Nachrichtenwarteschlange erfassen Diagramme zur Anzeige der Anzahl der Nachrichten, die in den Warteschlangen ExtraHop Remote (exremote) und Capture (excap) warten. Eine hohe Anzahl von Nachrichten in diesen Warteschlangen kann darauf hinweisen, dass der Nachrichtendurchsatz zu hoch ist, um vom ExtraHop-System oder vom Zielserver verarbeitet zu werden.

Wie hoch ist die geschätzte Lookback-Kapazität?

Lookback bezieht sich darauf, wie weit Sie derzeit historische Daten nachschlagen können. Beispielsweise können Sie Daten in Intervallen von einer Stunde bis zu 9 Tagen nachschlagen.

- Überwachen Sie die Lookback-Schätzungen für metrische Daten Diagramm zur Bestimmung der aktuellen geschätzten Lookback-Kapazität Ihres Gerät entdecken. Das Diagramm zeigt Lookback-Metriken für Zeitintervalle von 1 Stunde, 5 Minuten und 30 Sekunden auf der Grundlage der Schreibdurchsatzrate an.

Wie viele Geräte überwacht das ExtraHop-System?

Auf der Seite Systemzustand finden Sie Diagramme, anhand derer Sie ermitteln können, wie viele L2-, Gateway-, benutzerdefinierte und L3-Geräte von Ihrem ExtraHop-System überwacht werden.

- Überprüfe die Aktive Geräte Diagramm, um sicherzustellen, dass die Gesamtzahl der überwachten aktiven Geräte den Erwartungen entspricht.

Entschlüsseln meine TLS-Zertifikate wie erwartet?

Sie können auf eine Liste aller Zertifikate zugreifen, die auf dem ExtraHop-System eine Entschlüsselung durchführen, indem Sie auf **Bescheinigungen** oben auf der Seite „Systemstatus“.

- Überprüfe die Angaben zum Zertifikat Tabelle, um sicherzustellen, dass die richtigen TLS-Zertifikate auf dem ExtraHop-System installiert sind, und um die Verschlüsselungsmetriken für jedes Zertifikat anzuzeigen. Mithilfe von Verschlüsselungsmetriken können Sie feststellen, ob Ihre Zertifikate erwartungsgemäß entschlüsselt werden. Sie können beispielsweise die Anzahl der erfolgreich verschlüsselten Sitzungen oder die Anzahl der Sitzungen überprüfen, die aufgrund von Hardwarefehlern nicht entschlüsselt wurden.

Wie füge ich Systemintegritätsmetriken zu einem Dashboard hinzu?

Sie können ein neues, benutzerdefiniertes Dashboard mit Systemmetriken erstellen oder einem vorhandenen Dashboard ein einzelnes Systemstatusdiagramm hinzufügen. Suchen Sie das gewünschte Diagramm im Systemstatus-Dashboard, klicken Sie auf den Titel und wählen Sie dann **Kopieren nach...**. Wählen **Neues Dashboard** oder wählen Sie ein vorhandenes Dashboard aus.

Hinweis Wenn Sie mit dem Erstellen und Bearbeiten von Dashboards nicht vertraut sind, lesen Sie unsere Exemplarische Vorgehensweise für das Dashboard.

Welche anderen Tools können mir bei der Bewertung des Systemzustands helfen?

Der Abschnitt Status und Diagnose der Administrationseinstellungen enthält Kennzahlen über den allgemeinen Zustand des ExtraHop-Systems sowie Diagnosetools, die Folgendes ermöglichen: ExtraHop-Unterstützung um Systemfehler zu beheben.

- Prüfen Gesundheitsstatistiken um Kennzahlen anzuzeigen, die die Betriebseffizienz des ExtraHop-Systems angeben.
- Überprüfe die Audit-Log um Ereignisprotokollierungsdaten anzuzeigen und Syslog-Einstellungen zu ändern.
- Erfahre mehr über Ausnahmedateien und wie man sie im ExtraHop-System aktiviert oder deaktiviert.
- Erfahre mehr über Unterstützungsskripte und wie man sie hochlädt und auf dem ExtraHop-System ausführt.

Sie können sich auch die folgenden Ressourcen ansehen, um mehr über den Systemstatus zu erfahren:

- Exemplarische Vorgehensweise zur Systemintegrität: Bewertung der Triggerleistung