Häufig gestellte Fragen zur Systemgesundheit

Veröffentlicht: 2023-09-13

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

Wie überprüfe ich, ob ein Datenverlust möglich ist?

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

- Prüfen Sie die Drop-Rate erfassen Diagramm für Pakete, die an der Netzwerkkartenschnittstelle, dem SPAN oder dem Netzwerk-Tap verworfen wurden
- Prüfen Sie 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 verworfen werden. Beziehen Sie sich auf die Datenblatt für ExtraHop-Sensoren um mehr über Sensorraten und -grenzen zu erfahren.

Wie überwache ich den Ressourcenverbrauch?

Die Gerät entdecken weist Speicherressourcen für die Erfassung von Paketen, die Ausführung von Triggern, die Übertragung von Daten an Remoteserver und die Aufzeichnung im Datenspeicher zu.

In den folgenden Tabellen finden Sie die Speichermenge, die der Gerät entdecken widmet 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 Remote Packet Capture (RPCAP) -Bereitstellung sollten Sie sicherstellen, dass Ihre Bereitstellung wie erwartet funktioniert.

- Prüfen Sie 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 Pakete von RPCAP-Peers effizient empfangen.

Laufen meine Trigger richtig?

Um das Beste aus Ihren Triggern herauszuholen, stellen Sie sicher, dass neue und geänderte Trigger genaue Daten erzeugen, 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. Suchen Sie 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 gelöscht wurden. Das ExtraHop-System könnte einen Trigger mit langer Laufzeit auslöschen, 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 mehr Ressourcen als der Durchschnitt verbraucht, hat möglicherweise ein schlecht optimiertes Skript, das die Leistung beeinträchtigt.
- Prüfen Sie die Ausnahmen nach Trigger auslösen Diagramm zur Anzeige aller unbehandelten Trigger-Ausnahmen. Ausnahmen tragen wesentlich zu Problemen mit der Systemleistung bei und sollten sofort behoben werden.

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

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

Wie wirken sich Trigger auf mein ExtraHop-System aus?

Auf der Seite Systemstatus können Sie nicht nur überwachen, wie gut Ihre Trigger funktionieren, sondern auch Diagramme anzeigen, mit denen Sie die Auswirkungen laufender Trigger auf Ihr ExtraHop-System überwachen und bewerten können.

- Sehen Sie sich das an Last auslösen Diagramm zur Anzeige mehrerer Messungen des Ressourcenverbrauchs aller laufenden Trigger. Achten Sie auf Verbrauchsspitzen, die darauf hindeuten können, dass ein neuer Auslöser eingeführt wurde oder dass bei einem vorhandenen Auslöser Probleme auftreten.
- Prüfen Sie die Laden nach Trigger auslösen Diagramm, um die Anzahl der Zyklen anzuzeigen, die von jedem laufenden Auslöser verbraucht werden. Ein Auslöser, der selten ausgeführt wird, aber mehr Zyklen als der Durchschnitt verbraucht, kann dazu führen, dass andere Trigger aus der Warteschlange gelöscht werden.
- Prüfen Sie die Zyklen nach Thread auslösen Diagramm, um die Anzahl der Zyklen anzuzeigen, die jedem Thread zugewiesen wurden, um Operationen Auslöser. Achten Sie bei mehreren Threads auf einen gleichmäßigen Verbrauch. Triggerverluste können auftreten, wenn der Verbrauch eines Threads erheblich höher ist als der der anderen.

Sie können die Auswirkungen von Datenspeicher-Triggern, auch Bridge-Trigger genannt, 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 Open Data Stream (ODS) -Übertragungen an ein Syslog, eine Datenbank oder einen Server eines Drittanbieters beziehen.

- Klicken Sie auf Gesendete Nachrichten Diagramm zur Anzeige der Gesamtzahl der Nachrichten, die von allen aktiven Datenströmen übertragen wurden, und der Anzahl der Fehler, die während

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

- Klicken Sie auf Nachrichtendurchsatz Diagramm zur Anzeige der Gesamtzahl der Byte, die von allen aktiven Datenströmen übertragen wurden. Überwachen Sie dieses Diagramm, um sicherzustellen , dass die Byte wie erwartet übertragen werden. Wenn keine Bytes gesendet werden, liegt möglicherweise ein Problem mit der Konfiguration eines offenen Datenstroms oder eines ODS-Triggers vor.
- Prüfen Sie die Verbindungen Diagramm für eine Übersicht der Versuche, eine Verbindung zu ODS-Zielen herzustellen, und der Fehler, die während der Versuche aufgetreten sind.
- Überwachen Sie die Nach Remotetyp verworfene Nachrichten Diagramm , um die Geschwindigkeit anzuzeigen, mit der Nachrichten gelöscht werden, bevor sie einen Recordstore oder ein 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 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 hindeuten, dass der Nachrichtendurchsatz zu hoch ist, um vom ExtraHop-System oder dem 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 1 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, basierend auf der Schreibdurchsatzrate.

Wie viele Geräte überwacht das ExtraHop-System?

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

- Prüfen Sie die Aktive Geräte Diagramm, um sicherzustellen, dass die Gesamtzahl der überwachten aktiven Geräte den Erwartungen entspricht.
- Prüfen Sie die Geräte insgesamt Diagramm, um sicherzustellen, dass die Gesamtzahl aller vom ExtraHop-System erkannten Geräte, unabhängig davon, ob sie aktiv oder inaktiv sind, den Erwartungen entspricht.

Werden meine SSL-Zertifikate wie erwartet entschlüsselt?

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

- Prüfen Sie die Einzelheiten zum Zertifikat Tabelle, um sicherzustellen, dass die richtigen SSL-Zertifikate auf dem ExtraHop-System installiert sind, und um 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 einem Dashboard Kennzahlen zur Systemintegrität hinzu?

Sie können ein neues, benutzerdefiniertes Dashboard mit Systemmetriken erstellen oder einem vorhandenen Dashboard ein einzelnes Systemstatusdiagramm hinzufügen. Suchen Sie das gewünschte

Diagramm im Systemintegritäts-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 der Systemintegrität helfen?

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

- Prüfen Gesundheitsstatistik um Kennzahlen einzusehen, die die Betriebseffizienz des ExtraHop-Systems angeben.
- Prüfen Sie die Audit-Log um Daten zur Ereignisprotokollierung anzuzeigen und die Syslog-Einstellungen zu ändern.
- Erfahre mehr über Ausnahmedateien und wie man sie auf dem 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: Beurteilen Sie die Leistung von Auslöser
- ExtraHealth-Paket