Häufig gestellte Fragen zu Analyseprioritäten

Veröffentlicht: 2024-02-16

Hier finden Sie Antworten auf häufig gestellte Fragen zu Analyseprioritäten.

Wie wird die Gerätekapazität für Analysestufen bestimmt?

Die Anzahl der Geräte, die höhere Analysestufen erhalten, hängt von Ihrem ExtraHop-Abonnement und Ihrer Lizenz ab.

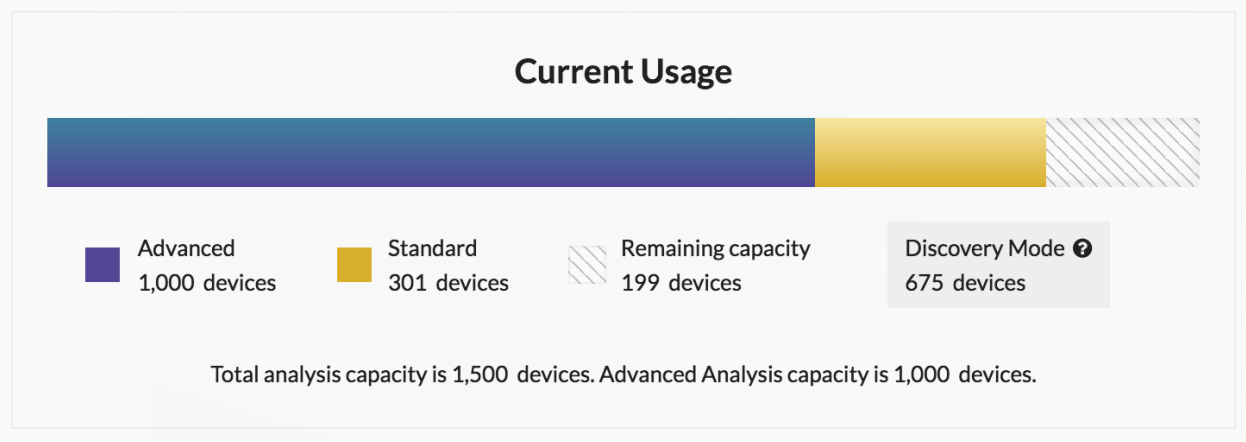
- Ihr Abonnement bestimmt die gesamte Analysekapazität, d. h. die Anzahl der Geräte, die Standard Analysis oder Erweiterte Analyse Analysis empfangen können.
- Ihre Lizenz bestimmt, wie viel von dieser Gesamtkapazität für Advanced Analysis, die höchste Analysestufe, verfügbar ist.

Beispielsweise beträgt die gesamte Analysekapazität für einen EDA 9200 50.000 gleichzeitig aktive Geräte. Bis zu 8.000 dieser aktiven Geräte können sich in Erweiterte Analyse. Weitere Informationen zur Analysekapazität für jedes ExtraHop-Abonnement erhalten Sie von Ihrem ExtraHop-Ansprechpartner.

Wo finde ich meine aktuelle Nutzung?

Auf der Seite Analyseprioritäten wird ein Diagramm angezeigt, das auf einen Blick die Bewertung der Anzahl der analysierten Geräte auf jeder Ebene im Vergleich zur verbleibenden Analysekapazität zeigt. Klicken Sie auf das Symbol Systemeinstellungen und dann klicken **Prioritäten der Analyse**.

Die lizenzierten Gesamtkapazitäten werden unter dem Diagramm angezeigt. Geräte im Entdeckungsmodus werden nicht auf Ihre Gesamtkapazität angerechnet.



Woher weiß ich, welche Geräte auf der Beobachtungsliste stehen?

Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`, klicken Sie auf Systemeinstellungen ⚙ Symbol und dann klicken **Prioritäten der Analyse**. Klicken Sie oben auf der Seite auf **Sehen Sie sich die Beobachtungsliste an**.

Wie füge ich mehrere Geräte zur Beobachtungsliste?

Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`. Klicken Sie oben auf der Seite auf **Vermögenswerte** und dann klicken **Geräte** im linken Bereich. Suchen Sie auf der Gerätelistenseite nach Geräten und klicken Sie dann auf das Kontrollkästchen neben jedem Gerät, das Sie der Beobachtungsliste hinzufügen möchten. Dann klicken Sie **Zur Watchlist hinzufügen** in der oberen rechten Ecke der Seite.

Weitere Informationen finden Sie unter Ein Gerät zur Beobachtungsliste hinzufügen.

Welchen Analysegrad erhalten benutzerdefinierte Geräte?

Maßgeschneiderte Geräte kann jede Analyseebene erhalten. Du kannst eine Gerätegruppe erstellen mit all Ihren benutzerdefinierten Geräten und priorisieren Sie diese Gruppe für Advanced oder Standard Analysis. Oder du kannst ein individuelles benutzerdefiniertes Gerät zur Beobachtungsliste hinzufügen.

Welche Analyseebene unterstützt benutzerdefinierte Metriken?

Benutzerdefinierte Metriken sind nur in Erweiterte Analyse verfügbar. Wenn Sie benutzerdefinierte Messwerte für ein bestimmtes Gerät sehen möchten, priorisieren Sie eine Gruppe, die das Gerät enthält, oder fügen Sie das Gerät zur Beobachtungsliste hinzu.

Welche Analyseebene unterstützt Trigger?

EIN Auslöser wird für jedes Gerät ausgeführt, dem es zugewiesen ist, unabhängig von der Analyseebene. Die Analyseebene eines Gerät hat keinen Einfluss darauf , wann der Auslöser ausgeführt wird. Wenn jedoch ein Auslöser, der einem Gerät zugewiesen ist, benutzerdefinierte Messwerte erfasst, müssen Sie das Gerät für Erweiterte Analyse priorisieren, bevor Sie die benutzerdefinierten Metrikdaten anzeigen können.

Wie ermittle ich die Analysestufe für ein Gerät?

Finde ein Gerät und klicken Sie dann auf den Gerätenamen, um das zu öffnen Seite „Geräteübersicht“. Die Analyseebene wird im Bereich Geräteeigenschaften angezeigt.

Klicken Sie in einer Geräteliste auf die Spalte Analyseebene, um Geräte nach Ebene zu sortieren.

Extrahieren Sie die Geräteliste über die REST-API und fügen Sie eine Option hinzu, um nach Analyseebene zu filtern. Für die Ausführung von Befehlen über die REST-API sind volle Schreibberechtigungen erforderlich.

Was passiert, wenn ein priorisiertes Gerät inaktiv wird?

Ein Gerät kann mit der Zeit inaktiv werden, wenn das Gerät in den letzten 30 Minuten keine Daten gesendet oder empfangen hat.

Ein inaktives Gerät, das auf der Beobachtungsliste steht oder Teil einer Gerätegruppe ist, verbraucht Ihre Advanced- oder Standard Analysis-Kapazität nicht. Wenn das Gerät wieder aktiv wird, erhält es basierend auf der konfigurierten Priorität eine erweiterte Analyse oder eine Standardanalyse.

Wenn ein Gerät für ein bestimmtes Protokoll inaktiv ist und dieses Gerät Teil einer priorisierten Gerätegruppe ist, kann das Gerät bis zu 96 Stunden lang in Advanced oder Standard Analysis verbleiben. Beispielsweise wird eine SSL-Server-Gerätegruppe für Erweiterte Analyse priorisiert. Ein Server, der normalerweise SSL-Anfragen empfängt, ist in dieser Gruppe enthalten. Wenn der Server in den letzten 30 Minuten keine SSL-Daten gesendet oder empfangen hat, aber weiterhin Daten über andere Protokolle

sendet und empfängt, verbleibt der Server in Erweiterte Analyse als Teil der Gerätegruppe SSL-Server. Wenn der Server nach 96 Stunden immer noch über das SSL-Protokoll inaktiv ist, ist der Server kein Mitglied der SSL-Servergruppe mehr und empfängt möglicherweise keine Erweiterte Analyse mehr.