Leitfaden zu den besten Praktiken von Bundles

Veröffentlicht: 2024-09-25

Wenn Sie ein Paket erstellen, das für ExtraHop-Benutzer in anderen Bereichen Ihrer Organisation nützlich sein könnte, können Sie dieses Paket herunterladen und teilen. Vor dem Teilen ist es wichtig, jedes Objekt im Paket zu überprüfen, um sicherzustellen, dass Namen und Beschreibungen informativ und gut geschrieben sind, vertrauliche Informationen entfernt werden und Abhängigkeiten für jedes Objekt enthalten sind. Benutzerdefinierte Metriken, benutzerdefinierte Erkennungen und Anwendungen werden über Trigger erstellt. Dashboards, Benachrichtigungen und Datensatzabfragen basieren häufig auf benutzerdefinierten Metriken und Anwendungen.

Bevor Sie beginnen

- Sie müssen Vollschreiben oder höher haben Privilegien um ein Paket zu erstellen oder hochzuladen.
- Sie müssen mindestens einen persönlichen Schreibstil haben Privilegien um ein Paket herunterzuladen und zu installieren.

Bevor Sie ein Paket hochladen, empfehlen wir Ihnen, die Einstellungen für jedes Ihrer Bundle-Objekte zu überprüfen und die in den folgenden Abschnitten aufgeführten Best-Practice-Richtlinien anzuwenden.

- Warnmeldungen - Entfernen Sie Warnmeldungen, notieren Sie alle Triggerabhängigkeiten und stellen Sie sicher, dass alle Beschreibungsfelder informativ sind.
- Anwendungen - Notieren Sie sich alle Gerätegruppe- und Warnungsabhängigkeiten und stellen Sie sicher, dass alle Beschreibungsfelder informativ sind.
- Armaturenbretter - notieren Sie sich alle Triggerabhängigkeiten und stellen Sie sicher, dass alle Beschreibungsfelder informativ sind.
- Benutzerdefinierte Erkennungen - notieren Sie sich alle Triggerabhängigkeiten.
- Dynamische Gerätegruppen - Entfernen Sie alle Kriterien, die in anderen Umgebungen möglicherweise nicht relevant sind, aus dynamischen Gerätegruppen und stellen Sie sicher, dass alle Beschreibungsfelder informativ sind.
- Abfragen aufzeichnen - notieren Sie sich alle Abhängigkeiten vom Datensatzformat und stellen Sie sicher, dass alle Beschreibungsfelder informativ sind.
- Formate aufzeichnen - notieren Sie sich alle Triggerabhängigkeiten und stellen Sie sicher, dass alle Beschreibungsfelder informativ sind.
- Trigger - stellen Sie sicher, dass alle triggerabhängigen Objekte definiert sind und die Kommentare informativ sind.

Einbeziehen von Warnmeldungen in Bundles (NPM-Modulzugriff erforderlich)

Benachrichtigungen werden häufig mit umgebungsspezifischen Einstellungen konfiguriert. Beispielsweise kann eine Alarm so konfiguriert werden, dass Benachrichtigungen an die E-Mail-Adressen Ihres Unternehmens gesendet werden. Diese Konfigurationen müssen aus den Benachrichtigungen entfernt werden, bevor die Alarm in ein Paket aufgenommen werden kann.

Überprüfen Sie die folgenden Warnungseinstellungen, bevor Sie eine Alarm in ein Paket aufnehmen. Weitere Informationen zu diesen Einstellungen finden Sie unter Warnmeldungen.

Einstellungen	Hinweise
Name	Geben Sie einen Namen für die Alarm ein, der beschreibend ist und keine vertraulichen Informationen enthält.

Einstellungen	Hinweise
Autor	Geben Sie einen Autor der Alarm ein, der für ein allgemeines Publikum geeignet ist und keine vertraulichen Informationen enthält. Möglicherweise möchten Sie Ihren Firmennamen als Autor eingeben, z. B. ExtraHop.
Metrisch	Wenn die Alarm auf eine benutzerdefinierte Anwendung oder Metrik verweist, muss Ihr Paket auch den Auslöser enthalten, der die benutzerdefinierte Anwendung oder Metrik erstellt.
E-Mail-Benachrichtigungsgruppen	Entferne alle E-Mail-Gruppen aus diesem Feld. Das Hinzufügen von Benachrichtigungsgruppen in Bündeln kann dazu führen, dass E-Mails an die falschen Empfänger gesendet werden.
Zusätzliche E-Mail-Adressen	Entferne alle E-Mail-Adressen aus diesem Feld. Die Aufnahme von E-Mail-Adressen in Bündeln kann dazu führen, dass E-Mails an die falschen Empfänger gesendet werden.
Beschreibung	Geben Sie eine Beschreibung der Alarm ein, die nützliche Informationen enthält, z. B. die Bedingungen, unter denen diese Alarm generiert wurde, und keine vertraulichen Informationen enthält.
Zuweisungen	Deaktivieren Sie das Kontrollkästchen Allen zuweisen. Bundles erfassen keine Zuweisungen zu einzelnen IP-Adressen. Wenn jedoch eine Alarm einem zugewiesen ist Gerätegruppe, die Aufgabe wird im Paket erfasst.

Anwendungen in Paketen einschließen

Anwendungen enthalten mehrere Verweise auf andere Komponenten. Bundles, die eine Anwendung enthalten, müssen auch alle benutzerdefinierten dynamischen Gerätegruppe oder Warnkonfigurationen enthalten, auf die von der Anwendung verwiesen wird.

Wenn Sie einem Paket eine Anwendung hinzufügen, stellen Sie sicher, dass die Anwendung und alle Gerätegruppen und Benachrichtigungen, auf die sie verweist, keine vertraulichen Informationen wie interne IP-Adressen oder Subnetze enthalten. Überprüfen Sie die folgenden Anwendungseinstellungen, bevor Sie eine Anwendung in ein Paket aufnehmen. Weitere Informationen zum Ändern dieser Einstellungen finden Sie unter Erstellen Sie eine Anwendung.

Einstellungen	Hinweise
Name anzeigen	Geben Sie einen Anwendungsnamen ein, der beschreibend ist und keine vertraulichen Informationen enthält.
Anwendungs-ID	Geben Sie eine eindeutige, permanente ID ein, die für ein allgemeines Publikum geeignet ist und keine vertraulichen Informationen enthält. Nachdem die

Einstellungen	Hinweise
	Anwendung gespeichert wurde, kann die ID nicht geändert oder gelöscht werden.
Seite	Wenn Sie eine Anwendung auf einem erstellen Konsole, die ausgewählte Standort ist nicht enthalten, wenn Sie die Anwendung zu einem Paket hinzufügen. Site-IDs sind spezifisch für Ihre Umgebung und werden automatisch entfernt, wenn eine Anwendung in einem Paket exportiert wird.
Quellen	Ihr Paket muss alle dynamischen Gerätegruppen enthalten , auf die Ihre Anwendung verweist. Schließen Sie keine Anwendungen ein, die auf einzelne Geräte verweisen.
Warnmeldungen	Wenn einer Anwendung Benachrichtigungen zugewiesen sind, muss Ihr Paket auch die zugewiesene Alarm enthalten.

Einbeziehen von Dashboards in Bundles (NPM-Modulzugriff erforderlich)

Dashboards sind die einfachste Möglichkeit, Metrikgruppen anzuzeigen. Wenn ein Dashboard in einem Paket jedoch benutzerdefinierte Metriken und Anwendungen enthält, die durch einen Auslöser generiert wurden, müssen Sie diese Trigger in das Paket aufnehmen.

Dashboards können sensible Informationen in ihren Metadaten enthalten. Es ist wichtig, dass Sie diese vertraulichen Informationen entfernen, bevor Sie das Dashboard in ein Paket aufnehmen. Es ist auch eine gute Idee, Ihr Dashboard zu überprüfen, um sicherzustellen, dass jede Komponente gut beschriftet ist.

Überprüfen Sie die folgenden Dashboard-Einstellungen, bevor Sie sie in ein Paket aufnehmen. Weitere Informationen zu diesen Einstellungen finden Sie unter Dashboards.

Einstellungen	Hinweise
Titel des Dashboards	Geben Sie einen beschreibenden Dashboard-Titel ein, der keine vertraulichen Informationen enthält.
Autor des Dashboards	Geben Sie einen Dashboard-Autor ein, der für ein allgemeines Publikum geeignet ist und keine vertraulichen Informationen enthält. Beispielsweise möchten Sie möglicherweise Ihren Firmennamen als Autor eingeben, z. B. ExtraHop.
Beschreibung des Dashboards	Geben Sie eine Dashboard-Beschreibung ein, die nützliche Informationen enthält, z. B. den Zweck des Dashboard, und keine vertraulichen Informationen enthält.
Permalink für das Dashboard	Fügen Sie zufällige Zeichen in den Permalink ein, um sicherzustellen, dass der Permalink nicht bereits auf einem anderen ExtraHop-System angegeben ist. Wenn ein Dashboard aus einem Paket einen Permalink enthält, der bereits im System angegeben ist, wird dem Dashboard aus dem Paket ein neuer Permalink zugewiesen, wenn das Paket angewendet wird, was bedeutet, dass Links zu

Einstellungen	Hinweise
	diesem Dashboard von einem anderen Dashboard aus nicht funktionieren.
Widget-Titel	Geben Sie Widget-Titel ein, die beschreibend sind und keine vertraulichen Informationen enthalten.
Widget-Quellen und Metriken	Wenn Widget-Quellen oder -Metriken benutzerdefinierte Anwendungen oder Metriken enthalten, muss Ihr Paket auch den Auslöser enthalten, der diese benutzerdefinierten Anwendungen oder Metriken erstellt.
Einzelheiten zum Widget	Entfernen Sie alle umgebungsspezifischen Konfigurationen und vertraulichen Informationen aus den Widget-Details. Ein Widget kann beispielsweise so konfiguriert werden, dass nur Ergebnisse angezeigt werden, die sich auf einen bestimmten Hostnamen beziehen.
Textfeld-Widgets	Geben Sie Beschreibungen in Textfeld-Widgets ein, die gut geschrieben und informativ sind.

Inklusive benutzerdefinierter Erkennungen in Paketen

Bundles, die eine benutzerdefinierte Erkennung enthalten, müssen sowohl den Auslöser, der die benutzerdefinierte Erkennung definiert, als auch den benutzerdefinierten Erkennungstyp enthalten. Stellen Sie sicher, dass die ID des benutzerdefinierten Erkennungstyps mit der Erkennungstyp-ID in der CommitDetection-Funktion des Auslöser übereinstimmt.

Überprüfen Sie die folgenden Einstellungen, bevor Sie eine benutzerdefinierte Erkennung in ein Paket aufnehmen. Weitere Informationen zum Ändern dieser Einstellungen finden Sie unter Erstellen Sie eine benutzerdefinierte Erkennung.

Einstellungen	Hinweise
Name anzeigen	Geben Sie einen Anzeigenamen für die benutzerdefinierte Erkennung ein, der beschreibend ist und keine vertraulichen Informationen enthält.
ID des Erkennungstyps	Geben Sie den ID-Wert für den Erkennungstyp ein, auf den in der CommitDetection-Funktion des benutzerdefinierten Erkennungsauslösers verwiesen wird.
Autor	Geben Sie einen Autor ein, der für ein allgemeines Publikum geeignet ist und keine vertraulichen Informationen enthält. Beispielsweise möchten Sie möglicherweise Ihren Firmennamen als Autor eingeben, z. B. ExtraHop.
MITRE Technik	Wählen Sie eine oder mehrere MITRE-Techniken aus, die Sie mit der Erkennung verknüpfen möchten.

Gerätegruppen in Bündeln einbeziehen

Bundles können dynamische Gerätegruppen enthalten, aber keine statischen Gerätegruppen. Statische Gerätegruppen basieren auf statischen IP-Adressen und sind wahrscheinlich nicht für mehrere Umgebungen relevant. Wenn Sie eine dynamische Gerätegruppe in Ihr Paket aufnehmen, stellen Sie sicher, dass die Gerätegruppe keine vertraulichen Informationen wie interne IP-Adressen oder Subnetze enthält.

Hinweis Zuweisungen zu Gerätegruppen werden in einem Paket erfasst. Die Gerätegruppe muss jedoch auch im Paket enthalten sein.

Überprüfen Sie die folgenden Gerätegruppeneinstellungen, bevor Sie eine Gerätegruppe in ein Paket aufnehmen. Weitere Informationen zu diesen Einstellungen finden Sie unter Erstellen Sie eine dynamische Gerätegruppe.

Einstellungen	Hinweise
Name	Geben Sie einen Gruppennamen ein, der beschreibend ist und keine vertraulichen Informationen enthält.
Autor	Geben Sie einen Autor ein, der für ein allgemeines Publikum geeignet ist und keine vertraulichen Informationen enthält. Beispielsweise möchten Sie möglicherweise Ihren Firmennamen als Autor eingeben, z. B. ExtraHop.
Kriterien	Entfernen Sie alle umgebungsspezifischen Konfigurationen. Entfernen Sie beispielsweise Verweise auf interne IP-Adressen oder Subnetze.

Einbeziehen von Datensatzabfragen in Bündeln

Datensatzabfragen sind häufig so konfiguriert, dass sie nach umgebungsspezifischen Ressourcen wie Subnetzen oder Hostnamen suchen. Entfernen Sie diese internen Verweise, bevor Sie eine Datensatzabfrage in einem Paket hochladen. Datensatzabfragen können auch auf Datensatztypen verweisen, die in benutzerdefinierten Datensatzformaten definiert sind. Wenn eine Datensatzabfrage von einem benutzerdefinierten Datensatzformat abhängig ist, muss das benutzerdefinierte Datensatzformat im Paket enthalten sein.

Überprüfen Sie die folgenden Einstellungen, bevor Sie eine Datensatzabfrage in ein Paket aufnehmen. Weitere Informationen zum Ändern dieser Einstellungen finden Sie unter Abfragen aufzeichnen.

Einstellungen	Hinweise
Art des Datensatzes	Wenn der Datensatztyp in einem benutzerdefinierten Datensatzformat definiert ist, muss Ihr Paket auch dieses benutzerdefinierte Datensatzformat enthalten.
Filter	Entfernen Sie alle Verweise auf interne Ressourcen oder vertrauliche Informationen aus den Filtern.
Name	Geben Sie einen beschreibenden Namen ein, der keine vertraulichen Informationen enthält.
Beschreibung	Geben Sie eine Beschreibung der Datensatzabfrage ein, die nützliche Informationen enthält, z. B. welche

Einstellungen	Hinweise
	Informationen in der Abfrage erfasst werden, und keine vertraulichen Informationen enthält.

Einschließlich von Datensatzformaten in Bündeln

Benutzerdefinierte Datensatzformate definieren Datensatztypen, auf die in Abfragen verwiesen werden kann. Wenn Sie eine Datensatzabfrage einschließen, die von einem benutzerdefinierten Datensatzformat abhängig ist, müssen Sie das Datensatzformat in das Paket aufnehmen.

Wenn ein benutzerdefiniertes Datensatzformat auf einen benutzerdefinierten Datensatztyp verweist, müssen Sie das benutzerdefinierte Datensatzformat und den Auslöser, der den benutzerdefinierten Datensatztyp definiert, in das Paket aufnehmen. Datensatzformate können auch vertrauliche Informationen in ihren Metadaten enthalten.

Überprüfen Sie die folgenden Eigenschaften der Schema-on-Read-Einstellungen eines Datensatzformats, bevor Sie das Datensatzformat in ein Paket aufnehmen. Weitere Informationen zum Ändern dieser Einstellungen finden Sie unter Erstellen Sie ein benutzerdefiniertes Datensatzformat.

Eigentum	Hinweise
Beschreibung	Geben Sie eine Beschreibung des Datensatzformat ein, die nützliche Informationen enthält, z. B. welche Informationen das Format anzeigt, und keine vertraulichen Informationen enthält.
Name	Geben Sie einen beschreibenden Namen ein, der keine vertraulichen Informationen enthält.
Anzeigename	Geben Sie einen beschreibenden Anzeigenamen ein, der keine vertraulichen Informationen enthält.
Metatypen	Stellen Sie das Feld meta_types entsprechend ein, um Verwirrung zu vermeiden. Beispielsweise wird ein Zeitstempel nicht wie ein Zeitstempel formatiert, es sei denn, der meta_type ist angegeben.

Trigger in Bündeln einbeziehen

Trigger sind häufig in Bundles enthalten, um benutzerdefinierte Metriken und Anwendungen zu erstellen, die häufig von anderen Bundle-Objekten wie Dashboards und Alerts benötigt werden. Nachdem Sie alle Abhängigkeiten von anderen Bundle-Objekten identifiziert haben, müssen Sie sicherstellen, dass Sie die zugehörigen Trigger zur Unterstützung dieser Objekte einbeziehen.

Auslöser können so konfiguriert werden, dass sie auf umgebungsspezifische Merkmale reagieren oder vertrauliche Informationen in den Kommentaren preisgeben. Bevor Sie einen Auslöser in ein Paket aufnehmen, stellen Sie sicher, dass diese Konfigurationen entfernt wurden.

Überprüfen Sie die folgenden Trigger-Einstellungen, bevor Sie einen Auslöser in ein Paket. Weitere Informationen zu diesen Einstellungen finden Sie unter Trigger.

Einstellungen	Hinweise
Name	Geben Sie einen beschreibenden Namen ein, der keine vertraulichen Informationen enthält.

Einstellungen	Hinweise
Autor	Geben Sie einen Trigger-Autor ein, der für ein allgemeines Publikum geeignet ist und keine vertraulichen Informationen enthält. Beispielsweise möchten Sie möglicherweise Ihren Firmennamen als Autor eingeben, z. B. ExtraHop.
Beschreibung	Geben Sie eine Triggerbeschreibung ein, die nützliche Informationen enthält, z. B. welche Metriken der Auslöser erstellt, und die keine vertraulichen Informationen enthält.
Debug-Log aktivieren	Deaktivieren Sie das Kontrollkästchen Debugging aktivieren. Stellen Sie sicher, dass ein Auslöser debuggt wurde, bevor Sie Auslöser mit anderen teilen.
Trigger-Skript	• Definieren Sie alle Abhängigkeiten von anderen Bundle-Objekten. • Entfernen Sie alle Verweise auf interne Ressourcen wie Hostnamen oder Subnetze und entfernen Sie vertrauliche Informationen aus den Kommentaren. • Erläutern Sie die Funktionalität der einzelnen Abschnitte des Auslöser in den Kommentaren.
Erweiterte Optionen	Wählen Sie den **Allen Geräten zuweisen** Checkbox. Bundles erfassen keine Zuweisungen zu einzelnen IP-Adressen. Wenn jedoch ein Auslöser einem zugewiesen ist Gerätegruppe, die Aufgabe wird im Paket erfasst.