

Seiten-Layouts und Berichte

Anleitung Collax Information and Security Intelligence

Reporting

Aus den Daten, die von einem Collax Logstash Server gesammelt wurden, können Berichte erstellt werden. Berichte können direkt im Browser angezeigt oder als PDF generiert und heruntergeladen werden. Es besteht auch die Möglichkeit, dass die Berichte automatisch per E-Mail verschickt werden. Dabei können aus den vordefinierten Vorlagen für Berichte ausgewählt, oder individuelle Berichte erstellt werden. Seiten-Layouts sind dafür da, um in den Berichten, verschiedene Daten in Diagrammen und Tabellen anzeigen zu können.

Voraussetzungen

Vorraussetzung ist das Collax Information and Security Intelligence Paket.

Installation

Unter Software → Lizenzen und Module → Zusatzmodule „Installieren“ klicken.

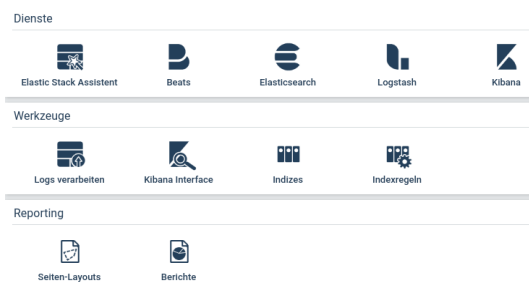
- Collax Information and Security Intelligence
- Benötigt mindestens Collax Version 7.0.32

Hinweis

Berichte werden erst sinnvoll, wenn genügend Daten von einem Client gesammelt wurde. Wenn Berichte im Browser angezeigt werden, ist die Auslastung des lokalen Browsers hoch. Deshalb ist es wichtig, dass der verwendete Computer mindestens 4GB RAM besitzt. Sonst sollten Sie sich die Berichte als PDF herunterladen.

Verwendung

Um Berichte zu erstellen oder zu bearbeiten, öffnen Sie das Berichte Formular unter Menü → ElasticStack → Reporting → Berichte. Es werden die voreingestellten Berichte angezeigt.




Berichte

Bei der Installation werden vorgefertigte Berichte hinzugefügt. Diese können nicht geändert werden. Bei den vorgefertigten Berichten kann der Zeitraum der Berichte gewählt, als PDF generiert oder im Browser angeschaut, sowie automatisch per E-Mail versendet werden. Verwenden Sie die vorgefertigten Berichte für Webproxy, Mail usw.

Bericht erstellen

Im Berichte Formular kann mit einem Klick auf das Drucker-Symbol ein Bericht erzeugt werden. Es öffnet sich die Einstellung für den Bericht. Wählen Sie nun das Papierformat und den Zeitraum für welchen der Bericht erstellt werden soll aus. Relative Zeitangaben beziehen sich immer auf das aktuelle Datum und Uhrzeit. Anschließend klicken Sie auf den Button „Im Browser ansehen“ und der Bericht wird direkt in einem neuen Tab im Browser geöffnet oder „Als PDF herunterladen“ und der Bericht wird als PDF heruntergeladen.

 **Bericht ansehen/drucken**

Bezeichnung	MailFilter
Papierformat	DIN A4
Beginne Seitenzählung bei	1
Zeitraum	Quick
Voreinstellung	Letzten 7 Tage

✕ Schließen ⌵ Im Browser ansehen ☑ Als PDF herunterladen

Hinweis:

Wenn Berichte keine Daten enthalten, kann es sein, dass noch keine Daten vom Beats Clienten auf den Logstash Server übertragen wurde, oder der Zeitraum falsch oder zu klein gewählt wurde und in dieser Zeit noch keine Daten vorhanden sind.

Automatisches Senden von E-Mails

Jeder Bericht kann automatisch per E-Mail an Benutzergruppen, sowie an den Administrator gesendet werden. Achten Sie darauf, dass die ausgewählten Benutzer eine gültige E-Mailadresse eingetragen haben. Die Frequenz kann aus drei verschiedenen Intervallen ausgesucht werden, in denen Berichte automatisch gesendet werden sollen.

Wenn die Frequenz „Täglich“ ausgewählt ist, werden Berichte für den vorherigen ganzen Tag verschickt.

Wenn „Wöchentlich“ ausgewählt ist, werden die Berichte jeden Montag für die ganze vorangegangene Woche verschickt. Der generierte Bericht ist von Montag bis Sonntag der vorherigen Woche.

Wenn „Monatlich“ ausgewählt wird, wird der Bericht am 1. Des Monats verschickt. Der Bericht ist für den vorherigen ganzen Monat.

Alle Berichte werden immer um 1 Uhr nachts verschickt.

Jeder Bericht hat eine eigene Frequenzeinstellung. So kann ein Firewall-Bericht täglich verschickt werden, jedoch ein Proxy-Bericht wöchentlich.

Berichte selbst erstellen

Berichte kopieren

Wenn Sie einen Bericht anpassen wollen kann ein Bericht mit Rechtsklick „Kopie anlegen“ kopiert werden. Dabei bleiben die Einstellungen des ursprünglichen Berichts erhalten. Tragen Sie einen neuen Namen für den Bericht ein und speichern sie diesen. Nun öffnen Sie den neu erstellten Bericht und können mit der Bearbeitung beginnen.

Bericht erstellen

Berichte können selbst erstellt werden. Dafür werden Seiten-Layouts benötigt, die in einem Bericht festlegen, an welcher Stelle die Visualisierungen erstellt werden.

Fügen Sie dem Bericht eine Seite hinzu und wählen für diese Seite ein Layout aus. Diese Layouts können selbst erstellt oder vordefinierte Layouts verwendet werden. Ein Layout ist dazu da, um auf der Seite die gewünschten Visualisierungen anzeigen zu können. Die Visualisierung wird für jede Box ausgewählt. Sie können der Visualisierung noch eine Überschrift geben. Wenn keine Überschrift eingetragen ist, wird der Name der Visualisierung

eingetragen. Erstellen Sie so alle Seiten, die für diesen Bericht angefertigt werden soll und speichern diesen.

Filter

Bei den Berichten können selbst definierte Filter gesetzt werden. Wenn z.B. bei einem Bericht nur ein Host angezeigt werden soll, muss bei jeder Visualisierung des Berichts, der Filter für den Host gesetzt werden.

```
{
  "query": {
    "match": {
      "beat.hostname.keyword": {
        "query": "<hostname>",
        "type": "phrase"
      }
    }
  }
}
```

Dabei muss der Hostname angepasst werden. Dadurch wird die Visualisierung nur für diesen Host angezeigt. Es können mehrere Filter definiert werden. Diese Filter können in Kibana selbst erstellt und in diesem Format angezeigt werden. Die Filter können so einfach erstellt und kopiert werden.

Achtung: Die Filterregel muss für jede ausgewählte Visualisierung eingetragen werden, für die diese Filterregel gelten soll.

Wenn mehrere Filter gesetzt werden sollen, müssen die einzelnen Filter mit einem „,(Komma) getrennt werden und alles in „[]“ eckige Klammern geschrieben werden.

Seiten-Layouts

Mit dem Paket Collax Information and Security Intelligence kommen vordefinierte Seiten-Layouts mit. Diese Layouts werden von den vordefinierten Berichten verwendet.

Reporting Seiten-Layouts			
Bezeichnung	↑	Kommentar	Max. Visualisierungen
1x3		Beispiel-Layout 3 Boxen	3
2x2		Beispiel-Layout 4 Boxen	4
2x4		Beispiel-Layout 8 Boxen	8
Firewall		7 Boxen für Firewall-Bericht	7
IntrusionPrevention		Intrusion-Prevention-Bericht, Seite 1	5
IntrusionPrevention Page 2		Intrusion-Prevention-Bericht, Seite 2	1
Mail		Mail-Bericht, Seite 1	7
Mail Page 2		Mail-Bericht, Seite 2	2
Syslog		Syslog-Bericht, Seite 1	5
Syslog Page 2		1 Box für Syslog-Bericht, Seite 2	1
Title		Deckblatt, 1 Box	1
WebProxy1		4 Boxen für Web-Proxy-Bericht, Seite 1	4
WebProxy2		4 Boxen für Web-Proxy-Bericht, Seite 2	4



Wenn sie mit dem Mauszeiger über ein Layout gehen, erscheint die Anordnung der Boxen auf dem Seiten-Layout.

Seiten-Layouts erstellen

Um einen Bericht selbst erstellen zu können benötigen sie Seiten-Layouts. Seiten-Layouts können selbst erstellt oder die vorgefertigten Layouts kopiert und verändert werden.

Um ein Seiten-Layout zu kopieren, klicken Sie mit der rechten Maustaste auf ein Seiten-Layout und wählen sie „Kopie anlegen“. Tragen Sie für das Layout einen Namen ein und speichern es. Anschließend öffnen Sie das neu erstellte Layout und können mit der Bearbeitung beginnen.

Erstellen Sie ein neues Seiten-Layout und fügen eine Box zum Seiten-Layout hinzu. Dabei kann die Box auf der Seite durch den Abstand zur Oberkante und dem linken Rand der Seite bestimmt werden. Die Größe einer Box wird durch die Breite und die Höhe bestimmt.

Um in der Vorschau die erstellte Box sehen zu können, klicken Sie im Formular in der rechten oberen Ecke auf das Aktualisierungssymbol. Geben Sie bei der Erstellung der Boxen darauf Acht, dass sich die Boxen nicht überlagern oder zu klein für die Visualisierung sind.

Menü • Elastic Stack • Reporting Seiten-Layouts • Seiten-Layout bearbeiten

Seiten-Layout bearbeiten

Bezeichnung: Kopie_8_Boxen
 Kommentar: Beispiel-Layout 8 Boxen
 Vorschau:

Bezeichnung: Top-Left
 Oben: 0% (Abstand zur Oberkante der Seite)
 Links: 0% (Abstand zur linken Kante der Seite)
 Breite: 50%
 Höhe: 25%
 [Löschen]

Bezeichnung: Top-Right
 Oben: 0% (Abstand zur Oberkante der Seite)
 Links: 50% (Abstand zur linken Kante der Seite)

[Schließen] [Speichern] [Box hinzufügen]

Beispiel Bericht Webproxy



Bericht über Web-Proxy

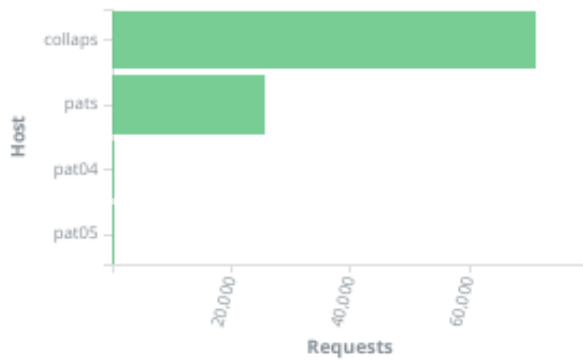
für den Zeitraum

von: 09.10.2018, 11:16

bis: 16.10.2018, 11:16

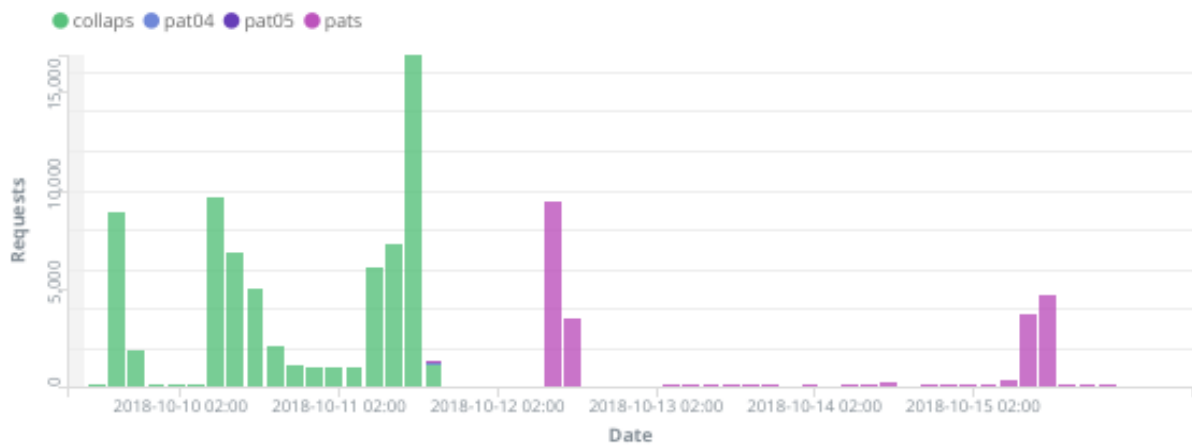
Erstellt am 16.10.2018, 11:16
auf pat05.dev.collax.com

Beteiligte Hosts

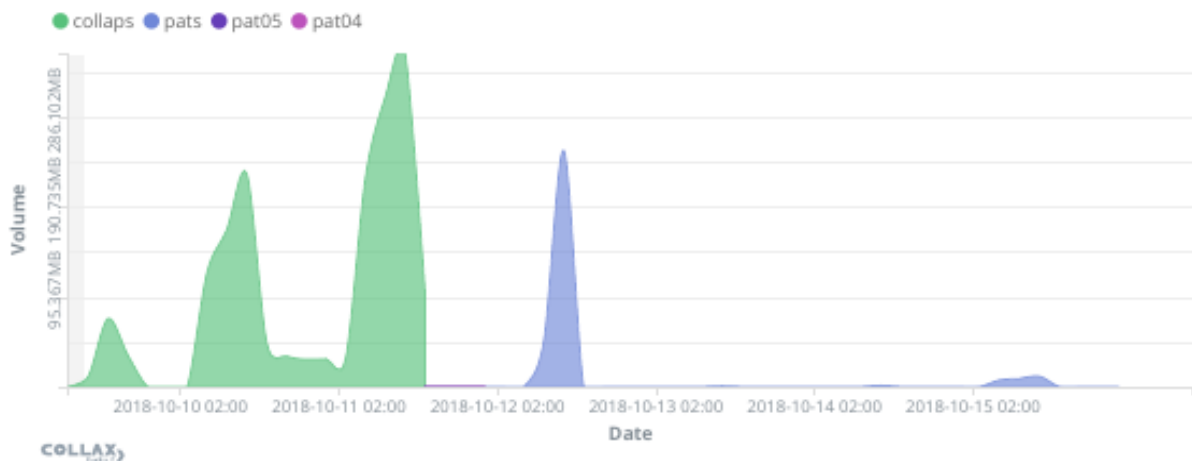


Hosts	Requests	Volume
collaps	71,291	1.746GB
pats	25,691	343.94MB
pat04	139	1.647MB
pat05	139	1.562MB
	97,260	2.085GB

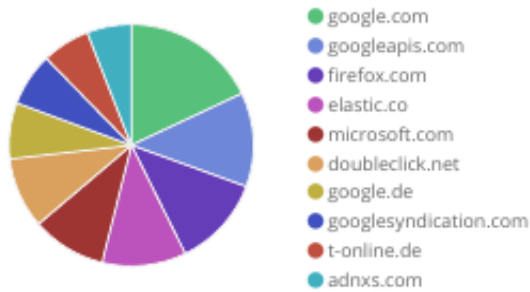
Verlauf: Anfragen



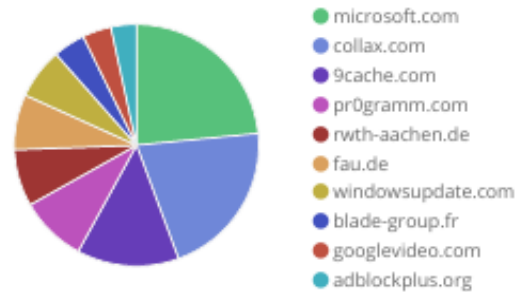
Verlauf: Volumen



Anfragen pro Domain



Volumen pro Domain



Domain-Übersicht

http: Domain Overview

Domain	Requests	Volume
microsoft.com	2,384	192.978MB
collax.com	9	6.486KB
rwth-aachen.de	15	939.342KB
	2,408	193.902MB

https: Domain Overview

Domain	Requests	Volume
collax.com	963	165.908MB
9cache.com	193	0B
pr0gramm.com	46	0B
rwth-aachen.de	4	0B
fau.de	7	0B
	1,213	165.908MB

Antworten aus Cache

