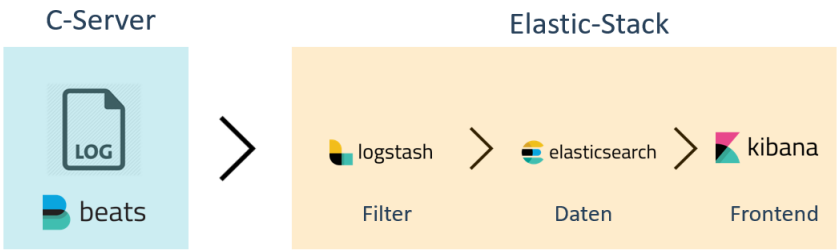
Kibana

Collax Information and Security Intelligence

Kibana

Kibana stellt die Weboberfläche für die Visualisierung der gesammelten Daten bereit. Auf der Weboberfläche von Kibana können verschiedene Visualisierungen ausgewählt werden und die Daten somit übersichtlich angezeigt werden. Für die Ersteinrichtung verwenden Sie die Anleitung „Collax CISI Einrichtung“.



Voraussetzungen

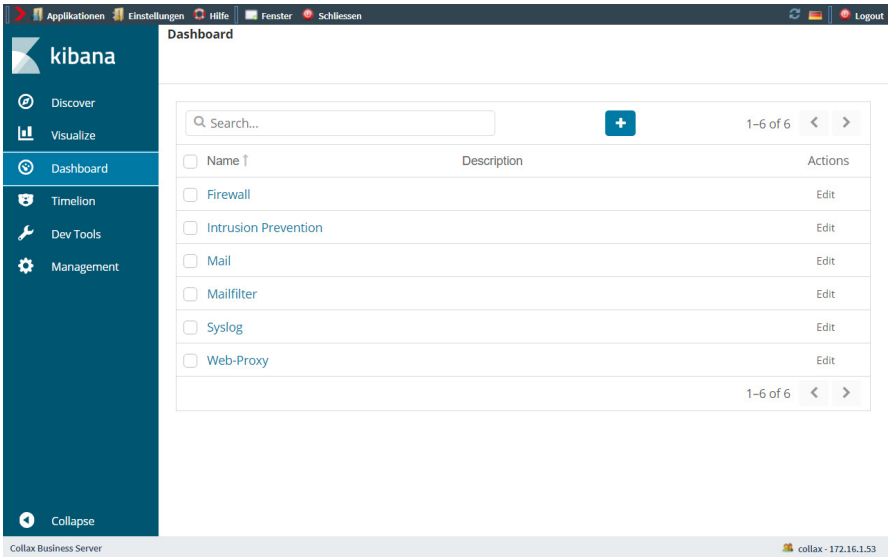
Für Kibana, wird das Paket „Collax Information and Security Intelligence“ benötigt. Um Kibana verwenden zu können muss es aktiviert sein. Zusätzlich muss ein Benutzer für den Zugriff auf Kibana eingerichtet sein.

Anmeldung

Öffnen Sie den Webaccess des Servers. Loggen Sie sich mit dem Benutzer, der die Rechte für Kibana hat ein. Klicken Sie anschließend auf Kibana. Die Weboberfläche für die Visualisierung öffnet sich.

Dashboard

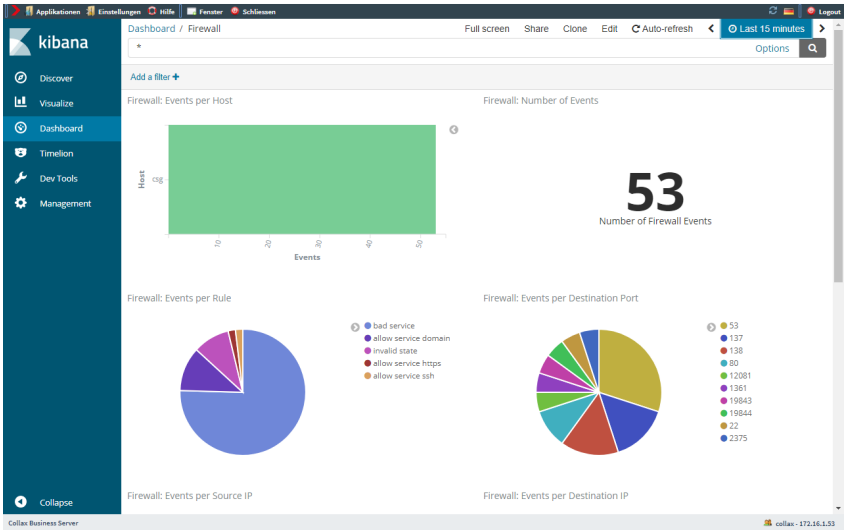
Um sich die Daten, die von den Beats-Clienten auf dem Server gesammelt wurden, wie Firewall, Mail usw. anzeigen zu lassen, klicken Sie im linken Menü auf „Dashboard“. Es erscheint eine Auswahl an verschiedenen Dashboards für verschiedene Bereiche, wie Syslog, Mail oder Firewall. Für diese Dashboards sind passende Visualisierungen voreingestellt. Es können auch selbst definierte Visualisierungen angelegt werden. Mit einem Klick auf ein Element in einer Visualisierung können Filter gesetzt werden. Ein Filter beschränkt alle Visualisierungen des Dashboards auf das ausgewählte Element (Drill-Down).



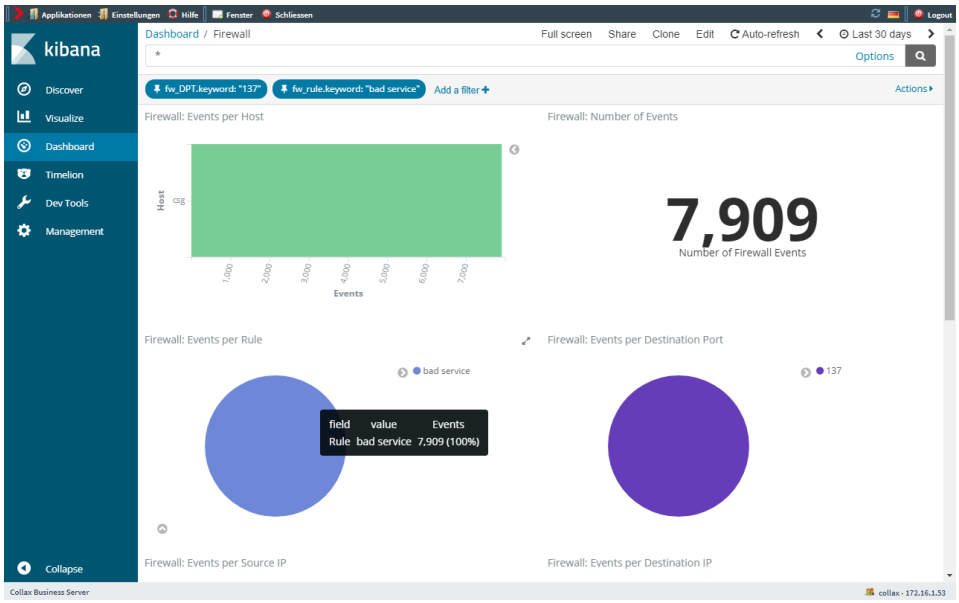
Filterregeln

Wählen Sie den gewünschten Bereich aus. Dadurch wird der Filter für die ausgewählten Logdatein gesetzt und alle Visualisierungen auf die Darstellung dieser Daten beschränkt.

Als Default-Wert werden die Ereignisse der letzten 15 Minuten angezeigt. Wenn Sie dies ändern möchten, klicken Sie im rechten oberen Rand auf das Zeitintervall. Es kann ein anderes Zeitintervall eingestellt werden. Danach werden die Events in diesem Zeitfenster angezeigt.



Es werden alle Events, die z. B. von der Firewall aufgezeichnet wurden, hier dargestellt. Wenn nur ein einzelnes Event dargestellt werden soll, kann mit einem Klick auf das Feld, mit dem gewünschten Dienst im Kreisdiagramm, der Filter verfeinert werden.



Es besteht die Möglichkeit, die Filterregeln anzupinnen. Klicken Sie dazu auf den zuvor gesetzten Filter auf die Pinnnadel. Dies ist hilfreich, wenn in der Übersicht in den Logdateien für diesen Filter angezeigt werden sollen. Klicken Sie nun im linken Reiter auf „Discover“ und wählen Sie dort den gewünschten Logbereich aus. Nun wird das Log, eingeschränkt auf die zuvor gesetzten Filterregeln, angezeigt. Überprüfen Sie die Filter und löschen Sie gegebenenfalls die gesetzten Filter wieder.