Logging, Analyzing, Reporting

Anleitung Collax Information and Security Intelligence

Konzept

Das Modul Collax Log-Analyse und Reporting ist nach dem Client-Server-Prinzip aufgebaut. Die Clients oder Agenten sammeln die Informationen aus den Log-Dateien ein und senden sie an einen zentralen Server. Dieser bereitet die Daten auf, speichert sie und stellt eine Oberfläche zur Auswertung bereit. Als Grundlage für das Modul setzen wir das mächtige Framework Elastic Stack der Firma elastic (www.elastic.co) ein, um es mit wichtigen Funktionen für den praktischen Einsatz zu erweitern.

Voraussetzungen

Auswertungs-Server

Faustregel: Der Platzbedarf ist ungefähr gleich groß, wie die ursprünglichen Daten [1]. Produziert ein Mail-Server pro Tag 1 GB Daten, so würde man für 10 Server über einen Zeitraum von 100 Tagen 1 TB an Daten ansammeln.

Der Datenbestand sollte in den Arbeitsspeicher passen.

Empfehlung: Erweiterbares Storage-Backend

Server mit Agenten

Netzwerk: Überträgt der exemplarische Mail-Server seine Log-Datei von 1 GB im Laufe eines Tages, so belegt er bei großzügiger Rechnung des Protokoll-Overheads (Faktor 2) ungefähr 0,02 % der zur Verfügung stehenden Bandbreite einer 1 GBit/s-Schnittstelle.

Installation

Registrieren Sie die Lizenzen für die beiden Module auf der Administrationsoberfläche im Menü unter Software / Lizenzen und Module im Tab Lizenz-Verwaltung. Gehen Sie anschließend in den Tab Zusatzmodule und klicken zum Installieren auf das Plus-Symbol.

- „Collax Information and Security Intelligence“ für den Auswertungs-Server
- „Beats“ für den Agenten

Konfiguration

Wenn Sie sich nun auf der Administrationsoberfläche einloggen oder einen Reload machen, finden Sie im Menü unter „Status/Wartung“ ein neues Icon „Elastic“. Falls es noch

keinen Benutzer gibt, der sich über die Benutzerseite anmelden kann, legen Sie diesen vorher noch an. Klicken Sie dann bei „Werkzeuge“ auf „ELK Assistent“ und führen die beschriebenen Schritte durch. Bei der Konfiguration des Servers wählen Sie im ersten Schritt als Datenquelle „Lokal und Remote“ aus. Im nächsten Schritt wird zuerst bestimmt welche Log-Zeilen übertragen werden sollen („Versenden“); als zweites welche Einträge für eine Auswertung aufbereitet werden („Verarbeiten“). Nur dann kann beispielsweise die Anzahl von Spam-Mails ermittelt werden. Im dritten Schritt wird die Netzwerkberechtigung gesetzt, aus welchen Netzen ein Agent seine Daten abliefern darf. Im vierten Schritt werden die Zertifikate erzeugt, die für eine sichere Übertragung notwendig sind. Die Voreinstellungen in den nächsten beiden Schritten für den Arbeitsspeicher und das Aufräumen können Sie unverändert lassen. Im letzten Schritt weisen Sie einen Benutzer zu, der über die Benutzerseite Zugriff auf die Visualisierungen erhalten soll.

Hinweis

Beim Start des Agenten „Filebeat“ ist etwas Geduld notwendig. Bis zur ersten Datenübertragung an den ELK-Server können einige Minuten vergehen. Denn Filebeat sammelt zuerst die zu übertragenden Informationen ein, bevor die Datenübermittelung beginnt. Gerade bei großen Log-Dateien kann es recht lange bis zur ersten Übertragung dauern.

Beschreibung Kibana

Kibana stellt viele nützliche Tools bereit. Die wichtigsten und interessantesten stellen wir hier kurz vor. Die Beschreibungen sind knapp gehalten und sollen so zum Ausprobieren animieren. Wer noch tiefer einsteigen will, findet hier weiterführende Informationen: https://www.elastic.co/guide/en/kibana/current/getting-started.html

Loggen Sie sich nun mit dem im Wizard benannten Benutzer auf der Benutzerseite ein und wählen „Kibana“ aus.

Einblick in die Rohdaten

Nach dem Einloggen landet man in der Ansicht „Discover“. Hier werden die einzelnen Log-Einträge – im ELK-Sprech: „Dokumente“ – angezeigt.

Rechts oben kann man den Zeitraum festlegen, aus welchem die Dokumente, also die Log-Einträge, angezeigt werden sollen. Daneben ist die Einstellung für das Intervall, nach welchem die Ansicht mit neuen Dokumenten aktualisiert wird.

Die Anzeige der Dokumente kann entweder über einen Begriff in der Suchleiste oder über einen Filter eingeschränkt werden. Links neben jedem Dokument ist ein Pfeil bzw. Dreieck. Ein Klick darauf, zeigt in welche Bestandteile der Eintrag zerlegt wurde. Neben jedem Bestandteil oder besser Feld sind vier Symbole. Mit den beiden Lupen lässt sich nach den Feldinhalten exklusiv oder inklusiv filtern. Mit der Doppelbox lässt sich steuern, welche Felder angezeigt werden, wenn die Detailansicht eingeklappt ist. Mit dem Stern werden

alle Dokumente ausgefiltert, bei denen dieses Feld leer ist. Kaputtmachen kann man in dieser Ansicht nichts.

Wollen Sie eine Suche und eine Ansicht später wiederverwenden, klicken Sie oben auf „Save“.

Die Übersicht

Wechseln Sie links im Menü auf „Dashboard“. Klicken Sie auf eines der vorgefertigten Dashboards. Wer schon Erfahrung mit Kibana hat, kann auch ein neues anlegen. Es werden nun verschiedene Visualisierungen zum ausgewählten Thema angezeigt. Hier können nun auch wieder Zeiträume und Filter wie in der Ansicht „Discover“ gesetzt werden. Besonders elegant lässt sich ein Drill-Down mit einem Klick auf einen Wert in einer Visualisierung durchführen. Klicken Sie beispielsweise im Syslog-Dashboard auf einen Prozessnamen im Kuchendiagramm, aktualisieren sich alle anderen Visualisierungen und oben wird ein neuer Filter gesetzt. Wenn Sie mit der Maus über den Filter fahren, erscheinen fünf Symbole:

- Checkbox: Ein- und Ausschalten des Filters
- Pin: Der Filter wird auch in der Ansicht „Discover“ gesetzt.
- Lupe: Filter umkehren
- Mülltonne: Filter löschen
- Blatt und Stift: Filter bearbeiten

Wenn Sie das Dashboard verändern wollen, speichern Sie es zuerst unter einem neuen Namen. Damit das bestehende Dashboard nicht gelöscht wird, setzen Sie das Häkchen „Save as a new dashboard“. Nun wechseln Sie mit einem Klick oben auf „Edit“ in den Bearbeitungsmodus. Sie können nun die einzelnen Visualisierungen neu arrangieren, bestehende verändern oder weitere hinzufügen. Wenn Sie eine Visualisierung über das Stift-Symbol verändern oder den Menüpunkt „Add“ neu hinzufügen, werden sie in die Ansicht „Visualize“ geleitet.

Vergessen Sie nicht am Schluss erneut zu sichern.

Wenn Sie rechts neben dem Kibana-Logo auf „Dashboard“ klicken kehren Sie zurück in die Auswahl der Dashboards.

[1] The true story behind Elasticsearch storage requirements:
https://www.elastic.co/blog/elasticsearch-storage-the-true-story