elastic

Der Elastic Observability-Leitfaden für AWS

elastic.co/de →

Inhalt

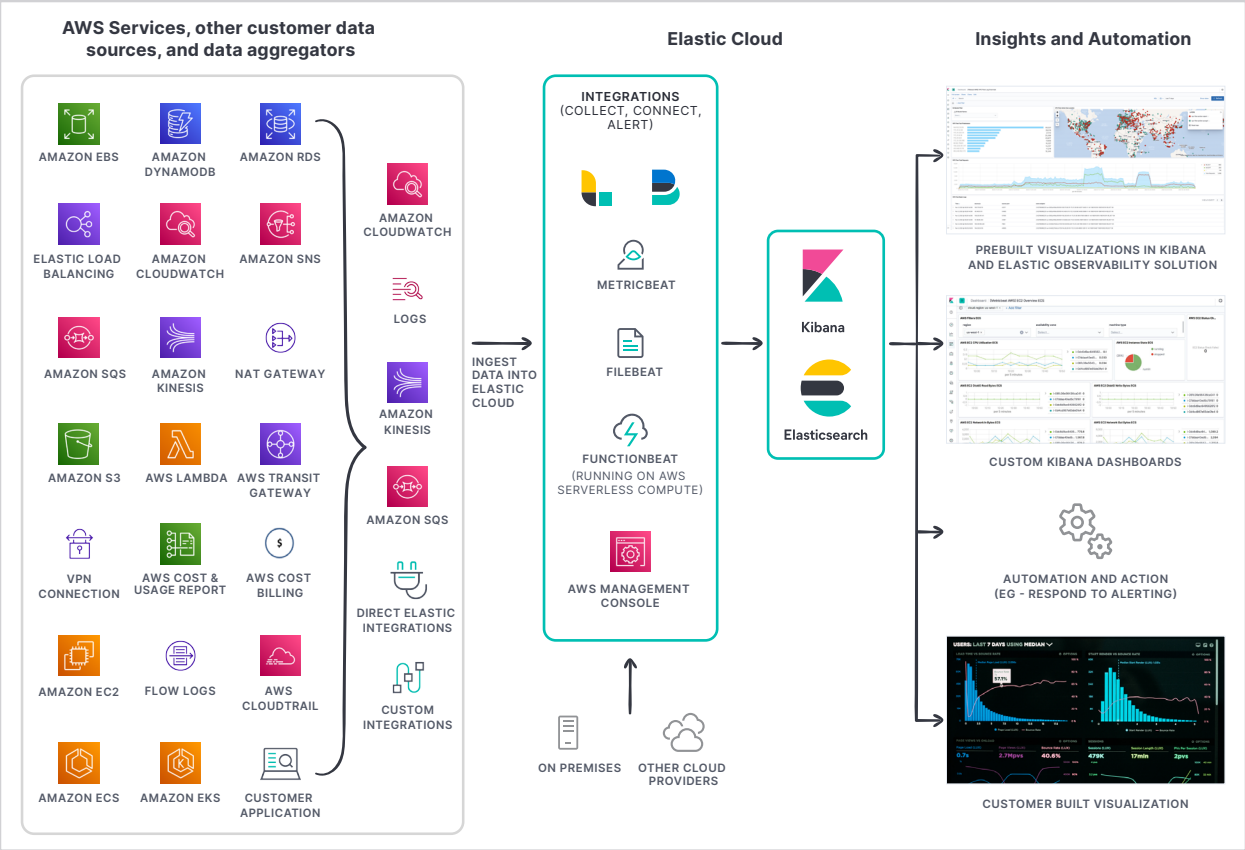
Einführung

Um das Agilitäts- und Flexibilitätspotenzial der Cloud voll auszuschöpfen, ist es wichtig, datenbasierte Erkenntnisse und Aktionen voranzubringen. Mit der Observability-Lösung von Elastic können Sie die Datentransparenz über Ihre gesamte AWS-Umgebung und On-Premises-Umgebungen hinweg zentralisieren und so einen besseren Einblick in die Verfügbarkeit, die Leistung und den Zustand Ihrer Infrastruktur, Ihrer Anwendungen und Ihres Geschäfts erhalten.

AWS stellt eine Reihe von Logdaten (dort „Protokolle“ genannt) und Metriken für seine Cloud-Dienste zur Verfügung, mit denen Sie Ihr Cloud-Deployment überwachen und fundiertere Entscheidungen treffen können. Elastic Observability unterstützt diese Datenquellen über Integrationen, damit sie an einem zentralen Ort zusammengeführt werden können, sodass Sie kontinuierlich Einblicke in Ihre IT, Ihre Abläufe und Ihr Geschäft erhalten und entsprechende Erkenntnisse daraus gewinnen können. Vorkonfigurierte Dashboards und Tools helfen Ihnen bei der Analyse Ihrer Daten und mit individuell eingerichteten Visualisierungen können Sie schnell auf Ihre Geschäftsanforderungen reagieren.

In diesem Leitfaden erfahren Sie, wie Sie Elastic Observability so für die AWS-Dienste konfigurieren können, dass Sie die Dienste effektiver überwachen und schneller auf Ereignisse reagieren können. Sie finden hier zusätzliche Informationen über diese AWS-Dienste und die Vorteile der Nutzung von Elastic für das Monitoring. Außerdem geben wir Ihnen Best Practices an die Hand, die Ihnen dabei helfen, Ihre Investitionen in Elastic und AWS maximal zu nutzen. Es lohnt sich also weiterzulesen.

Mit Elastic können Sie mehr mit Ihren AWS-Daten tun



Überwachen und Analysieren von Amazon CloudWatch Logs mit Elastic

Mit Amazon CloudWatch können Sie Protokolldaten aus Ihrer gesamten Infrastruktur, Ihren Anwendungen und den von Ihnen genutzten AWS-Diensten in einem zentralen, skalierbaren Dienst zusammenführen.

Mit Amazon CloudWatch Logs können schnell und einfach Folgendes tun:

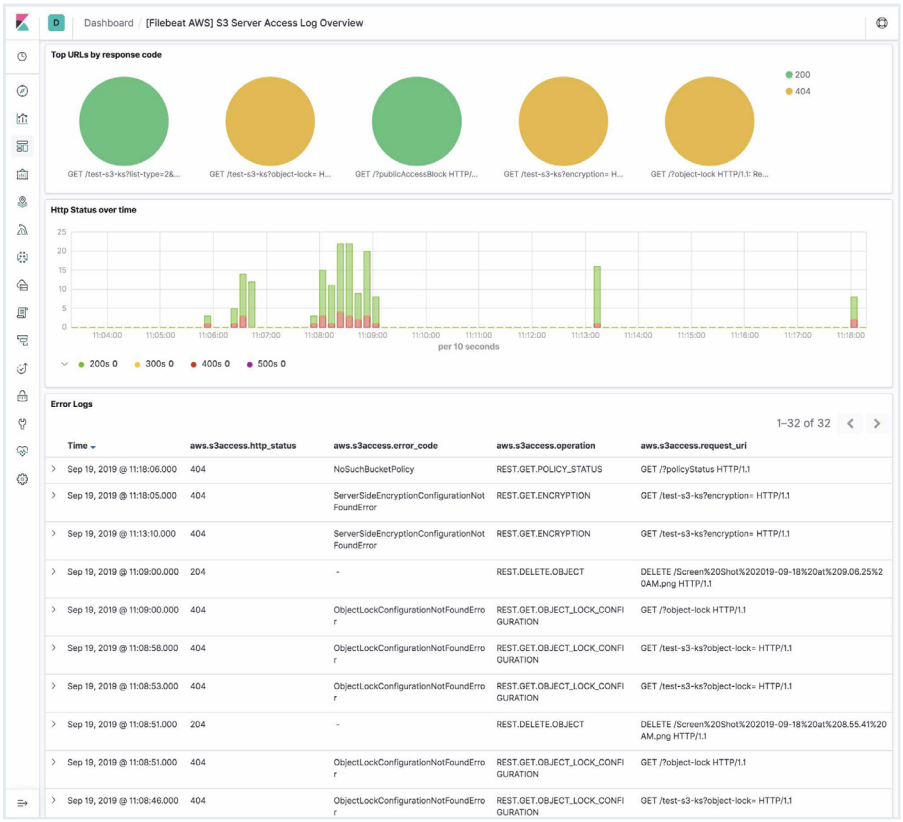
Erfassen, Speichern und Nutzen von Protokolldateien aus unterschiedlichen Quellen

Überwachen des Zustands und der Leistung Ihrer Infrastruktur und Ihrer Anwendungen

Beobachten von Amazon CloudWatch Logs-Protokollen direkt von verschiedenen AWS-Protokollgruppen aus.

elastic

So senden Sie Amazon CloudWatch Logs-Protokolldateien an Elastic:



Zunächst müssen Sie Angaben zu Ihrer AWS-Umgebung und Ihrem Elastic Cloud-Deployment zusammensammeln. Welche Angaben benötigt werden, entnehmen Sie bitte **Anhang A**. Informationen zur Vorgehensweise bei Amazon CloudWatch-Protokollen finden Sie in **Anhang B**. Dort werden die folgenden Themen behandelt:

1. Einrichten eines Amazon Simple Storage Service(Amazon S3)-Buckets und Erstellen einer Amazon Simple Queue Service(Amazon SQS)-Warteschlange
2. Herunterladen und Installieren von Filebeat
3. Verbinden mit dem Elastic Stack
4. Konfigurieren von Filebeat zum Erfassen von Amazon CloudWatch Logs-Protokolldateien
5. Aktivieren und Konfigurieren Ihrer Datenerfassungsmodule
6. Einrichten Ihrer vorkonfigurierten Kibana-Dashboards und Starten von Filebeat
7. Analysieren von Amazon CloudWatch-Daten in Kibana

elastic

Analysieren der Amazon S3-Logging-Aktivität und Überwachen des Zugriffs mit Elastic

Mit Amazon S3 können Sie Daten und Geschäftsanwendungen speichern und statische Websites hosten. Bei Amazon S3 können zwei Arten von Workflows implementiert werden: die Erfassung von mit Amazon S3 gespeicherten nutzerdefinierten Logdaten und die Überwachung des Zugriffs auf den Amazon S3-Dienst und die zugehörigen Metriken.

Die Kombination aus Elastic und Amazon S3 kann für die folgenden Zwecke verwendet werden:

Erfassen von Informationen zu Anfragen, wie Remote-IP-Adresse, Anforderer, Bucket-Name und so weiter, für ein besseres Verständnis der Art des Traffics Ihrer Buckets

Ermitteln von Referenzwerten, Analysieren von Zugriffsmustern und Identifizieren von Trends in den vordefinierten Kibana-Dashboards

Ermitteln von Security- und Compliance-Problemen sowie Durchführen von Ursachenanalysen für die gesamte Organisation

Analysieren der in **Amazon S3** gespeicherten individuellen geschäfts- oder anwendungsspezifischen Logdaten

So senden Sie Amazon S3-Protokolldateien an Elastic:

Zunächst müssen Sie Angaben zu Ihrer AWS-Umgebung und zu Ihrem Elastic Cloud-Deployment zusammensammeln. Welche Angaben benötigt werden, entnehmen Sie bitte **Anhang A**. Wenn Sie sich mit Amazon S3-Protokollen noch nicht so gut auskennen, lesen Sie **Anhang B**. Dort finden Sie Informationen zu folgenden Themen:

1. Einrichten eines Amazon S3-Buckets und Erstellen einer Amazon SQS-Warteschlange
2. Herunterladen und Installieren von Filebeat
3. Verbinden mit dem Elastic Stack
4. Aktivieren und Konfigurieren Ihrer Datenerfassungsmodule
5. Konfigurieren von Filebeat für das Erfassen von Amazon S3-Protokolldateien
6. Einrichten Ihrer vorkonfigurierten Kibana-Dashboards und Starten von Filebeat
7. Analysieren von Amazon S3-Protokollen in Kibana

Streamen von Daten nach Elasticsearch mit Amazon Kinesis

Amazon Kinesis ist ein komplett verwalteter Dienst für die Lieferung von Echtzeit-Streaming-Daten an Ziele wie Amazon S3 und Elastic.

Amazon Kinesis ermöglicht Folgendes:

Streamen von Logdaten in Echtzeit und Analysieren dieser Daten mit Elasticsearch und Kibana, um schnell Erkenntnisse für fundiertere Entscheidungen zu gewinnen

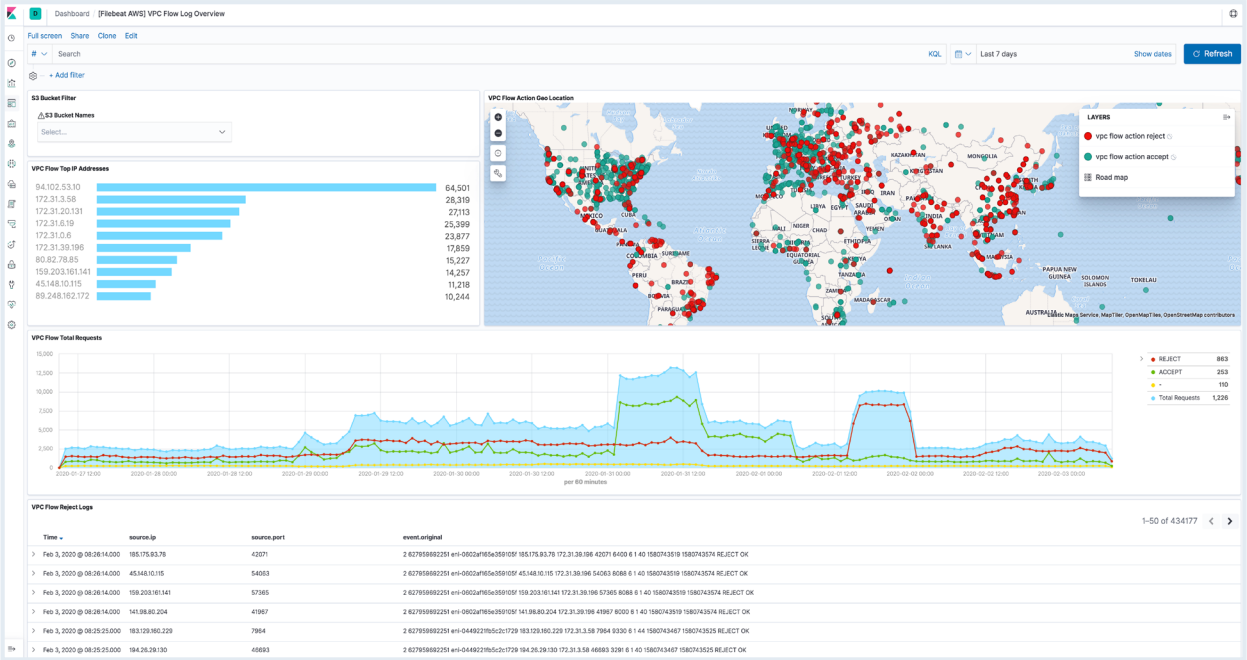
Kompromieren, Konvertieren und Verschlüsseln der Daten beim Transport zur Reduzierung der Speicherbeanspruchung und für mehr Sicherheit

So streamen Sie mit Amazon Kinesis Daten nach Elastic:

Zunächst müssen Sie Angaben zu Ihrer AWS-Umgebung sowie zu Ihrem Elastic Cloud-Deployment zusammensammeln. Welche Angaben benötigt werden, entnehmen Sie bitte **Anhang A**. Wenn Sie sich mit Amazon Kinesis noch nicht so gut auskennen, lesen Sie **Anhang C**. Dort finden Sie Informationen zu folgenden Themen:

1. Herunterladen und Installieren von Metricbeat
2. Verbinden mit dem Elastic Stack
3. Konfigurieren von Metricbeat für das Streamen von Daten
4. Aktivieren und Konfigurieren Ihrer Datenerfassungsmodule
5. Einrichten Ihrer vorkonfigurierten Kibana-Dashboards und Starten von Filebeat
6. Analysieren von Daten in Kibana

Überwachen des Netzwerkverkehrs anhand von Amazon VPC Flow Logs-Daten mit Elastic



Mit Elastic Observability können Sie schnell Amazon Virtual Private Cloud (Amazon VPC)-Flow-Protokolle durchsuchen, ansehen und filtern. Das ermöglicht die Überwachung des Netzwerkverkehrs innerhalb Ihrer Amazon-VPC mithilfe von Kibana. Diese Integration macht es möglich, die Daten in Flow-Protokollen zu analysieren und sie mit Sicherheitsgruppenkonfigurationen zu vergleichen, um Ihre Cloud-Security aufrechtzuerhalten und zu verbessern.

Das Ingestieren von Amazon VPC Flow Logs-Daten in Elastic ermöglicht Folgendes:

- Durchführen besserer Analysen für fundiertere Entscheidungen
- Bewerten von Sicherheitsgruppenregeln und Aufdecken von Sicherheitslücken
- Einrichten von Alarmen bei Erkennung bestimmter Arten von Verkehr
- Identifizieren von Latenzproblemen und Ermitteln von Referenzwerten zur Gewährleistung einer einheitlichen Leistung

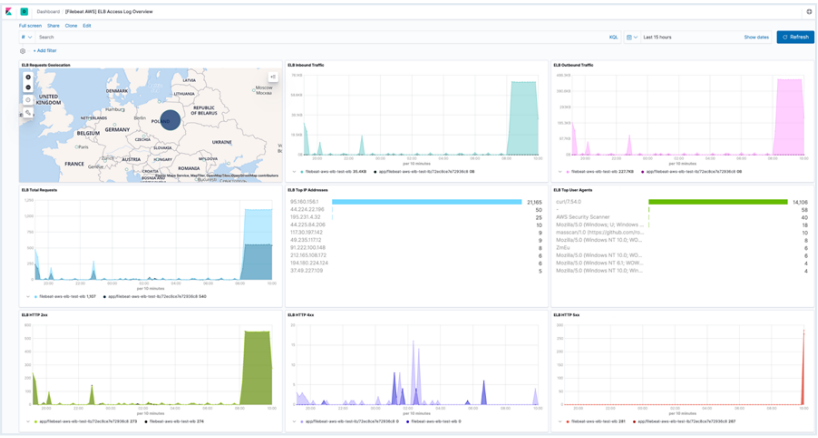
elastic

So ingestieren Sie Amazon VPC-Protokolle in Elastic:

Sammeln Sie zunächst Angaben zu Ihrer AWS-Umgebung sowie zu Ihrem Elastic Cloud-Deployment zusammen. Welche Angaben benötigt werden, entnehmen Sie bitte **Anhang A**. Informationen zur Vorgehensweise bei Amazon VPC-Flow-Protokollen finden Sie in **Anhang B**. Dort werden die folgenden Themen behandelt:

1. Einrichten eines Amazon S3-Buckets und Erstellen einer Amazon SQS-Warteschlange
2. Herunterladen und Installieren von Filebeat
3. Verbinden mit dem Elastic Stack
4. Konfigurieren von Filebeat zum Erfassen von Amazon VPC-Flow-Protokollen
5. Aktivieren und Konfigurieren Ihrer Datenerfassungsmodule
6. Einrichten Ihrer vorkonfigurierten Kibana-Dashboards und Starten von Filebeat
7. Analysieren von Protokollen in Kibana

Überwachen von Lastausgleichsoperationen in Elastic mit Amazon ELB



Mit dem AWS-Dienst Elastic Load Balancing (ELB) können Sie festlegen, dass der Netzwerkverkehr automatisch auf mehrere Cloud-Ressourcen aufgeteilt werden soll.

Das Zentralisieren von ELB-Protokollen mit Elastic ermöglicht Folgendes:

Überwachen detaillierter Informationen zu den Anforderungen, die an den Load Balancer gesendet werden

Analysieren von Traffic-Mustern und Problemereignissen zur Aufdeckung von Leistungsproblemen

Aufrufen detaillierter Informationen aus ELB-Log-daten zur Untersuchung von Serverreaktionen usw.

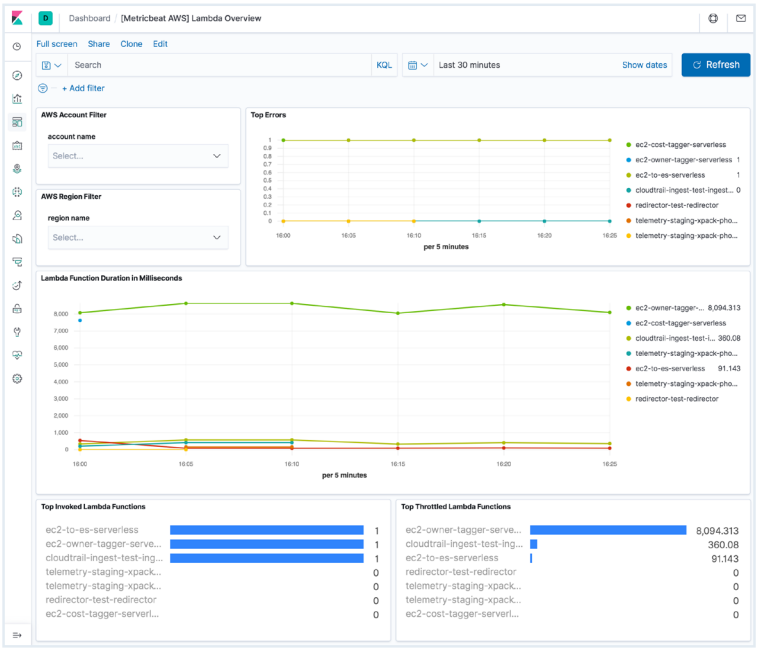
elastic

So senden Sie ELB-Daten an Elastic:

Bevor Sie beginnen können, müssen Sie einige Angaben zu Ihrer AWS-Umgebung und zu Ihrem Elastic Cloud-Deployment zusammensammeln. Welche Angaben benötigt werden, entnehmen Sie bitte **Anhang A**. Wenn Sie sich mit ELB auf AWS noch nicht so gut auskennen, lesen Sie **Anhang B**. Dort finden Sie Informationen zu folgenden Themen:

1. Einrichten eines Amazon S3-Buckets und Erstellen einer Amazon SQS-Warteschlange
2. Herunterladen und Installieren von Filebeat
3. Verbinden mit dem Elastic Stack
4. Konfigurieren von Filebeat zum Erfassen von AWS-ELB-Protokollen
5. Aktivieren und Konfigurieren Ihrer Datenerfassungsmodule
6. Einrichten Ihrer vorkonfigurierten Kibana-Dashboards und Starten von Filebeat
7. Analysieren von ELB-Protokollen in Kibana

Optimieren betrieblicher Workflows mit AWS Lambda in Elastic



AWS Lambda ist ein serverloser Berechnungsservice, mit dem Sie dynamisch Code ausführen können, um auf Ereignisse zu reagieren und Ihre betrieblichen Workflows zu optimieren. Mit AWS Lambda können Sie Berechnungsaufgaben jeder Art ausführen und Ihre Ressourcen mit Code für jede beliebige Anwendung automatisch verwalten lassen – ganz ohne Administrationsaufwand.

elastic

Die Verwendung von AWS Lambda in Elastic ermöglicht Ihnen Folgendes:

Performance-Monitoring von verschiedenen serverlosen Anwendungen aus

Verarbeiten von Logdaten und Metriken in Echtzeit

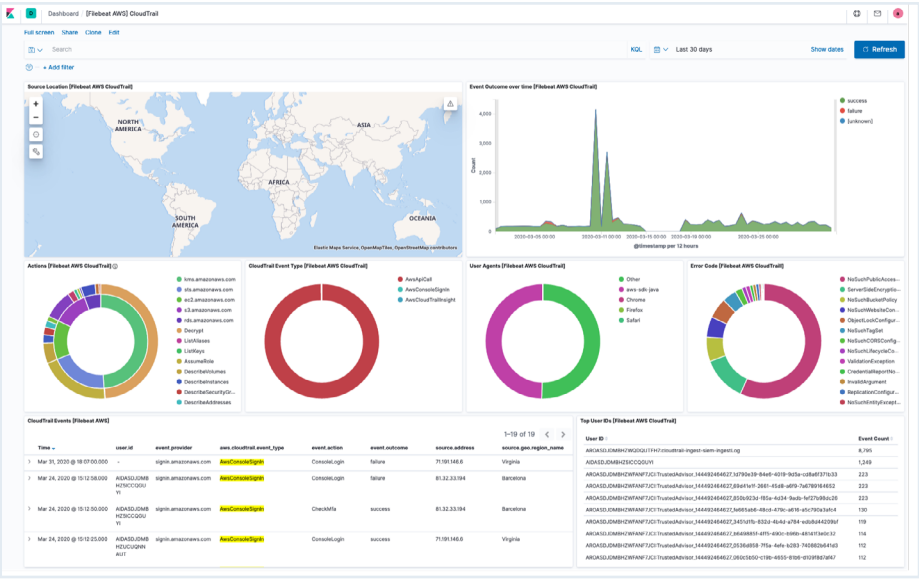
Erfassen und Korrelieren von Leistungsdaten mit Elastic-Lösungen

So richten Sie die Nutzung von AWS Lambda in Elastic ein:

Sammeln Sie zunächst Angaben zu Ihrer AWS-Umgebung sowie zu Ihrem Elastic Cloud-Deployment zusammen. Welche Angaben benötigt werden, entnehmen Sie bitte **Anhang A**. Wenn Sie sich mit AWS Lambda noch nicht so gut auskennen, lesen Sie **Anhang D**. Dort finden Sie Informationen zu folgenden Themen:

1. Herunterladen und Installieren von Functionbeat
2. Verbinden mit dem Elastic Stack
3. Konfigurieren von Cloud-Funktionen
4. Aktivieren und Konfigurieren von Datenerfassungsmodulen
5. Einrichten von Assets und Bereitstellen von Functionbeat
6. Erstellen von Kibana-Dashboards für Analysezwecke

Sicherstellen der Einhaltung von Governance- und Compliance-Standards mit AWS CloudTrail in Elastic



elastic

AWS CloudTrail ist ein Dienst zur Überwachung von Governance, Compliance, Betrieb und Risiken in Ihrem AWS-Konto.

Das Zentralisieren von AWS CloudTrail-Logdaten in Elastic ermöglicht Folgendes:

Visualisieren Ihrer AWS CloudTrail-Logdaten sowie der Konto- und Nutzeraktivität in vordefinierten Kibana-Dashboards für eine schnellere Analyse

Aufzeichnen von Informationen zu allen Aktionen, um Änderungen nachverfolgen und Probleme lösen zu können

Absichern und Überwachen Ihrer Netzwerkverbindungen

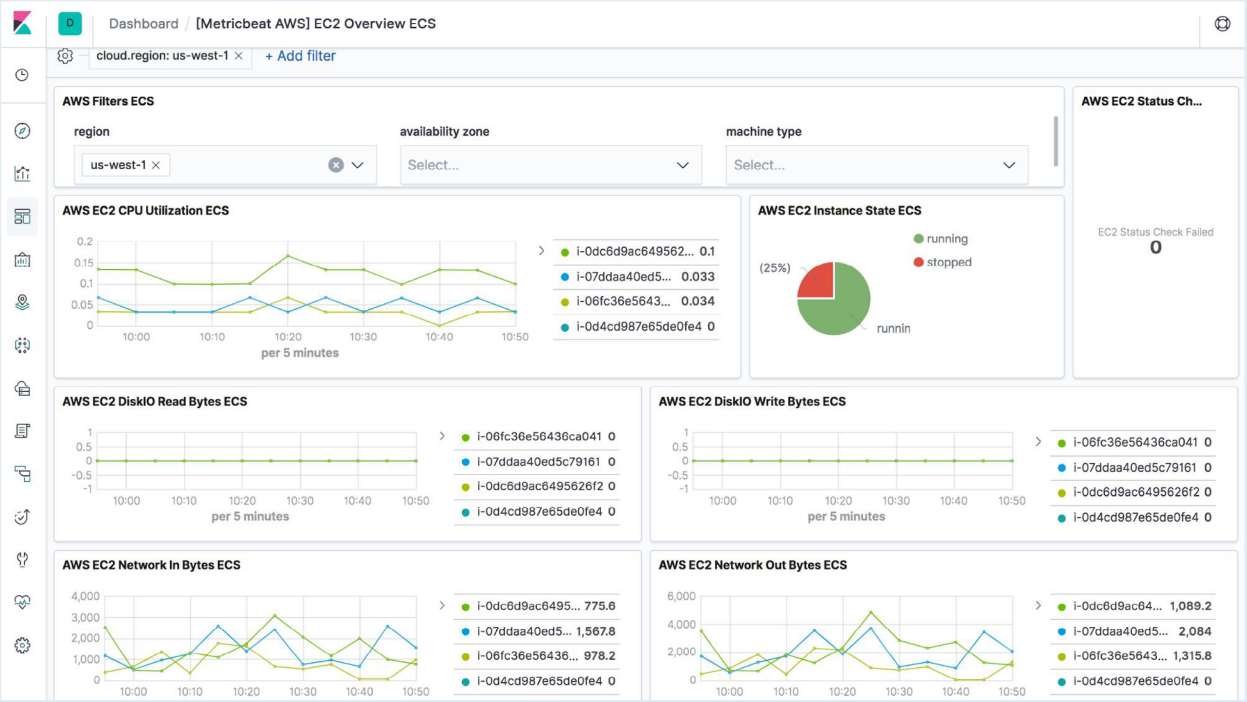
Sicherstellen der Einhaltung regulatorischer Vorgaben und Richtlinien

So ingestieren Sie AWS CloudTrail-Logdaten in Elastic:

Bevor Sie beginnen können, müssen Sie einige Angaben zu Ihrer AWS-Umgebung und zu Ihrem Elastic Cloud-Deployment zusammensammeln. Welche Angaben benötigt werden, entnehmen Sie bitte **Anhang A**. Wenn Sie sich mit AWS CloudTrail noch nicht so gut auskennen, lesen Sie **Anhang B**. Dort finden Sie Informationen zu folgenden Themen:

1. Einrichten eines Amazon S3-Buckets und Erstellen einer Amazon SQS-Warteschlange
2. Herunterladen und Installieren von Filebeat
3. Verbinden mit dem Elastic Stack
4. Konfigurieren von Filebeat zum Erfassen von AWS CloudTrail-Protokollen
5. Aktivieren und Konfigurieren Ihrer Datenerfassungsmodule
6. Einrichten Ihrer vorkonfigurierten Kibana-Dashboards und Starten von Filebeat
7. Analysieren von AWS CloudTrail-Logdaten in Kibana

Ingestieren und Zentralisieren von Metriken aus der gesamten AWS-Umgebung für umfassende Einblicke



Mit den Integrationen und vorkonfigurierten Dashboards für AWS von Elastic können Sie AWS-Metriken wie Nutzung, Leistung, Abrechnung und mehr erfassen und sich ein Bild von den Signalkorrelationen machen, um fundiertere Geschäftsentscheidungen treffen zu können.

Das kontinuierliche Überwachen und Analysieren Ihrer Berechnungs-, Speicher-, Netzwerk- und Datenmetriken aus AWS ermöglicht es Ihnen, schnell auf sich wandelnde Geschäftsanforderungen zu reagieren:

- Amazon Relational Database Service (Amazon RDS)
- Amazon Elastic Block Store (Amazon EBS)
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon VPC Network Address Translation (NAT) Gateway
- Amazon CloudWatch
- Amazon S3
- Amazon DynamoDB
- Amazon Simple Notification Service (SNS)
- Amazon SQS
- AWS-Kosten- und Nutzungsbericht
- AWS Billing and Cost Management
- AWS Virtual Private Network (AWS VPN)
- AWS Transit Gateway

Die AWS-Metriken ermöglichen umfassende Analysen, mit denen Sie fundiertere Entscheidungen treffen und so Folgendes tun können:

Korrelieren von Metriken aus Berechnungs-, Speicher- und Datendiensten für die zentralisierte Fehlerbehebung

Bewerten von Kapazitäts-, Leistungs- und Nutzungsbeschränkungen für ganzheitliche Skalierungsentscheidungen

Überwachen und Aufrechterhalten eines optimierten Cloud-Deployments mit automatisierter Analyse und Alerting unter Nutzung zentralisierter Daten

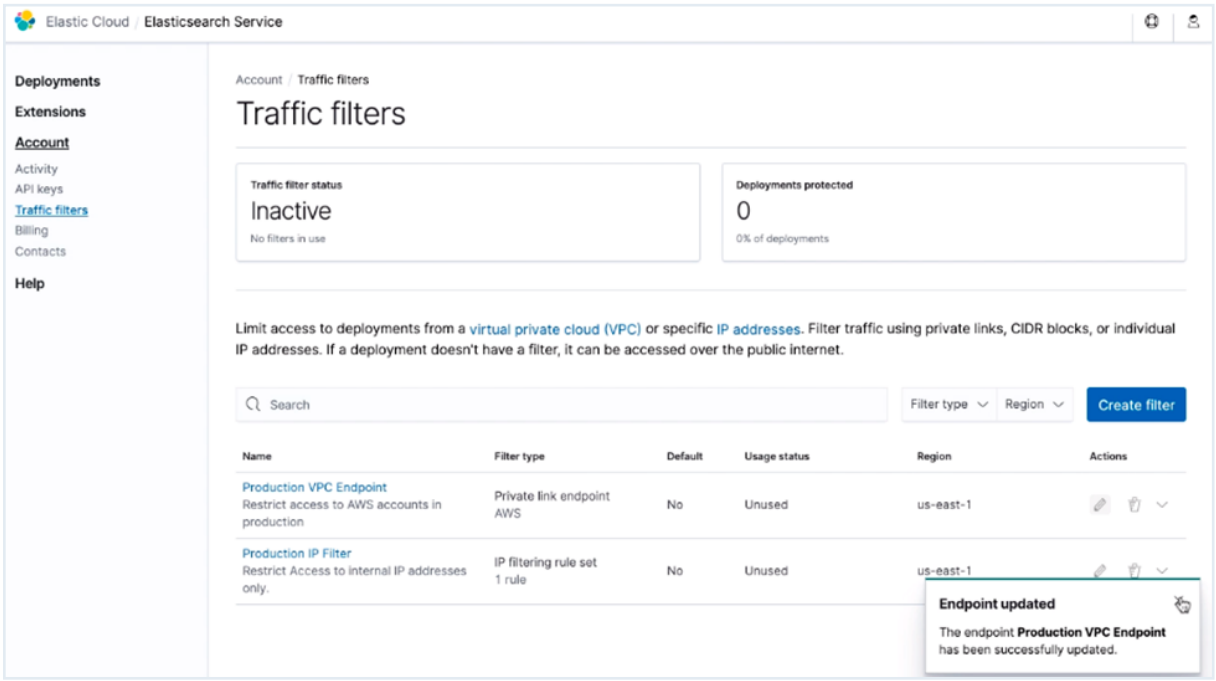
So beginnen Sie mit der Nutzung von AWS-Metriken und individueller Dashboards:

Zunächst müssen Sie Angaben zu Ihrer AWS-Umgebung sowie zu Ihrem Elastic Cloud-Deployment zusammensammeln. Welche Angaben benötigt werden, entnehmen Sie bitte **Anhang A**. Informationen zur Vorgehensweise beim Erstellen Ihres Dashboards finden Sie in **Anhang C**. Dort werden die folgenden Themen behandelt:

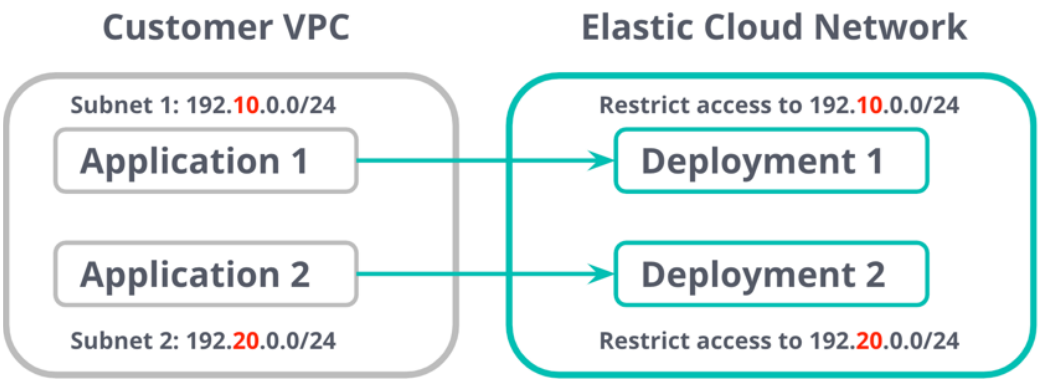
1. Herunterladen und Installieren von Metricbeat
2. Verbinden mit dem Elastic Stack
3. Konfigurieren von Metricbeat zur Erfassung von Metriken
4. Aktivieren und Konfigurieren Ihrer Datenerfassungsmodule
5. Einrichten Ihrer vorkonfigurierten Kibana-Dashboards und Starten von Filebeat
6. Analysieren Ihrer Metriken in Kibana

Wenn Sie mehr über das Erstellen individueller, auf Ihre Bedürfnisse zugeschnittener Dashboards erfahren möchten, sehen Sie sich unsere **Dokumentation** sowie dieses kurze **Video-Tutorial** an.

Zusätzliche Sicherheit und Flexibilität bei der Nutzung von Elastic mit AWS PrivateLink



AWS PrivateLink bietet private Konnektivität zwischen Ihren Amazon-VPCs, weiteren AWS-Ressourcen und Ihren On-Premises-Anwendungen. Auf diese Weise können Sie die Netzwerkverbindungen zwischen Ihren Anwendungen und Ihrem Elastic-Deployment schützen. Statt über das öffentliche Internet wird der Verkehr zwischen Ihrem virtuellem Netzwerk und Ihrem Elastic-Deployment über das AWS-Netzwerk geleitet und so vor unbefugtem Zugriff geschützt.



elastic

AWS PrivateLink bietet die folgenden Möglichkeiten:

- Erstellen von Endpoints mit privaten IP-Adressen, sodass Workloads so aussehen, als würden sie in Ihrem Netzwerk ausgeführt
- Sicherstellen, dass der gesamte Verkehr innerhalb des Amazon-Netzwerks bleibt und es zu keiner Zeit verlässt
- Profitieren von einer einfacheren Netzwerkverwaltung, sodass Sie keine komplexe Infrastruktur mehr aufrechterhalten müssen (NAT-Gateways, Zugriffssteuerungen)
- Beschränken des Verkehrs aus den virtuellen Netzwerken des Kunden zum Endpoint (im Gegensatz zum bidirektionalen Verkehr beim Amazon VPC-Peering ist AWS PrivateLink-Verkehr unidirektional)

So richten Sie die Nutzung von AWS PrivateLink in Elastic ein:

Eine detaillierte Schrittanleitung finden Sie in unserer **Dokumentation**.

elastic

Warum Elastic?

Durch die Bereitstellung von Elastic ergänzen Sie den bestehenden Funktionsumfang der Cloud und können so dazu beitragen, dass sich Ihre AWS-Investitionen schnell amortisieren.

Elastic Observability und die zugrundeliegenden Suchplattformfunktionen ergänzen Cloud-Infrastruktur-Innovationen

Elastic liefert seit jeher ständig neue Innovationen in den Bereichen Suche und Datenanalyse und hat damit die Suche immer wertvoller gemacht. Elastic, das Unternehmen hinter Elasticsearch und Kibana, veröffentlicht fortlaufend neue Funktionen, Sicherheits-Updates und Überarbeitungen für diese Produkte. Die Suche-Innovationen von Elastic auf der Softwareanwendungsebene ergänzen die Innovationen von AWS auf der Cloud-Infrastruktur-Ebene. Diese Kombination sorgt dafür, dass Sie schnell auf Geschäfts- und Betriebsdaten reagieren können und so weiter auf dem Weg zu einer agileren, datengesteuerten Organisation vorankommen.

Auswahl und Flexibilität – in der Cloud und „on-premises“

Die Elastic Search Platform bietet Entwicklern und Kunden die Flexibilität, selbst zu entscheiden, wo sie sie laufen lassen möchten. Dank erheblicher Investitionen können so Kernfunktionen für die Plattform bereitgestellt und gleichzeitig tiefe Integrationen für die Cloud entwickelt werden. Auch die Elastic Search Platform bietet ein konsistentes Sucherlebnis in der Cloud und „on-premises“. Die hybride Konsistenz erweist sich vor allem dann als wertvoll, wenn Sie schrittweise Ihre Cloud-Nutzung ausbauen, was bei großen Unternehmen durchaus Jahre dauern kann.

Cloud-Anbieter-übergreifende Konsistenz hilft auch dabei, die vorhandene Lösung um die jeweils besten Dienste auf dem Markt zu erweitern – unabhängig vom jeweiligen Cloud-Anbieter. Dies ist besonders für Observability- und Security-Anwendungsfälle wichtig, bei denen eine zentralisierte Ansicht aller Standorte dazu beitragen kann, die Fehlersuche und -behebung zu beschleunigen und das Risiko zu minimieren.

Schlüsselfertige Lösungen für Enterprise Search, Observability und Security

Elastic liefert „out-of-the-box“ vorkonfigurierte, schlüsselfertige Anwendungen für Enterprise-Search-Anwendungsfälle – Workplace Search, App Search und Site Search –, Observability-Anwendungsfälle – Logging und Application Performance Monitoring (APM) – und Security-Anwendungsfälle – SIEM und Endpoint-Schutz.

Alle Funktionen und externen Integrationen, die diese lösungsspezifischen Anwendungen ermöglichen, sind Teil der Elastic-Suchplattform und können von Kunden genutzt werden, die eigene Anwendungen für ihre Anforderungen entwickeln möchten. Dies umfasst auch ein breites Angebot an Integrationen zum Ingestieren der für Observability- und Security-Lösungen benötigten Daten in AWS.

Community und technische Kompetenz

Die Elastic Search Platform hat sich zum De-facto-Standard für Lösungen entwickelt, die auf der Suche basieren. Die Elasticsearch-Community bei GitHub zählt mehr als 1.500 Mitglieder. Darüber hinaus gehören Elasticsearch- und Kibana-Kenntnisse zum Grundwissen in der Branche. Elasticsearch wartet zudem mit leicht verfügbaren Integrationen für häufig genutzte zugehörige Anwendungen und Datenquellen auf. Wenn Sie für den Ausbau Ihrer suchebasierten Lösung Elastic Observability mit AWS nutzen, können Sie auf diese Ressourcen – die Experten, die Integrationen und die Elasticsearch-Community – zurückgreifen.

Wie werde ich Teil der Elastic-Community?

Diskussionsforen

Wenn Sie sich an der Elastic-Community beteiligen möchten, weil Sie eine Frage haben oder Ihre Erfahrungen mit anderen Nutzern teilen möchten, besuchen Sie unsere **Diskussionsforen**, an denen Sie sich auch in Ihrer Muttersprache beteiligen können.

Slack und lokale Communitys

Machen Sie in unserem schnell wachsenden **Elastic-Slack** mit, um auf den verschiedenen Kanälen, z. B. #elasticsearch, #kubernetes und #kibana-development, zu chatten oder Hilfe zu erhalten.

Außerdem gibt es überall in der Welt auch noch eine Vielzahl **anderer Online-Communitys**, in denen Sie sich mit Nutzern aus Ihrer Region über Elastic austauschen können.

Man lernt nie aus

Sie arbeiten sich gerade in den Elastic Stack ein? Sie suchen nach Detailinformationen? Im **Elastic-Beispiele-Repo** warten kuratierte Datensätze und Schrittanleitungen auf Sie. Und über unseren **Community-Newsletter** erfahren Sie, was es Neues von unserem Entwicklungsteam gibt.

Ihre Meinung ist uns wichtig

Nicht nur die Technologie entwickelt sich weiter, auch Elastic bleibt nicht stehen. Und wir sind sehr daran interessiert zu erfahren, was unsere Community zu sagen hat. Wenn Sie Hilfe benötigen oder Anmerkungen zu Ihren Erfahrungen mit Elastic haben, **lassen Sie es uns bitte wissen**.

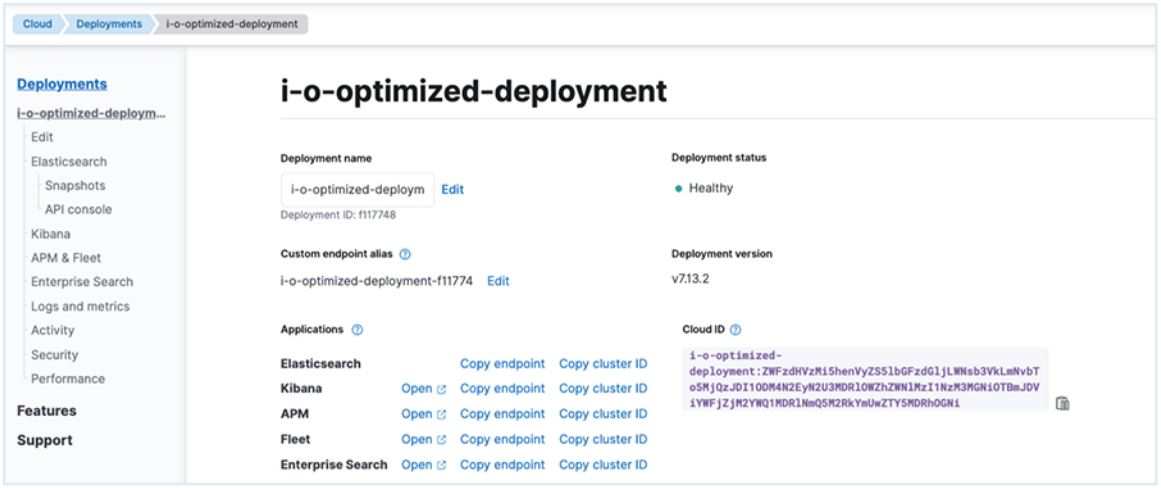
Anhang A – Vorbereitende Schritte

Bevor Sie mit dem Ingestieren Ihrer AWS-Daten beginnen können, müssen Sie zunächst einige Informationen zusammensammeln. Befolgen Sie dazu die folgenden Schritte:

- Ermitteln der Cloud-ID
- Abrufen der Anmeldeinformationen
- Erstellen der Zugriffsschlüssel-ID („Access Key ID“) und des Zugriffsschlüssels („Access Key“)

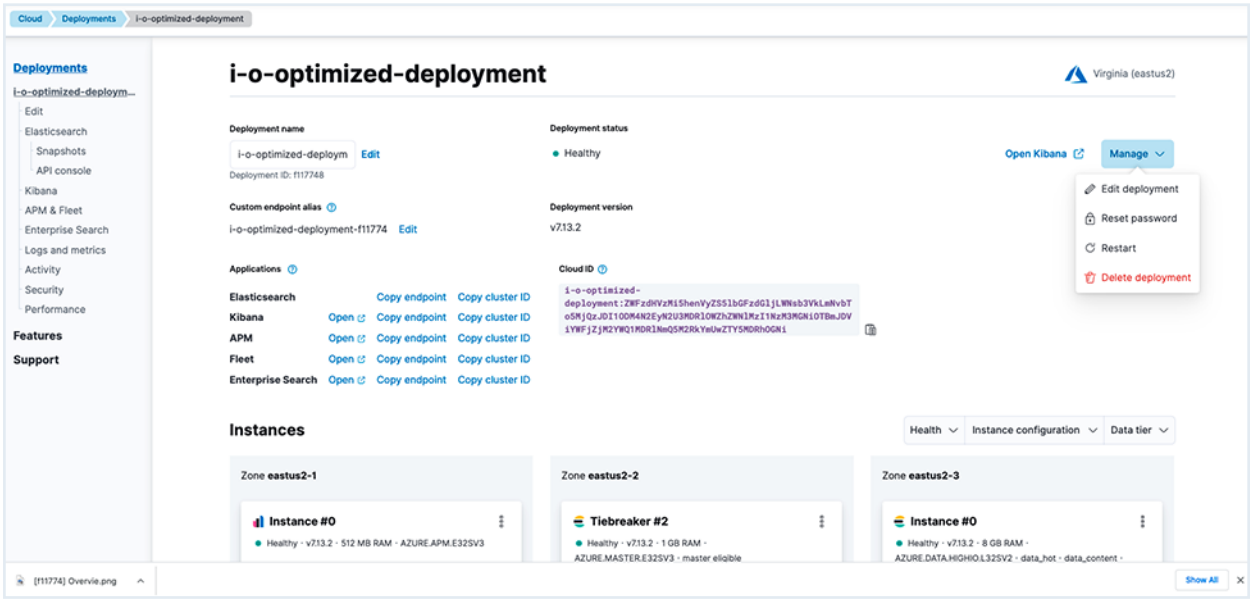
Ermitteln der Cloud-ID

Wenn Sie Ihre Cloud-ID herausfinden möchten, gehen Sie zu cloud.elastic.co und wählen Sie das entsprechende Deployment aus.



elastic

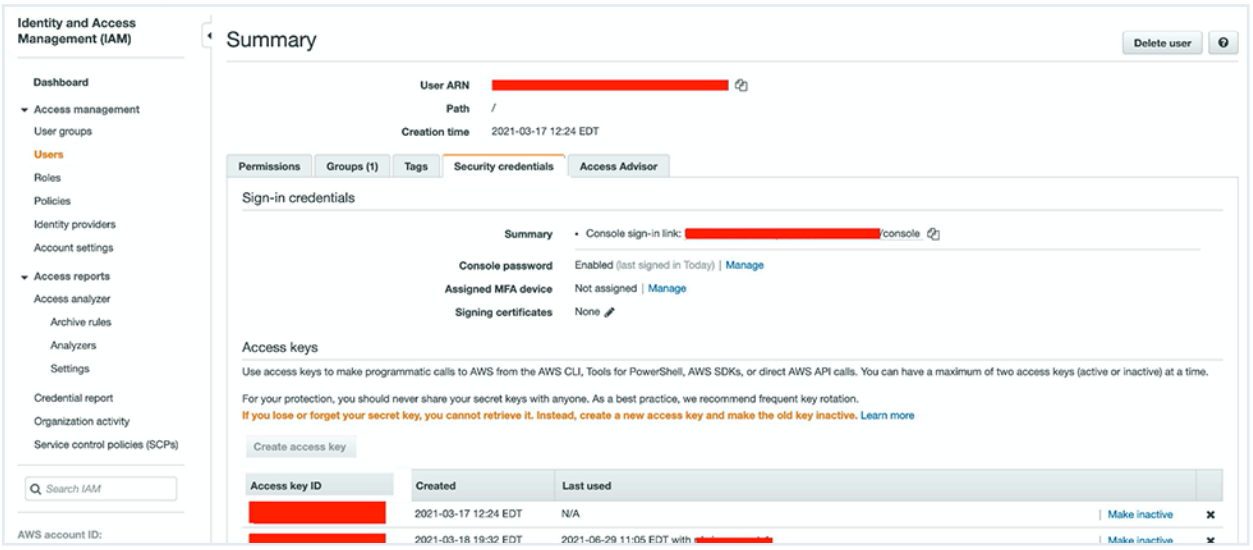
Abrufen der Anmeldeinformationen



Für das Senden von Daten an Elasticsearch können Sie den Standardnutzer „Elastic“ und das Passwort verwenden, das Sie beim Erstellen des Clusters erhalten haben, oder Sie können spezielle Nutzer und Rollen einrichten und ihnen nur die für die jeweilige Aufgabe absolut notwendigen Berechtigungen einräumen. In diesem Beispiel verwenden wir den Nutzer „Elastic“ und das bereitgestellte Passwort.

Wenn Sie das Passwort nicht abgerufen oder vergessen haben, können Sie zu cloud.elastic.co gehen und es durch Klicken auf „Manage“ zurücksetzen.

Erstellen der Zugriffsschlüssel-ID („Access Key ID“) und des Zugriffsschlüssels („Access Key“)



Die Zugriffsschlüssel-ID („Access Key ID“) und der Zugriffsschlüssel („Access Key“) werden für das Signieren Ihrer programmgesteuerten Anforderungen an AWS verwendet. Sie erhalten diese wie folgt:

- Melden Sie sich bei AWS Identity and Access Management (AWS IAM) an und öffnen Sie unter **https://console.aws.amazon.com/iam/** die IAM-Konsole.
- Wählen Sie links in der Navigationsansicht „Users“.
- Wählen Sie den gewünschten Nutzer aus und klicken Sie dann auf den Tab „Security credentials“.
- Klicken Sie unter „Access Keys“ auf „Create access key“ und wählen Sie „Show“. Daraufhin wird das Zugriffsschlüsselpaar angezeigt. Kopieren Sie die Schlüssel und speichern Sie sie. Sie benötigen sie für das Konfigurieren von Filebeat and Metricbeat.

Anhang B – Filebeat-Konfiguration

Im Folgenden erfahren Sie, wie Sie Filebeat installieren und AWS-Module aktivieren können. Zusammengefasst besteht der Prozess aus den folgenden Schritten:

1. Einrichten eines Amazon S3-Buckets und Erstellen einer Amazon SQS-Warteschlange
2. Herunterladen und Installieren von Filebeat
3. Verbinden mit dem Elastic Stack
   - Hierfür benötigen Sie Ihre Cloud-ID und das Cloud-Passwort für Ihr Elastic-Deployment.
4. Aktivieren und Konfigurieren Ihres Filebeat-Moduls
5. Konfigurieren von Filebeat, damit es Ihre AWS-Protokolle erfassen kann
   - Hierfür benötigen Sie Ihren AWS-Modul-Code sowie die AWS-Zugriffsschlüssel-ID („Access Key ID“) und den Zugriffsschlüssel („Access Key“).
6. Einrichten Ihrer vorkonfigurierten Kibana-Dashboards und Starten von Filebeat
7. Anzeigen und Analysieren von Daten in Kibana

Schritt 1: Einrichten eines Amazon S3-Buckets und Erstellen einer Amazon SQS-Warteschlange

Zur Vermeidung langer Wartezeiten beim Polling sämtlicher Protokolldateien aus jedem Amazon S3-Bucket kombiniert Filebeat die Benachrichtigung und das Polling, indem beim Erstellen eines neuen Amazon S3-Objekts über Amazon SQS eine Amazon S3-Benachrichtigung gesendet wird. Mehr darüber, wie Sie Ihr Amazon S3-Bucket und die Amazon SQS-Warteschlange einrichten können, erfahren Sie unter „**Konfigurieren von S3-Ereignisbenachrichtigungen mit SQS**“.

Schritt 2: Herunterladen und Installieren von Filebeat

Laden Sie Filebeat herunter und installieren Sie es. Verwenden Sie dazu die für Ihr System geltenden Befehle.

- Wir verwenden zur Demonstration Linux-Befehle. Die jeweils neueste Version können Sie der **Filebeat-Dokumentation** entnehmen. Klicken Sie dort auf „Quick start: installation and configuration“. Dort finden Sie auch Befehle für andere Betriebssysteme.

```
curl -L -O
https.//artifacts.elastic.co/downloads/beats/
filebeat/filebeat-7.13.3-linux-x86_64.tar.gz
tar xzvf filebeat-7.13.3-linux-x86_64.tar.gz
```

Schritt 3: Verbinden mit dem Elastic Stack

Für das Einrichten von Filebeat müssen Verbindungen zu Elasticsearch und Kibana hergestellt werden. Dazu müssen Sie die Konfigurationsdatei filebeat.yml ändern.

Um dies tun zu können, benötigen Sie die Cloud-ID und das zugehörige Passwort. Geben Sie mit **cloud.id** die ID Ihres Elasticsearch Service an und legen Sie für **cloud.auth** unter Verwendung des Formats „nutzername:passwort“ den Nutzer fest, der die Berechtigung hat, Filebeat einzurichten. Das könnte beispielsweise wie folgt aussehen:

```
cloud.id.
"staging.dxMtZWFzdC0xLmF3cy5mb3VuZC5pbyRjZWM2ZjI2MWE3NGJmMjRjZTMzYmI4ODExY
jg0Mjk0ZiRjNmMyY2E2ZDA0MjI0OWFmMGNjN2Q3YTllOTYyNTc0Mw=="
cloud.auth. "elastic.<elastic-password>"
```

Zusätzliche Sicherheit erhalten Sie, indem Sie den **Filebeat-Keystore** verwenden, um die Anmeldeinformationen (Nutzername, Passwort, Cloud-ID usw.) zu verschleiern, und Nutzer und Rollen anlegen, denen Sie nur die für die Erfüllung der jeweiligen Aufgabe absolut nötigen Berechtigungen einräumen. In unserem Beispiel werden der Standard-Nutzername und das Passwort verwendet, das Sie beim Erstellen Ihres Deployments erhalten haben. Außerdem wird der Standard-Superuser als Beispiel verwendet. Für den Einsatz in einer Produktionsumgebung empfiehlt es sich, Nutzer und Rollen **mit nur so vielen Berechtigungen wie für die Aufgabe erforderlich** („least privileges necessary“) einzurichten.

Denken Sie daran, für die bereitgestellte Funktion eine eigene Rolle zu erstellen. Das könnte beispielsweise wie folgt aussehen:

```
role. arn.aws.iam..123456789012.role/MyFunction
```

Sorgen Sie dafür, dass diese eigene Rolle die Berechtigungen erhält, die für die Ausführung der Funktion erforderlich sind. Weitere Informationen finden Sie unter „**IAM permissions required to deploy Functionbeat**“.

Schritt 4: Aktivieren und Konfigurieren von Datenerfassungsmodulen

Gehen Sie zum Aktivieren des AWS-Moduls zum Filebeat-Verzeichnis und geben Sie den folgenden Befehl ein:

```
./filebeat modules enable aws
```

Schritt 5: Konfigurieren von Filebeat für das Erfassen Ihrer AWS-Protokollen

Navigieren Sie in der Datei aws.yml im Verzeichnis „modules.d“ zu den AWS-Modul-Konfigurationen. Wenn der Code für die gewünschte Integration fehlt, lesen Sie den **Anhang E**.

Außerdem benötigen Sie die AWS-Anmeldeinformationen aus Anhang A. Diese müssen am Anfang der Datei aws.yml eingegeben werden:

- access_key_id: "IHRE AWS-ZUGRIFFSSCHLÜSSEL-ID"
- secret_access_key: "IHR AWS-ZUGRIFFSSCHLÜSSEL"

Wenn Sie eine andere Authentifizierungsmethode vorziehen, finden Sie unter „**AWS Credentials Configuration**“ entsprechende Optionen.

Wie Sie Ihre AWS-Zugriffsschlüssel-ID („access_key_id“) und Ihren Zugriffsschlüssel („secret_access_key“) eingeben müssen, zeigt das folgende Beispiel:

```
module. aws
var.access_key_id. "XyzW4VIA6DCIEKDUNB"
var.secret_access_key. "p4873PxKFRB/enxV98PExUtQkEU82Coafo1w6"
```

Wie Sie Ihre IAM-Rolle eingeben müssen, zeigt das folgende Beispiel:

```
module. aws
#Zu übernehmende AWS-IAM-Rolle
var.role_arn. arniam..123456789012.role/test-mb
```

Wenn Sie Ihre AWS-Zugriffsschlüssel-ID und den Zugriffsschlüssel verschleiern möchten, können Sie den **Filebeat-Keystore** verwenden.

Schritt 6: Einrichten Ihrer vorkonfigurierten Kibana-Dashboards und Starten von Filebeat

Filebeat enthält standardmäßig vordefinierte Assets für das Parsen, Indexieren und Visualisieren Ihrer Daten. Gehen Sie zum Laden dieser Assets wie folgt vor:

- Wenn Sie nicht den Nutzer „elastic“ (Standardnutzer) verwenden, achten Sie darauf, dass der in filebeat.yml angegebene Nutzer **zur Einrichtung von Filebeat berechtigt** ist.
- Führen Sie vom Installationsverzeichnis aus Folgendes aus:
  `./filebeat setup -e`

Ändern Sie vor dem Starten von Filebeat in filebeat.yml die Anmeldeinformationen und geben Sie einen Nutzer an, der berechtigt ist, Ereignisse zu veröffentlichen.

Starten Sie Filebeat mit den folgenden Befehlen:

```
sudo chown root filebeat.yml
sudo chown root modules.d/aws.yml
sudo ./filebeat -e -c filebeat.yml &
```

Schritt 7: Aufrufen und Analysieren von Daten in Kibana

Filebeat enthält standardmäßig vorkonfigurierte Kibana-Dashboards und eine spezielle Anwendung für das Visualisieren, Suchen und Filtern von Logdaten namens Logs. Hinzu kommen Anomalieerkennungsfunktionen, die sich ganz einfach konfigurieren lassen. Sie haben die Dashboards bereits geladen, als Sie den Setup-Befehl ausgeführt haben.

So starten Sie Kibana:

- **Melden Sie sich bei Ihrem Elastic Cloud-Konto an.**
- Navigieren Sie in Ihrem Deployment zum Kibana-Endpoint, um Ihre Daten aufzurufen und zu analysieren.

Anhang C – Metricbeat-Konfiguration

Im Folgenden erfahren Sie, wie Sie Metricbeat installieren und AWS-Module aktivieren können. Zusammengefasst besteht der Prozess aus den folgenden Schritten:

1. Herunterladen und Installieren von Metricbeat
2. Verbinden mit dem Elastic Stack
   - Hierfür benötigen Sie Ihre Cloud-ID und das Cloud-Passwort für Ihr Elastic-Deployment.
3. Aktivieren und Konfigurieren von Datenerfassungsmodulen
4. Konfigurieren von Metricbeat, damit es AWS-Metriken erfassen kann
   - Hierfür benötigen Sie Ihren AWS-Modul-Code sowie die AWS-Zugriffsschlüssel-ID („Access Key ID“) und den Zugriffsschlüssel („Access Key“).
5. Einrichten Ihrer vorkonfigurierten Kibana-Dashboards und Starten von Metricbeat
6. Aufrufen und Analysieren von Daten in Kibana

Schritt 1: Herunterladen und Installieren von Metricbeat

Laden Sie Metricbeat herunter und installieren Sie es. Verwenden Sie dazu die für Ihr System geltenden Befehle.

Wir verwenden zur Demonstration Linux-Befehle. Die jeweils neueste Version können Sie der **Metricbeat-Dokumentation** entnehmen. Klicken Sie dort auf „Quick start: installation and configuration“. Dort finden Sie auch Befehle für andere Betriebssysteme.

```
curl -L -O https://artifacts.elastic.co/downloads/beats/
metricbeat/metricbeat-7.13.4-linux-x86_64.tar.gz
tar xzvf metricbeat-7.13.4-linux-x86_64.tar.gz
```

Schritt 2: Verbinden mit dem Elastic Stack

Für das Konfigurieren von Metricbeat müssen Sie die Konfigurationsdatei metricbeat.yml bearbeiten.

Um dies tun zu können, benötigen Sie die Cloud-ID und das zugehörige Passwort. Geben Sie mit **cloud.id** die ID Ihres Elasticsearch Service an und legen Sie für **cloud.auth** unter Verwendung des Formats „nutzername:passwort“ den Nutzer fest, der die Berechtigung hat, Metricbeat einzurichten. Das könnte beispielsweise wie folgt aussehen:

```
cloud.id.
"staging.dxMtZWFzdC0xLmF3cy5mb3VuZC5pbyRjZWM2ZjI2MWE3NGJmMjRjZTMzYmI4ODExY
jg0Mjk0ZiRjNmMyY2E2ZDA0MjI0OWFmMGNjN2Q3YTllOTYyNTc0Mw=="
cloud.auth. "elastic.<elastic-password>"
```

Zusätzliche Sicherheit erhalten Sie, indem Sie den **Metricbeat-Keystore** verwenden, um die Anmeldeinformationen (Nutzername, Passwort, Cloud-ID usw.) zu verschleiern, und Nutzer und Rollen anlegen, denen Sie nur die für die Erfüllung der jeweiligen Aufgabe absolut nötigen Berechtigungen einräumen. In unserem Beispiel werden der Standard-Nutzername und das Passwort verwendet, das Sie beim Erstellen Ihres Deployments erhalten haben. Außerdem wird der Standard-Superuser als Beispiel verwendet. Für den Einsatz in einer Produktionsumgebung empfiehlt es sich, Nutzer und Rollen **mit nur so vielen Berechtigungen wie für die Aufgabe erforderlich** („least privileges necessary“) einzurichten.

Denken Sie daran, für die bereitgestellte Funktion eine eigene Rolle zu erstellen. Das könnte beispielsweise wie folgt aussehen:

```
role. arn.aws.iam..123456789012.role/MyFunction
```

Sorgen Sie dafür, dass diese eigene Rolle die Berechtigungen erhält, die für die Ausführung der Funktion erforderlich sind. Weitere Informationen finden Sie unter „**IAM permissions required to deploy Functionbeat**“.

Schritt 3: Aktivieren und Konfigurieren von Datenerfassungsmodulen

Beim Konfigurieren von Metricbeat müssen Sie angeben, welche Module ausgeführt werden sollen. Metricbeat verwendet zum Erfassen von Metriken Module. Geben Sie zum Aktivieren des AWS-Konfigurationsmoduls im Verzeichnis „modules.d“ den folgenden Befehl ein:

```
./metricbeat modules enable aws
```

Schritt 4: Konfigurieren von Metricbeat, damit es Ihre AWS-Metriken erfassen kann

Navigieren Sie in der Datei aws.yml im Verzeichnis „modules.d“ zu den AWS-Modul-Konfigurationen. Wenn der Code für die gewünschte Integration fehlt, lesen Sie den **Anhang E**.

Außerdem benötigen Sie die AWS-Anmeldeinformationen. Diese müssen am Anfang der Datei aws.yml eingegeben werden:

- access_key_id: "IHRE AWS-ZUGRIFFSSCHLÜSSEL-ID"
- secret_access_key: "IHR AWS-ZUGRIFFSSCHLÜSSEL"

Wenn Sie eine andere Authentifizierungsmethode vorziehen, finden Sie unter „**AWS Credentials Configuration**“ entsprechende Optionen.

Wie Sie Ihre AWS-Zugriffsschlüssel-ID („access_key_id“) und Ihren Zugriffsschlüssel („secret_access_key“) eingeben müssen, zeigt das folgende Beispiel:

```
module. aws
access_key_id. "XyzW4VIA6DCIEKDUNB"
secret_access_key. "p4873PxKFRB/enxV98PExUtQkEU82Coafo1w6"
```

Wie Sie Ihre IAM-Rolle eingeben müssen, zeigt das folgende Beispiel:

```
module. aws
#Zu übernehmende AWS-IAM-Rolle
role_arn. arniam..123456789012.role/test-mb
```

Wenn Sie Ihre AWS-Zugriffsschlüssel-ID und den Zugriffsschlüssel verschleiern möchten, können Sie den **Metricbeat-Keystore** verwenden.

Schritt 5: Einrichten Ihrer vorkonfigurierten Kibana-Dashboards und Starten von Metricbeat

Metricbeat enthält standardmäßig beispielhafte Kibana-Dashboards, -Visualisierungen und -Suchen zum Visualisieren von AWS-Metrikdaten in Kibana sowie Alerting- und Anomalieerkennungsfunktionen, die sich ganz einfach konfigurieren lassen.

- Wenn Sie nicht den Nutzer „elastic“ (Standardnutzer) verwenden, achten Sie darauf, dass der in metricbeat.yml angegebene Nutzer **zur Einrichtung von Metricbeat** berechtigt ist.
- Führen Sie vom Installationsverzeichnis aus Folgendes aus:

  ```
  ./metricbeat setup -e
  ```

Starten Sie Metricbeat mit den folgenden Befehlen:

```
sudo chown root metricbeat.yml
sudo chown root modules.d/aws.yml
sudo ./metricbeat -e -c metricbeat.yml &
```

Schritt 6: Aufrufen und Analysieren von Daten in Kibana

Metricbeat enthält standardmäßig vorkonfigurierte Kibana-Dashboards und eine spezielle Anwendung für das Visualisieren von Metrikdaten. Sie haben die Dashboards bereits geladen, als Sie den Setup-Befehl ausgeführt haben.

So starten Sie Kibana:

- **Melden Sie sich bei Ihrem Elastic Cloud-Konto an.**
- Navigieren Sie in Ihrem Deployment zum Kibana-Endpoint.

Anhang D – Functionbeat-Konfiguration

Im Folgenden erfahren Sie, wie Sie Functionbeat installieren und AWS-Module aktivieren können. Zusammengefasst besteht der Prozess aus den folgenden Schritten:

1. Functionbeat herunterladen und installieren
2. Verbinden mit dem Elastic Stack
   - Hierfür benötigen Sie Ihre Cloud-ID und das Cloud-Passwort für Ihr Elastic-Deployment.
3. Konfigurieren von Cloud-Funktionen
   - Hierfür benötigen Sie Ihren AWS-Modul-Code sowie die AWS-Zugriffsschlüssel-ID („Access Key ID“) und den Zugriffsschlüssel („Access Key“).
4. Einrichten von Assets und Bereitstellen von Functionbeat
5. Erstellen von Kibana-Dashboards für Analysezwecke

Schritt 1: Herunterladen und Installieren von Functionbeat

Laden Sie Functionbeat herunter und installieren Sie es. Verwenden Sie dazu die für Ihr System geltenden Befehle.

- Wir verwenden zur Demonstration Linux-Befehle. Die Befehle für andere Betriebssysteme finden Sie in unserer **Dokumentation**.

```
curl -L -O https://artifacts.elastic.co/downloads/beats/
functionbeat/functionbeat-7.13.4-linux-x86_64.tar.gz
tar xzvf functionbeat-7.13.4-linux-x86_64.tar.gz
```

Schritt 2: Verbinden mit dem Elastic Stack

Für die Verwendung von Functionbeat müssen Verbindungen zu Elasticsearch und Kibana hergestellt werden. Dazu müssen Sie die Konfigurationsdatei functionbeat.yml ändern.

Um dies tun zu können, benötigen Sie die Cloud-ID und das zugehörige Passwort. Geben Sie mit **cloud.id** die ID Ihres Elasticsearch Service an und legen Sie für **cloud.auth** (Passwort) einen Nutzer fest, der die Berechtigung hat, Functionbeat einzurichten. Das könnte beispielsweise wie folgt aussehen:

```
cloud.id.
"staging.dxMtZWFzdC0xLmF3cy5mb3VuZC5pbyRjZWM2ZjI2MWE3NGJmMjRjZTMzYmI4ODExY
jg0Mjk0ZiRjNmMyY2E2ZDA0MjI0OWFmMGNjN2Q3YTllOTYyNTc0Mw=="
cloud.auth. "functionbeat_setup.YOUR_PASSWORD"
```

Denken Sie daran, für die bereitgestellte Funktion eine eigene Rolle zu erstellen. Das könnte beispielsweise wie folgt aussehen:

```
role. arn.aws.iam..123456789012.role/MyFunction
```

Sorgen Sie dafür, dass diese eigene Rolle die Berechtigungen erhält, die für die Ausführung der Funktion erforderlich sind. Weitere Informationen finden Sie unter „**IAM permissions required to deploy Functionbeat**“.

Schritt 3: Konfigurieren von Cloud-Funktionen

Bevor Sie Functionbeat für AWS bereitstellen, müssen Sie Details zu den Cloud-Funktionen angeben, die Sie bereitstellen möchten. Dazu gehören die Funktionsnamen und -typen sowie die Auslöser für das Ausführen der Funktion.

Konfigurieren Sie in functionbeat.yml die Funktionen, die Sie bereitstellen möchten. Die Konfigurationseinstellungen hängen vom Typ der Funktion und vom verwendeten Cloud-Anbieter ab. Wenn der Code für die gewünschte Integration fehlt, lesen Sie den **Anhang E**. Eine Konfiguration könnte zum Beispiel wie folgt aussehen:

```
functionbeat.provider.aws.endpoint. "s3.amazonaws.com"
functionbeat.provider.aws.deploy_bucket. "functionbeat-deploy"
functionbeat.provider.aws.functions.
  - name. cloudwatch
    enabled. true
    type. cloudwatch_logs
    description. "lambda function for cloudwatch logs"
    triggers.
      - log_group_name. /aws/lambda/my-lambda-function
```

Sie brauchen auch Ihre AWS-Anmeldeinformationen. Geben Sie Ihre AWS-Anmeldeinformationen am Beginn der Datei functionbeat.yml an:

- access_key_id: "IHRE AWS-ZUGRIFFSSCHLÜSSEL-ID"
- secret_access_key: "IHR AWS-ZUGRIFFSSCHLÜSSEL"

Wenn Sie eine andere Authentifizierungsmethode vorziehen, finden Sie unter „**AWS Credentials Configuration**“ entsprechende Optionen.

Sehen Sie sich dazu das folgende Beispiel an:

```
module. cloudwatch
enabled. true
access_key_id. "XyzW4VIA6DCIEKDUNB"
secret_access_key. "p4873PxKFRB/enxV98PExUtQkEU82Coafo1w6"
```

Schritt 4: Einrichten von Assets und Bereitstellen von Functionbeat

Functionbeat enthält standardmäßig vordefinierte Assets für das Parsen, Indexieren und Visualisieren Ihrer Daten. Gehen Sie zum Laden dieser Assets wie folgt vor:

Vergewissern Sie sich, dass der in functionbeat.yml angegebene Nutzer **zum Einrichten von Functionbeat berechtigt ist**. Führen Sie vom Installationsverzeichnis aus Folgendes aus:

```
./functionbeat setup -e
```

Verwenden Sie zum Bereitstellen der Cloud-Funktionen den folgenden Befehl:

```
./functionbeat -v -e -d "*" deploy cloudwatch
```

Die Funktion ist damit für AWS bereitgestellt und kann ab sofort Protokollereignisse an das konfigurierte Ausgabeziel senden.

Schritt 5: Erstellen von Kibana-Dashboards für Analysezwecke

Jetzt können Sie Ihre Dashboards in Kibana erstellen. Wenn Sie mehr über das Anzeigen und Erkunden Ihrer Daten erfahren möchten, lesen Sie das **Kibana-Benutzerhandbuch**. So starten Sie Kibana:

- **Melden Sie sich bei Ihrem Elastic Cloud-Konto an.**
- Navigieren Sie in Ihrem Deployment zum Kibana-Endpoint.

Anhang E – Weitere Ressourcen

Weiterführende Informationen zu AWS-Konfigurationen finden Sie in den entsprechenden Abschnitten der Dokumentationen für die einzelnen Module:

- **Filebeat**
- **Metricbeat**
- **Functionbeat**

elastic

Search. Observe. Protect.

Elastic macht Daten für Anwendungen wie Enterprise Search, Observability und Security nutzbar – in Echtzeit und unabhängig von ihrer Menge. Die Lösungen von Elastic bauen auf einem kostenlosen und offenen Technologie-Stack auf, der überall bereitgestellt werden kann und in kürzester Zeit Einblicke ermöglicht. Das Datenformat ist dabei ebenso wenig eingeschränkt wie die Anwendungsbereiche – vom Finden von Dokumenten über die Infrastrukturüberwachung bis hin zur Jagd auf Bedrohungen. Tausende Organisationen weltweit, darunter Cisco, Goldman Sachs, Microsoft, The Mayo Clinic, NASA, The New York Times, Wikipedia und Verizon, nutzen Elastic zur Unterstützung ihrer unternehmenskritischen Systeme. Elastic wurde 2012 gegründet und die Aktien des Unternehmens werden an der New Yorker Börse (NYSE) unter dem Symbol „ESTC“ gehandelt. Weitere Informationen erhalten Sie unter elastic.co/de.

AMERICAS HQ
800 West El Camino Real, Suite 350, Mountain View, California 94040, USA
Allgemein +1 650 458 2620, Vertrieb +1 650 458 2625

info@elastic.co