

Analyse von Log Analytics-ELK Stack auf der ISE

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[ELK Stack](#)

[ELK Stack als Protokollanalyse](#)

[Aktivieren von Protokollanalysen](#)

[Navigationsmenü](#)

[Integrierte Dashboards](#)

[Neue Dashboards erstellen](#)

[Schritt 1: Indexmuster erstellen \(Datenquelle\)](#)

[Schritt 2: Visualisierungen erstellen](#)

[Schritt 3: Dashboard erstellen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

Dieses Dokument beschreibt die ELK Stack-Komponenten, die in die Cisco Identity Services Engine (ISE) 3.3 bis System 360 Log Analytics integriert sind.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Identity Service Engine
- ELK Stack

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- ISE 3.3

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

System 360 umfasst Monitoring und Log Analytics.

Mit der **Überwachungsfunktion** können Sie eine Vielzahl von Anwendungs- und Systemstatistiken sowie die Leistungskennzahlen aller Knoten in einer Bereitstellung über eine zentrale Konsole überwachen. KPIs sind nützlich, um einen Einblick in den allgemeinen Zustand der Knotenumgebung zu gewinnen. Die Statistik bietet eine vereinfachte Darstellung der Systemkonfigurationen und nutzungsspezifischen Daten.

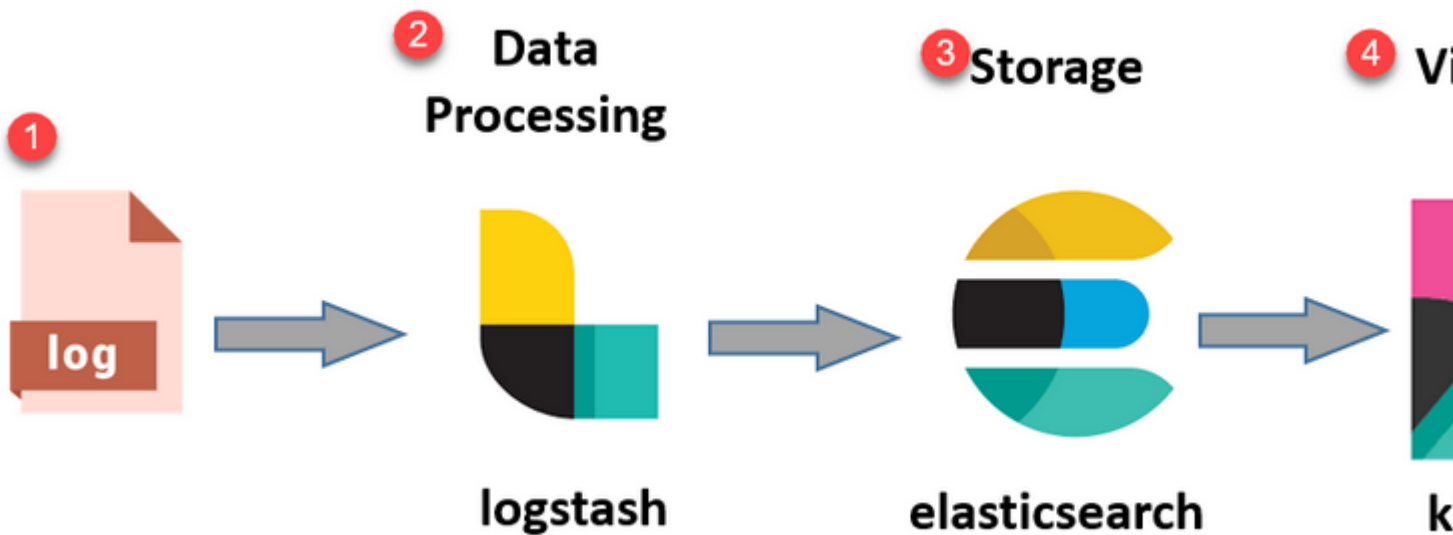
Log Analytics bietet ein flexibles Analysesystem für die detaillierte Analyse von Endgeräteauthentifizierungs-, Autorisierungs- und Accounting (AAA)-Daten sowie die Profilerstellung für Syslog-Daten. Sie können auch die Statusübersicht und den Prozessstatus der Cisco ISE analysieren. Sie können Berichte erstellen, die dem Cisco ISE-Bericht "Zähler" und "Statusübersicht" ähneln.

ELK Stack

Der ELK Stack ist ein beliebter Open-Source-Software-Stack, der zum Sammeln, Verarbeiten und Visualisieren großer Datenmengen verwendet wird. Es steht für Elasticsearch, Logstash und Kibana.

- **Elasticsearch:** Elasticsearch ist eine verteilte Such- und Analysemaschine. Es wurde entwickelt, um große Datenmengen schnell und nahezu in Echtzeit zu speichern, zu durchsuchen und zu analysieren. Es verwendet eine JSON-basierte Abfragesprache und ist hochskalierbar.
- **Logstash:** Logstash ist eine Pipeline für die Datenverarbeitung, die Daten aus mehreren Quellen verarbeitet und transformiert. Es kann Daten analysieren und anreichern, sodass sie besser strukturiert und für Analysen geeignet sind. Logstash unterstützt eine Vielzahl von Eingangs- und Ausgangsquellen.
- **Kibana:** Kibana ist eine Datenvisualisierungsplattform, die mit Elasticsearch zusammenarbeitet. Sie ermöglicht es Benutzern, interaktive Dashboards, Diagramme, Diagramme und Visualisierungen zu erstellen, um die in Elasticsearch gespeicherten Daten zu erkunden und zu verstehen. Kibanas Schnittstelle vereinfacht die Abfrage und Visualisierung von Daten.

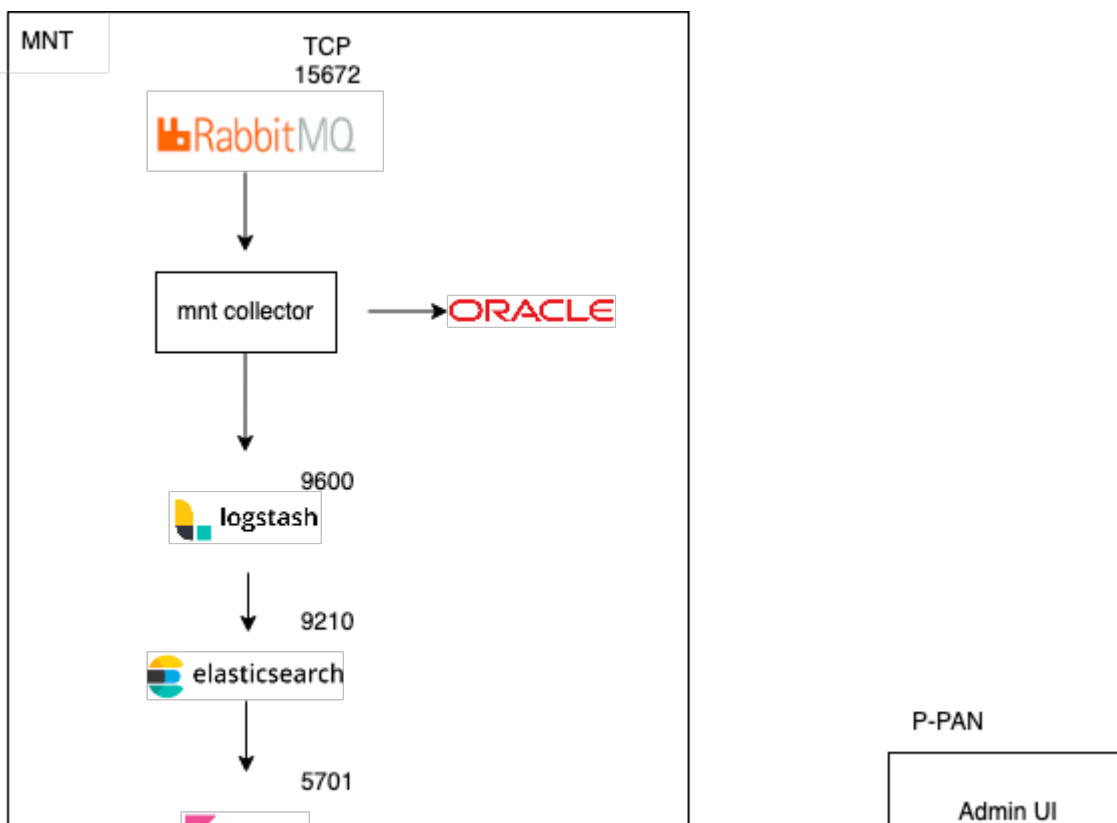
In Kombination bilden diese Komponenten einen leistungsstarken Stack für das Management und die Analyse verschiedener Datentypen, von Protokolldateien bis hin zu Metriken und mehr. Gleichzeitig bieten sie Visualisierungsfunktionen, um die Informationen verständlich zu machen.



ELK-Stack-Fluss

ELK Stack als Protokollanalyse

- Eine separate Instanz des Stacks ElasticSearch+LogStash+Kibana wird nur auf MnT-Knoten ausgeführt.
 - Dies steht in keinem Zusammenhang mit der elastischen Suche nach Kontexttransparenz.
 - Mit ELK 7.17
- Primäre und sekundäre MNTs haben ihre eigenen separaten Instanzen von ELK.
 - Kibana ist nur auf sekundärem MNT aktiviert, wenn es verfügbar ist, und zeigt nur Daten von diesem Knoten an.
- Log Analytics ist standardmäßig deaktiviert.
- Verwendet Oracle-Ressourcen.
- Speichert Daten für maximal 7 Tage.
- Die Gesamtgröße der von Log Analytics verwendeten Daten ist auf 10 GB beschränkt.
 - Sobald eine der Beschränkungen erreicht ist, entfernt ElasticSearch die Daten.



ISE Logstash Service running 614339

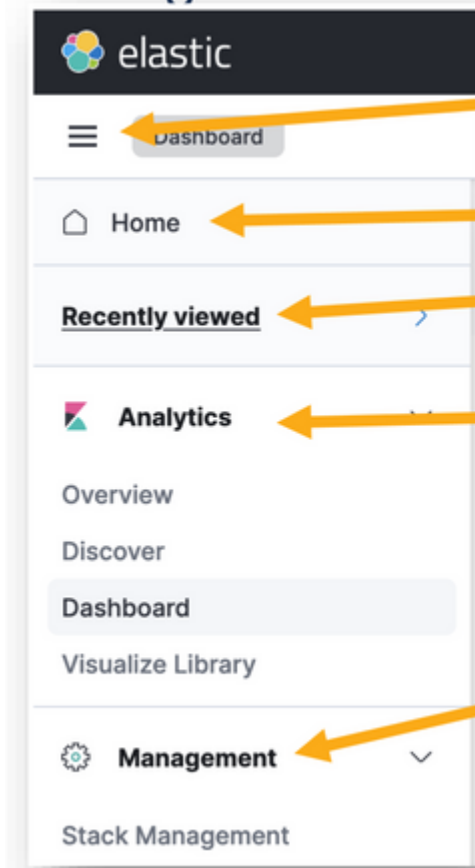
ISE Kibana Service running 616064

ISE Native IPSec Service running 75883

MFC Profiler running 651910

Navigationsmenü

Sobald die ELK-Services gestartet wurden, können Sie auf das Navigationsmenü "Elastic" zugreifen.

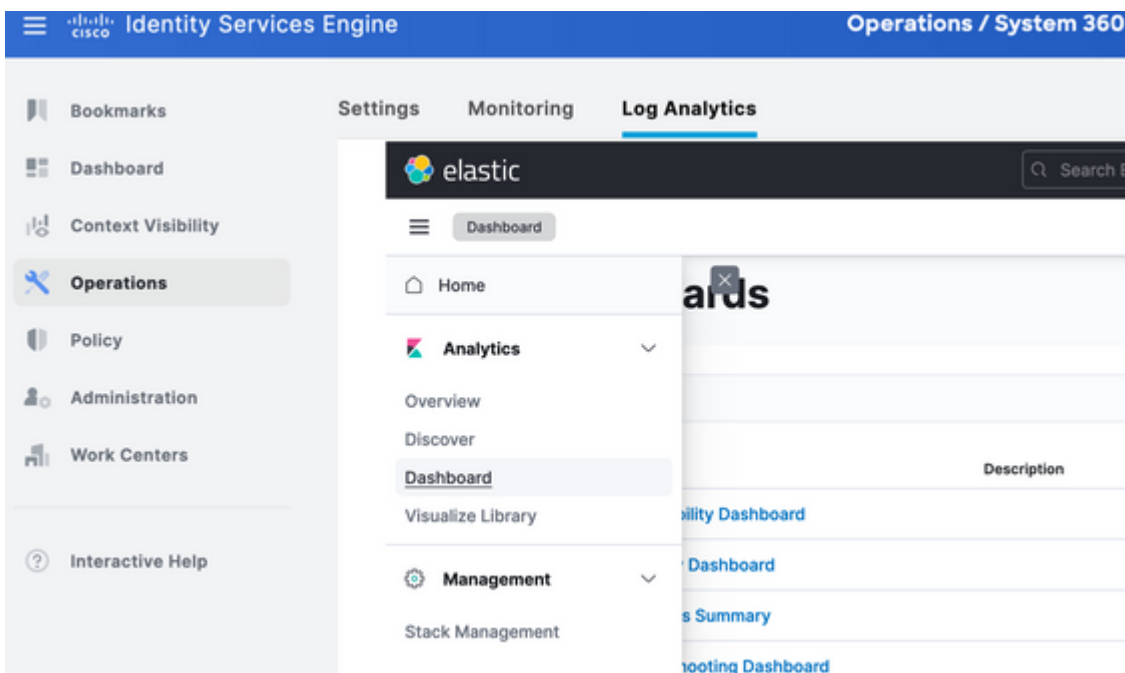


- Menu access
- Homepage for Kibana
- Recent dashboards viewed
- Configuration area for dashboards
- System settings/configuration

Navigationsmenü

Integrierte Dashboards

- Die ISE verfügt standardmäßig über integrierte Dashboards mit Daten von Radius, TACACs, Systemleistung und ISE-Überwachung.
- Auf diese Dashboards kann zugegriffen werden, indem zu Operations (Vorgänge) > Log Analytics (Protokollanalyse) navigiert wird.
 - Sobald die elastische Benutzeroberfläche geöffnet ist, klicken Sie auf das Sandwich-Menü >Analytics>Dashboards.



Integrierte Dashboards

- Verfügbare Dashboards auf der ISE 3.3

- Wählen Sie Zeitstempelfeld, log_at, log_at_timezone oder "Ich möchte keinen Zeitfilter verwenden".
- Klicken Sie dann auf "Indexmuster erstellen".

Create index pattern

Name

mnt_analytics_radius_authentication

Use an asterisk (*) to match multiple characters. Spaces and the characters , / , ? , " , < , > , | are not allowed.

Timestamp field

logged_at

Select a timestamp field for use with the global time filter.

[Show advanced settings](#)

✓ Your index pattern matches 1

mnt_analytics_radius_authentication

Rows per page: 50

× Close

Create index pattern

Index auswählen

Nach der Erstellung listet der Index alle zugehörigen Variablen auf, die später zum Erstellen von Visualisierungen verwendet werden können.

Stack Management > Index patterns > mnt_analytics_radius_authentication

mnt_analytics_radius_authentication

Time field: 'logged_at'

View and edit fields in mnt_analytics_radius_authentication. Field attributes, such as type and searchability, are base

Fields (105) Scripted fields (0) Field filters (0)

Search

Name ↑	Type	Format	Searchable
_id	_id		●
_index	_index		●
_score			

: Diese Diagramme zeigen Daten in vertikalen Balken an, sodass Werte leicht über Kategorien oder Zeitintervalle hinweg verglichen werden können.

- **Liniendiagramme:** Liniendiagramme zeigen Daten als eine Reihe von Datenpunkten an, die durch Linien verbunden sind. Sie sind nützlich, um Trends im Laufe der Zeit zu visualisieren.
- **Tortendiagramme:** Tortendiagramme stellen Daten in einem Kreisdiagramm dar, wobei jedes Segment des Kuchens eine Kategorie darstellt und die Größe des Segments seinen Anteil angibt.
- **Flächendiagramme:** Ähnlich wie Liniendiagramme zeigen Flächendiagramme auch Trends im Zeitverlauf an, füllen jedoch den Bereich unterhalb der Linien aus, wodurch die Größenordnung der Änderungen leichter erkennbar wird.
- **Heat Maps:** Heat Maps verwenden Farben, um Datenwerte in einer Matrix oder einem Raster darzustellen. Sie sind nützlich, um Konzentrationen oder Schwankungen der Daten zu zeigen.
- **Metrische Visualisierungen:** Diese zeigen einzelne numerische Werte an, z. B. Zählungen oder Durchschnittswerte. Sie werden häufig verwendet, um wichtige Leistungsindikatoren anzuzeigen.
- **Datentabellen:** Datentabellen stellen Rohdaten in Tabellenform dar, sodass Sie detaillierte Informationen anzeigen und die Daten sortieren oder filtern können.
- **Histogramme:** Histogramme teilen Daten in Behälter oder Intervalle und zeigen die Häufigkeit oder Anzahl der Datenpunkte in jedem Behälter. Sie sind nützlich, um Datenverteilungen zu verstehen.
- **Koordinatenkarten:** Diese visualisieren räumliche Daten, sodass Sie Daten auf einer Karte anzeigen und verschiedene Markierungen, Farben oder Größen verwenden können, um Datenattribute darzustellen.
- **Tag-Wolken:** Tag-Wolken zeigen die Häufigkeit von Wörtern an, wobei die Größe jedes Worts seine Bedeutung oder Häufigkeit in einem Datensatz angibt.

Navigieren Sie zu Analytics>Visualize Library und klicken Sie dann auf "Create visualization" (Visualisierung erstellen).

Visualize Library

Building a dashboard? Create and add your visualizations right from the [Dashboard application](#).

Search...

Title	Type	Description	Tags
AD Connector	Lens		
App Server	Lens		
Authentication Success Rate -markdown	Markdown		
Authentication latency Per ID -markdown	Markdown		

Visualisierung erstellen

Wählen Sie die Visualisierung Ihrer Präferenz, in diesem Beispiel ist Objektiv aus praktischen Gründen vorzuziehen.

New visualization



Lens

Create visualizations with our drag and drop editor. Switch between visualization types at any time. *Recommended for most users.*



TSVB

Perform advanced analysis of your time series data.



Custom visualization

Use Vega to create new types of visualizations. *Requires knowledge of Vega syntax.*



Aggregation based

Use our classic visualize library to create charts based on aggregations.

[Explore options](#) →

Tools



Text

Add text and images to your dashboard.

Controls



Im linken Bereich können Sie die Datenquelle oder das Elasticsearch-Indexmuster auswählen, das Sie für die Visualisierung verwenden möchten.

- **Visualisierungsbereich:** Im zentralen Bereich erstellen Sie Ihre Visualisierung, indem Sie Felder ziehen und ablegen, Diagrammtypen auswählen und Diagrammeinstellungen konfigurieren.
- **Visualisierungssymbolleiste:** Über der Zeichenfläche befindet sich eine Symbolleiste, mit der Sie die Visualisierung anpassen können, einschließlich Optionen zum Ändern von Diagrammtypen, Hinzufügen von Filtern und Konfigurieren von Diagrammeinstellungen.
- **Datenfeld:** Auf der rechten Seite können Sie auf das Datenfeld zugreifen, in dem Sie die Transformation, Aggregation und Feldeinstellungen verwalten können.
- **Layer Management:** Abhängig von der Art der Visualisierung, die Sie erstellen (z.B. Layer-Diagramme), können Sie einen Layer-Management-Bereich zur Konfiguration mehrerer Ebenen in Ihrer Visualisierung haben.
- **Vorschau:** Wenn Sie Änderungen an Ihrer Visualisierung vornehmen, wird normalerweise eine Echtzeitvorschau bereitgestellt, sodass Sie sehen können, wie Ihr Diagramm mit den aktuellen Einstellungen aussieht.
- **Visualisierungseinstellungen:** Abhängig vom ausgewählten Diagrammtyp können Sie auf bestimmte Einstellungen für diesen Visualisierungstyp zugreifen, z. B. Achsenkonfiguration, Farbschemata und Beschriftungen.
- **Einstellungen für Interaktivität:** Sie können Interaktionen und Aktionen zu Ihrer Visualisierung hinzufügen, sodass Benutzer Daten filtern oder zu anderen Teilen Ihrer Kibana Dashboards navigieren können.
- **Speichern und gemeinsam nutzen:** Oben auf der Objektivoberfläche gibt es normalerweise Optionen, um Ihre Visualisierung zu speichern, sie einem Dashboard hinzuzufügen oder sie für andere freizugeben.

Search KQL Today

Index selection **Diagram style** **Time range**

mnt_analytics_radius_aut... Donut

Search field names

Filter by type 0

Records

Available fields

There are no available fields that contain data.


Try:

- Extending the time range

> Empty fields 114

> Meta fields 3

Drop some fields here to start



Lens is a new tool for creating visualization

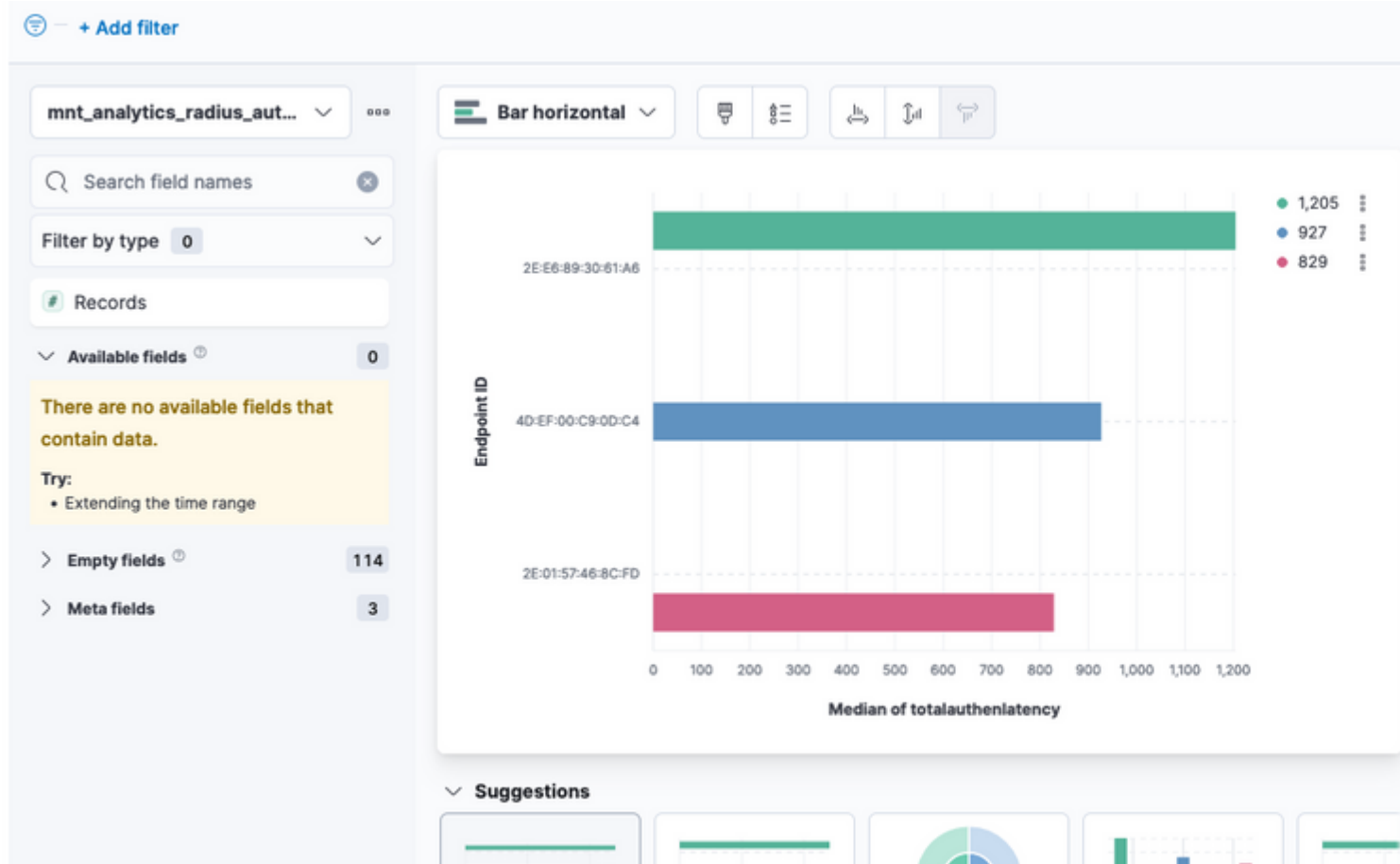
[Make requests and give feedback](#)

Suggestions

Current visualization

Linsenvisualisierung

Aufgrund der Cisco Bug-ID [CSCwh48057](#) werden auf der linken Seite keine verfügbaren Felder angezeigt. Auf der rechten Seite können Sie jedoch die erforderlichen Felder und den Diagrammstil auswählen. Da die Authentifizierungslatenz ein Thema von gemeinsamem Interesse ist, wird in diesem Beispiel der Graph erstellt, um die Authentifizierungslatenz im Vergleich zur Endpunkt-ID darzustellen.



```
admin#show logging application ise-logstash/logstash.log  
admin#show logging application mnt-la-elasticsearch/mnt-la-elasticsearch.log
```

Zugehörige Informationen

[ISE 3.3 - Administratorhandbuch](#)

[Kibana-Dokumentation](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.