Comprendere Log Analytics-ELK Stack su ISE

Sommario

Introduzione

Questo documento descrive i componenti dello stack ELK integrati di Cisco Identity Services Engine (ISE) da 3.3 a System 360 Log Analytics.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Identity Service Engine
- Stack ELK

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- ISE 3.3

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

System 360 include Monitoring e Log Analytics.

La **funzionalità Monitoraggio** consente di monitorare un'ampia gamma di statistiche di sistema e applicazioni e gli indicatori di prestazioni chiave (KPI) di tutti i nodi di una distribuzione da una console centralizzata. Gli indicatori KPI sono utili per ottenere informazioni dettagliate sullo stato complessivo dell'ambiente del nodo. Le statistiche offrono una rappresentazione semplificata delle configurazioni di sistema e dei dati specifici dell'utilizzo.

Log Analytics fornisce un sistema di analisi flessibile per un'analisi approfondita dell'autenticazione, dell'autorizzazione e dell'accounting degli endpoint (AAA) e per l'analisi dei dati di syslog. È inoltre possibile analizzare il riepilogo dello stato di salute e gli stati del processo di Cisco ISE. È possibile generare report simili al report dei contatori Cisco ISE e del riepilogo dello stato.

Stack ELK

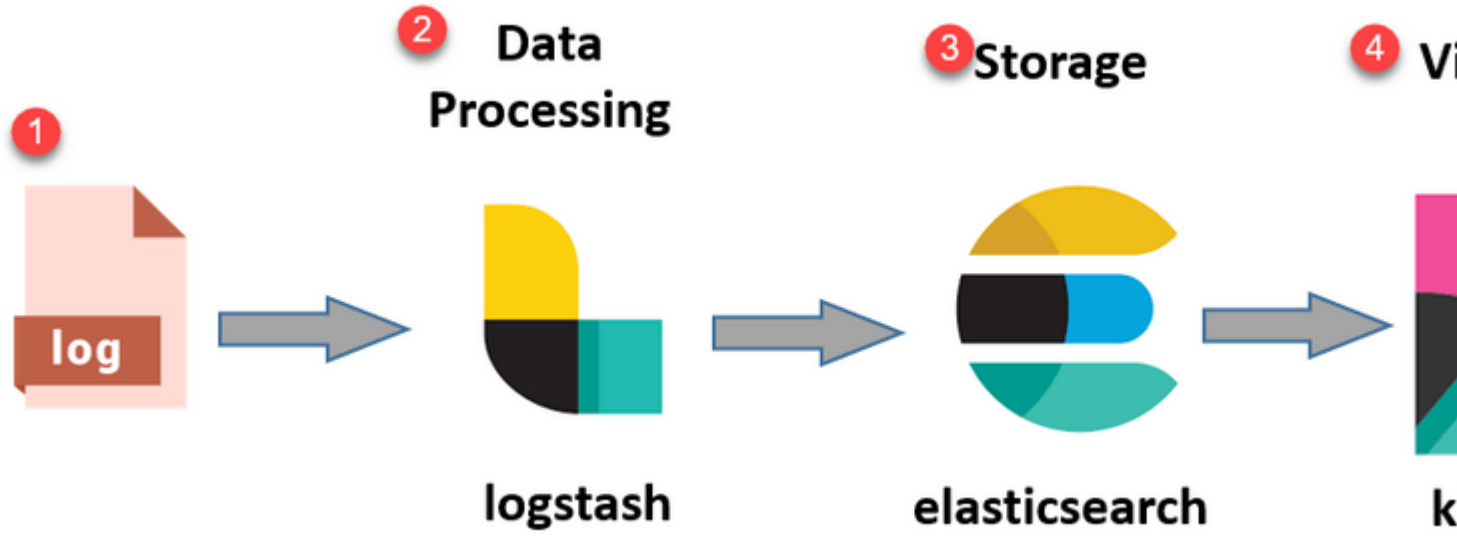
ELK Stack è un popolare stack di software open source utilizzato per la raccolta, l'elaborazione e la visualizzazione di grandi volumi di dati. Sta per Elasticsearch, Logstash e Kibana.

- **Elasticsearch**: Elasticsearch è un motore di ricerca e analisi distribuito. È progettato per archiviare, ricercare e analizzare grandi volumi di dati in modo rapido e quasi in tempo reale. Utilizza un linguaggio di query basato su JSON ed è altamente scalabile.

- **Logstash**: Logstash è una pipeline di elaborazione dei dati che acquisisce, elabora e trasforma i dati da più origini. È in grado di analizzare e arricchire i dati, rendendoli più strutturati e adatti per l'analisi. Logstash supporta un'ampia gamma di origini di input e destinazioni di output.

- **Kibana**: Kibana è una piattaforma di visualizzazione dei dati che lavora con Elasticsearch. Consente agli utenti di creare dashboard interattivi, grafici e visualizzazioni per esplorare e comprendere i dati archiviati in Elasticsearch. L'interfaccia di Kibana semplifica le query e la visualizzazione dei dati.

Se combinati, questi componenti costituiscono un potente stack per la gestione e l'analisi di diversi tipi di dati, dai file di log alle metriche e altro ancora, fornendo al contempo funzionalità di visualizzazione per dare un senso alle informazioni.

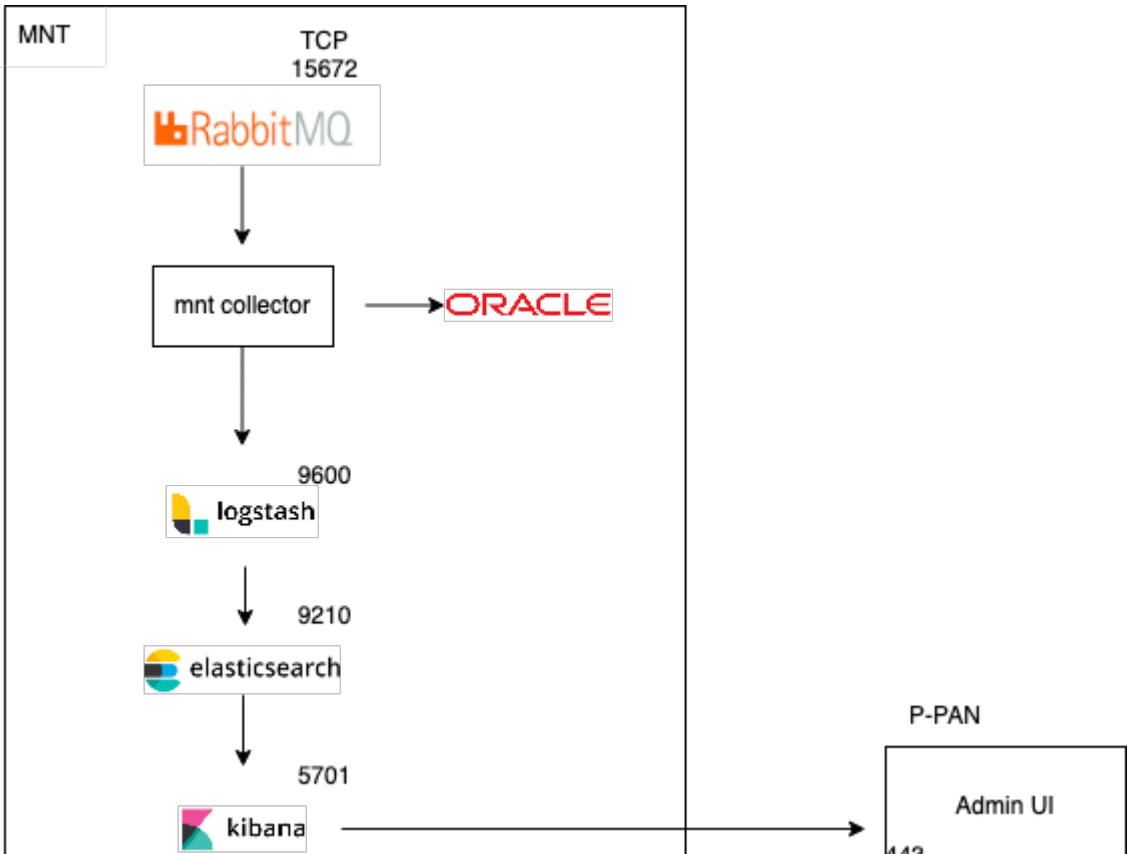


Flusso ELK stack

ELK Stack as Log Analytics

- Un'istanza separata dello stack ElasticSearch+LogStash+Kibana è in esecuzione solo sui nodi MnT.
  - Questo non ha alcuna correlazione con Elasticsearch di Context-Visibility.
  - ELK 7.17 in esecuzione

- Le MNT primarie e secondarie hanno istanze separate di ELK.
  - Kibana è abilitato solo sul MNT secondario se disponibile, visualizzando solo i dati da questo nodo.
- Log Analytics è disabilitato per impostazione predefinita.
- Utilizza le risorse Oracle.
- Memorizza fino a 7 giorni di dati.
- Le dimensioni totali dei dati utilizzati da Log Analytics sono limitate a 10 GB.
  - Una volta raggiunto uno qualsiasi dei limiti, ElasticSearch elimina i dati.



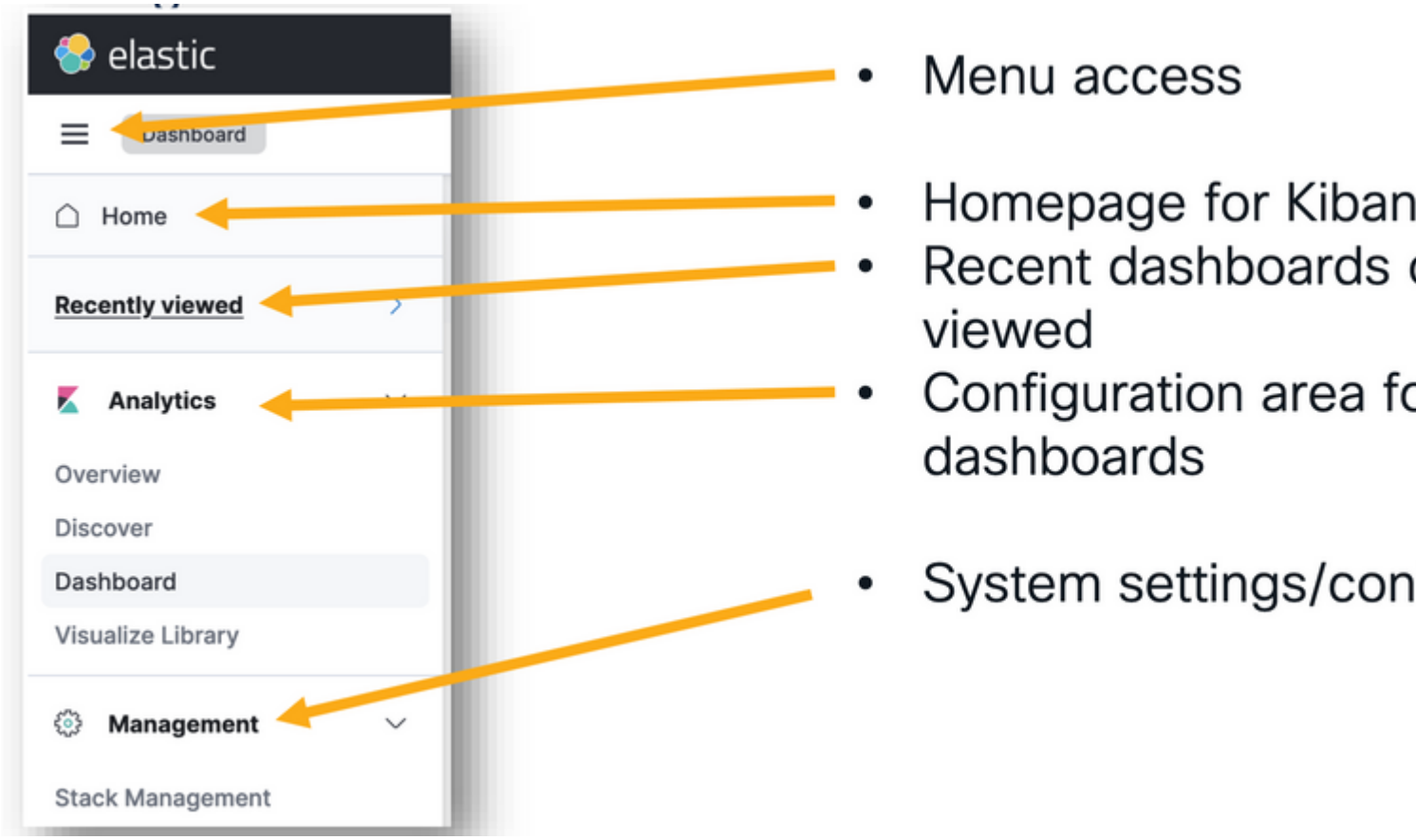
```
ISE Logstash Service running 614339


ISE Kibana Service running 616064


ISE Native IPSec Service running 75883
MFC Profiler running 651910
```

Menu di navigazione

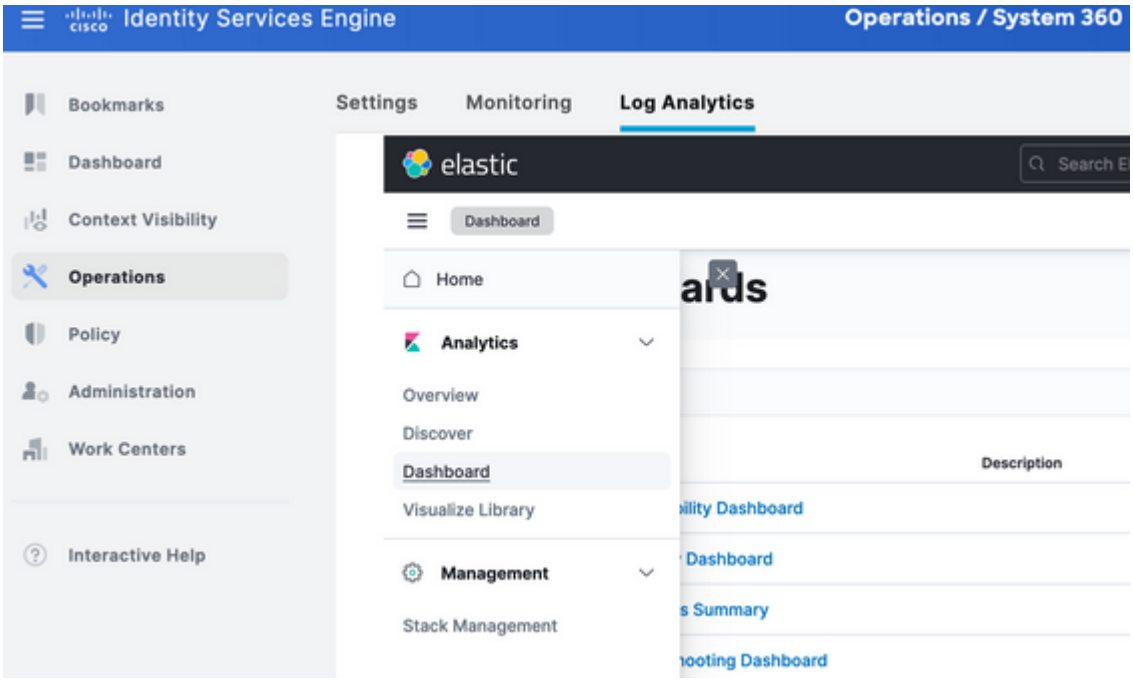
Una volta avviati i servizi ELK, è possibile accedere al menu di navigazione Elastic.



Menu di navigazione

Dashboard incorporati

- Per impostazione predefinita, ISE dispone di dashboard integrati con dati provenienti da Radius, TACAC, prestazioni del sistema e visibilità ISE.
- È possibile accedere a questi dashboard passando a Operazioni>Analisi log.
  - Una volta aperta l'interfaccia utente elastica, fare clic su menu sandwich > Analisi > Dashboard.



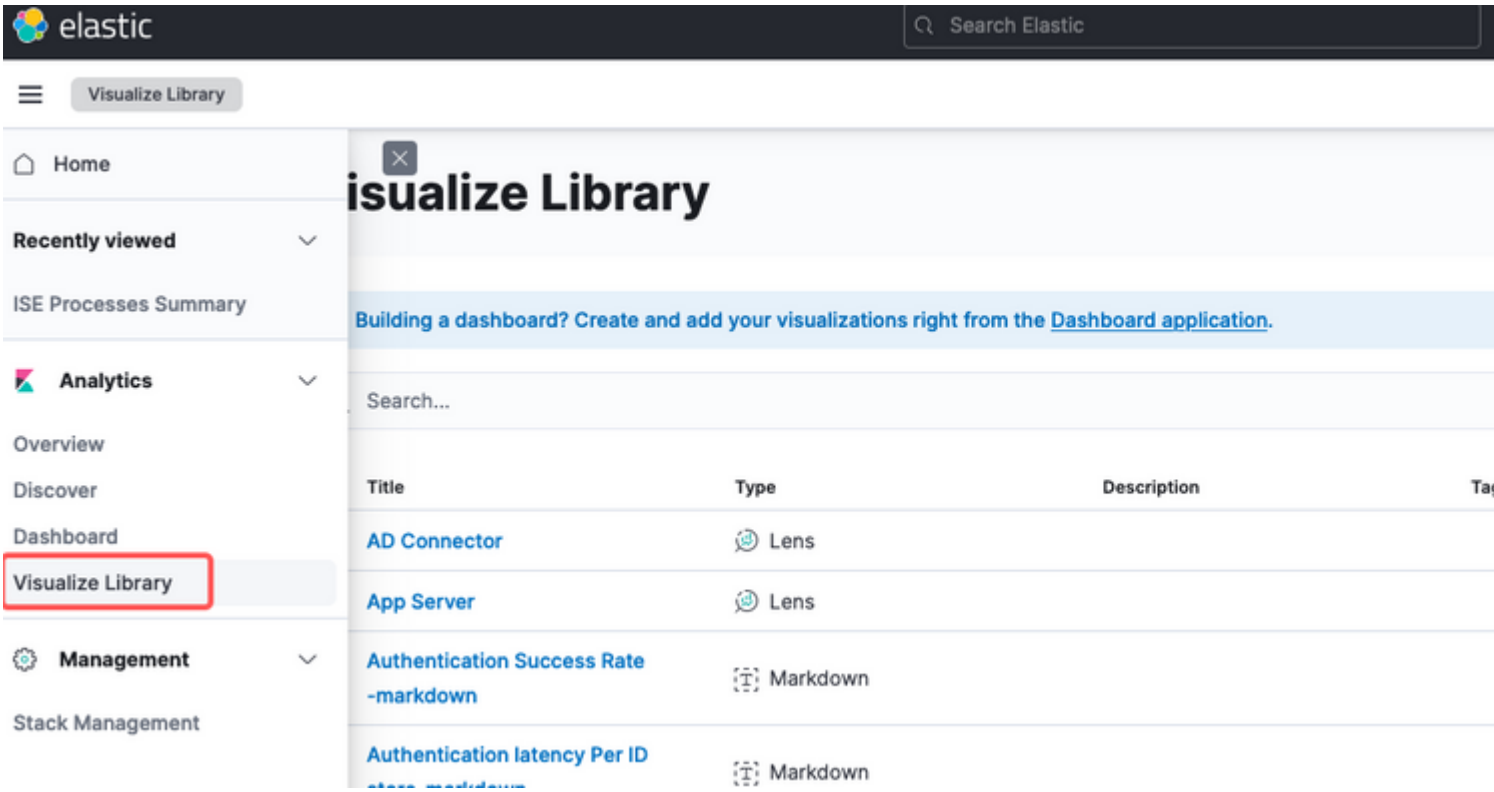
Dashboard incorporati

- Dashboard disponibili su ISE 3.3

: visualizzano i dati in barre verticali, semplificando il confronto dei valori tra categorie o intervalli di tempo.

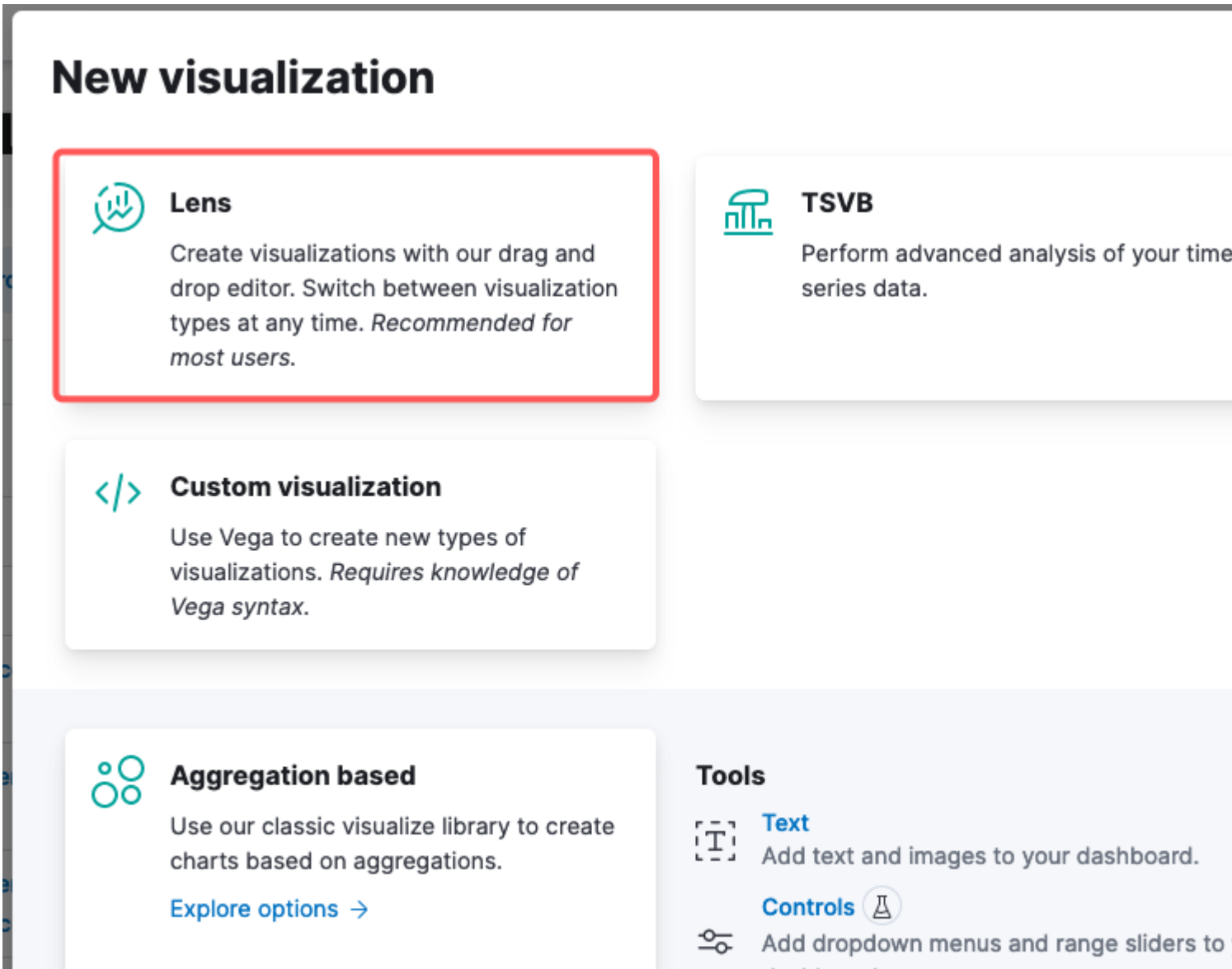
- **Grafici a linee**: nei grafici a linee i dati vengono visualizzati come una serie di coordinate collegate da linee. Sono utili per visualizzare le tendenze nel tempo.
- **Grafici a torta**: i grafici a torta rappresentano i dati in un grafico circolare, in cui ogni segmento della torta rappresenta una categoria e le dimensioni del segmento ne indicano le proporzioni.
- **Grafici ad area**: simili ai grafici a linee, anche i grafici ad area mostrano le tendenze nel tempo, ma riempiono l'area sotto le linee, rendendo più facile vedere l'entità delle modifiche.
- **Mappe termiche**: le mappe termiche utilizzano i colori per rappresentare i valori dei dati in una matrice o griglia. Sono utili per mostrare concentrazioni o variazioni nei dati.
- **Visualizzazioni metriche**: visualizzano singoli valori numerici, ad esempio conteggi o medie. Vengono spesso utilizzati per visualizzare indicatori di prestazioni chiave (KPI).
- **Tabelle di dati**: le tabelle di dati presentano dati non elaborati in formato tabulare, consentendo di visualizzare informazioni dettagliate e di ordinare o filtrare i dati.
- **Istogrammi**: gli istogrammi dividono i dati in raccoglitori o intervalli e visualizzano la frequenza o il conteggio dei dati in ciascun raccoglitore. Sono utili per comprendere le distribuzioni dei dati.
- **Mappe coordinate**: consentono di visualizzare i dati geospaziali e di utilizzare diversi marcatori, colori o dimensioni per rappresentare gli attributi dei dati.
- **Tag cloud**: le tag cloud visualizzano le frequenze delle parole, con le dimensioni di ogni parola che ne indicano l'importanza o la frequenza in un dataset.

Passare ad Analisi>Libreria di visualizzazione, quindi fare clic su "Crea visualizzazione".



Crea visualizzazione

Selezionare la visualizzazione della preferenza, in questo esempio Lente è preferibile per praticità.



: nel pannello a sinistra, è possibile selezionare l'origine dati o il modello di indice di ricerca elastica da utilizzare per la visualizzazione.

- **Area di visualizzazione**: l'area centrale è quella in cui è possibile creare la visualizzazione trascinando e rilasciando i campi, selezionando i tipi di grafico e configurando le impostazioni del grafico.
- **Barra degli strumenti Visualizzazione**: sopra l'area di lavoro è disponibile una barra degli strumenti che consente di personalizzare la visualizzazione, incluse le opzioni per la modifica dei tipi di grafico, l'aggiunta di filtri e la configurazione delle impostazioni del grafico.

- **Pannello dati**: sul lato destro, è possibile accedere al pannello "Dati", che consente di gestire la trasformazione dei dati, l'aggregazione e le impostazioni dei campi.

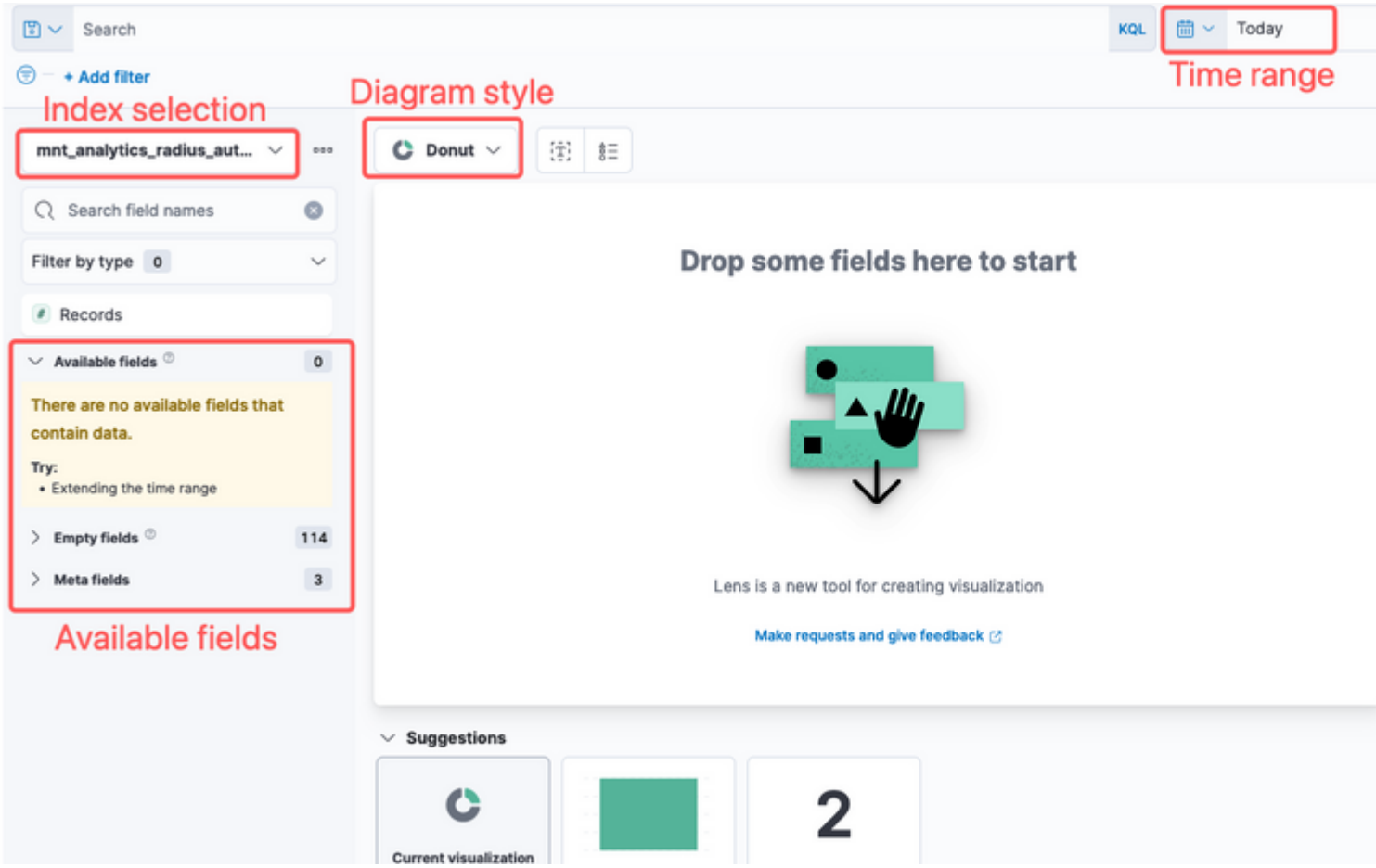
- **Gestione livelli**: a seconda del tipo di visualizzazione che si sta creando (ad esempio, i grafici a livelli), è possibile che sia disponibile un'area di gestione dei livelli per la configurazione di più livelli nella visualizzazione.

- **Anteprima:** quando si apportano modifiche alla visualizzazione, in genere viene fornita un'anteprima in tempo reale che consente di verificare l'aspetto del grafico con le impostazioni correnti**.**

- **Impostazioni visualizzazione**: a seconda del tipo di grafico selezionato, è possibile accedere a impostazioni specifiche per il tipo di visualizzazione, ad esempio la configurazione degli assi, le combinazioni di colori e le etichette.

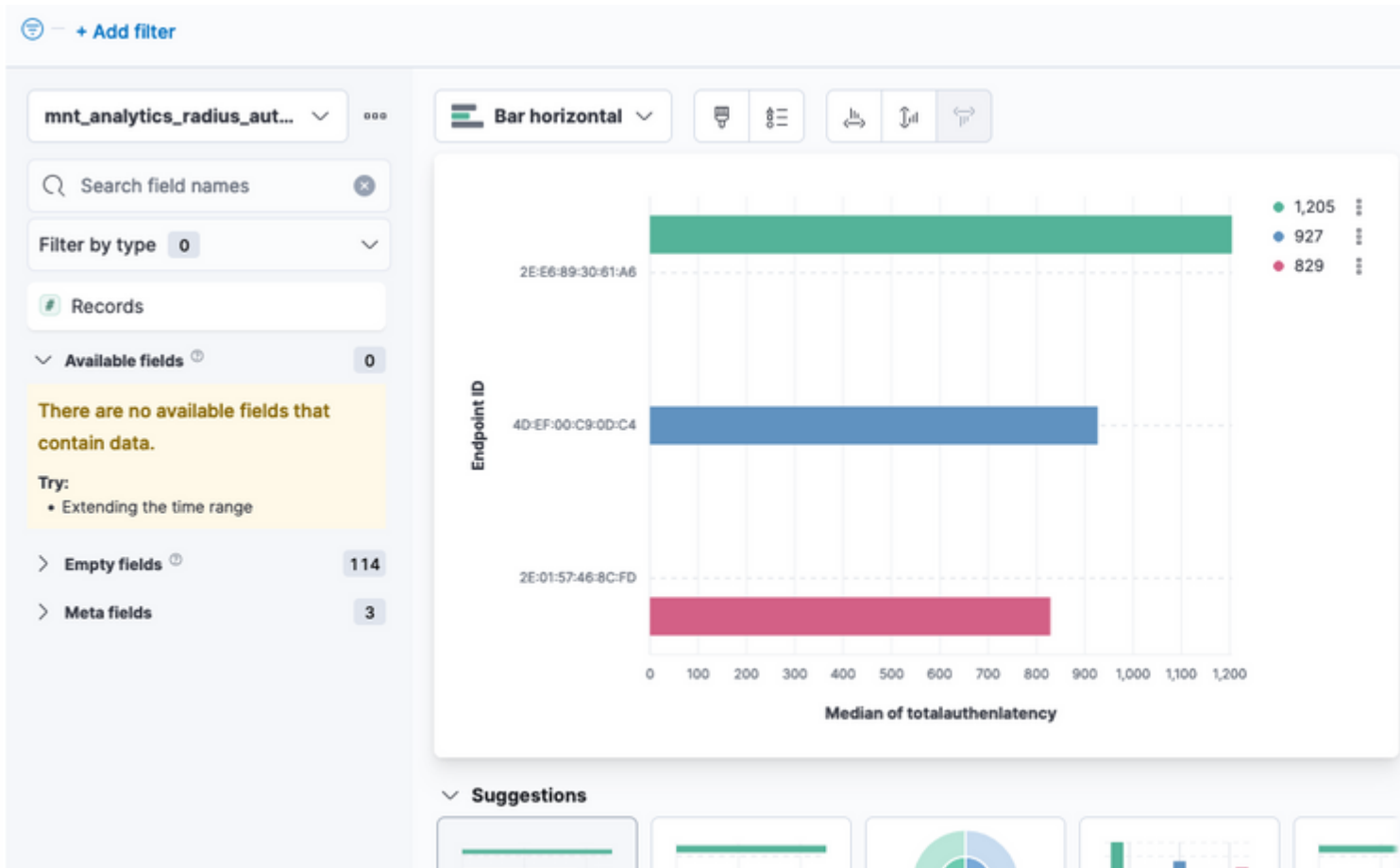
- **Impostazioni interattività**: è possibile aggiungere interazioni e azioni alla visualizzazione, consentendo agli utenti di filtrare i dati o di passare ad altre parti dei dashboard Kibana.

- **Salva e condividi**: nella parte superiore dell'interfaccia dell'obiettivo sono in genere disponibili opzioni per salvare la visualizzazione, aggiungerla a un dashboard o condividerla con altri utenti.



Visualizzazione dell'obiettivo

A causa dell'ID bug Cisco CSCwh48057, nel pannello sinistro non vengono visualizzati i campi disponibili per l'uso. Tuttavia, dal lato destro è possibile selezionare i campi richiesti più lo stile del diagramma. In questo esempio, poiché la latenza di autenticazione è un argomento di interesse comune, il grafico viene creato per visualizzare la latenza di autenticazione rispetto all'ID dell'endpoint.



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

Informazioni correlate

Guida per l'amministratore di ISE 3.3

Documentazione su Kibana

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).