فهم حزمة تحليلات السجل على ISE

المحتويات

المقدمة

يصف هذا المستند مكون مكدس ELK المضمن في Cisco Identity Services Engine (ISE) 3.3 من خلال تحليلات سجل النظام 360.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- Cisco ISE
- إلكاتالوج

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى Cisco ISE 3.3.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

يتضمن System 360 المراقبة وتحليلات السجل.

تتيح لك ميزة المراقبة إمكانية مراقبة مجموعة كبيرة من إحصائيات التطبيقات والنظام ومؤشرات الأداء الرئيسية (KPI) لجميع العقد في عملية نشر من وحدة تحكم مركزية. تعد مؤشرات الأداء الأساسي (KPI) مفيدة للحصول على رؤية متعمقة حول الصحة العامة لبيئة العقدة. توفر الإحصائيات تمثيلا مبسطا لتكوينات النظام والبيانات الخاصة باالستخدام.

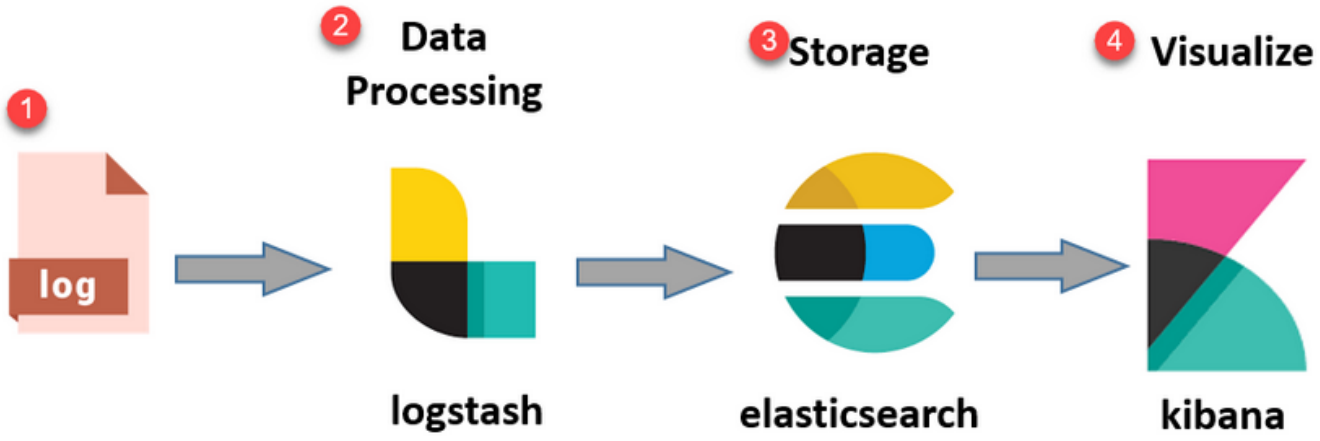
توفر تحليلات السجل نظام تحليلات مرن للتحليل المتعمق لمصادقة نقطة النهاية والتفويض والمحاسبة (AAA) وبيانات syslog للتصنيف. يمكنك أيضا تحليل ملخص صحة Cisco ISE وحالات المعالجة. يمكنك إنشاء تقارير مماثلة لـ Cisco ISE Counters وتقرير ملخص الصحة.

إلك ستاك

إن مكدس ELK عبارة عن مجموعة شائعة من البرامج مفتوحة المصدر تستخدم لجمع ومعالجة وعرض كميات كبيرة من البيانات. وهي ترمز إلى Elasticsearch، Logstash، و Kibana.

- Elasticsearch: Elasticsearch هو محرك تحليلات وبحث موزع. وهو مصمم لتخزين كميات كبيرة من البيانات والبحث عنها وتحليلها بسرعة وفي الوقت الفعلي تقريبا. وهو يستخدم لغة إستفسار تستند إلى JSON وهو قابل للتطوير بدرجة كبيرة.
- Logstash: Logstash هو مسار معالجة البيانات الذي يقوم بإدخال البيانات ومعالجتها وتحويلها من مصادر متعددة. فهو قادر على تحليل وإثراء البيانات، وجعلها أكثر تنظيما ومناسبة للتحليل. يدعم Logstash مجموعة واسعة من مصادر الإدخال وجهات الإخراج.
- كيبانا: كيبانا هي منصة عرض للبيانات تعمل مع Elasticsearch. وهو يسمح للمستخدمين بإنشاء لوحات معلومات ومخططات ورسومات بيانية ومرئيات تفاعلية لاستكشاف البيانات المخزنة في Elasticsearch وفهمها. تجعل واجهة كيبانا من السهل االستعالم عن البيانات وتخيلها.

وعند الجمع بين هذه المكونات، فإنها تشكل مكدس قوي إلدارة وتحليل أنواع مختلفة من البيانات، من ملفات السجل إلى القياسات وغير ذلك، مع توفير إمكانات المحاكاة الافتراضية لاستخالص المعلومات.

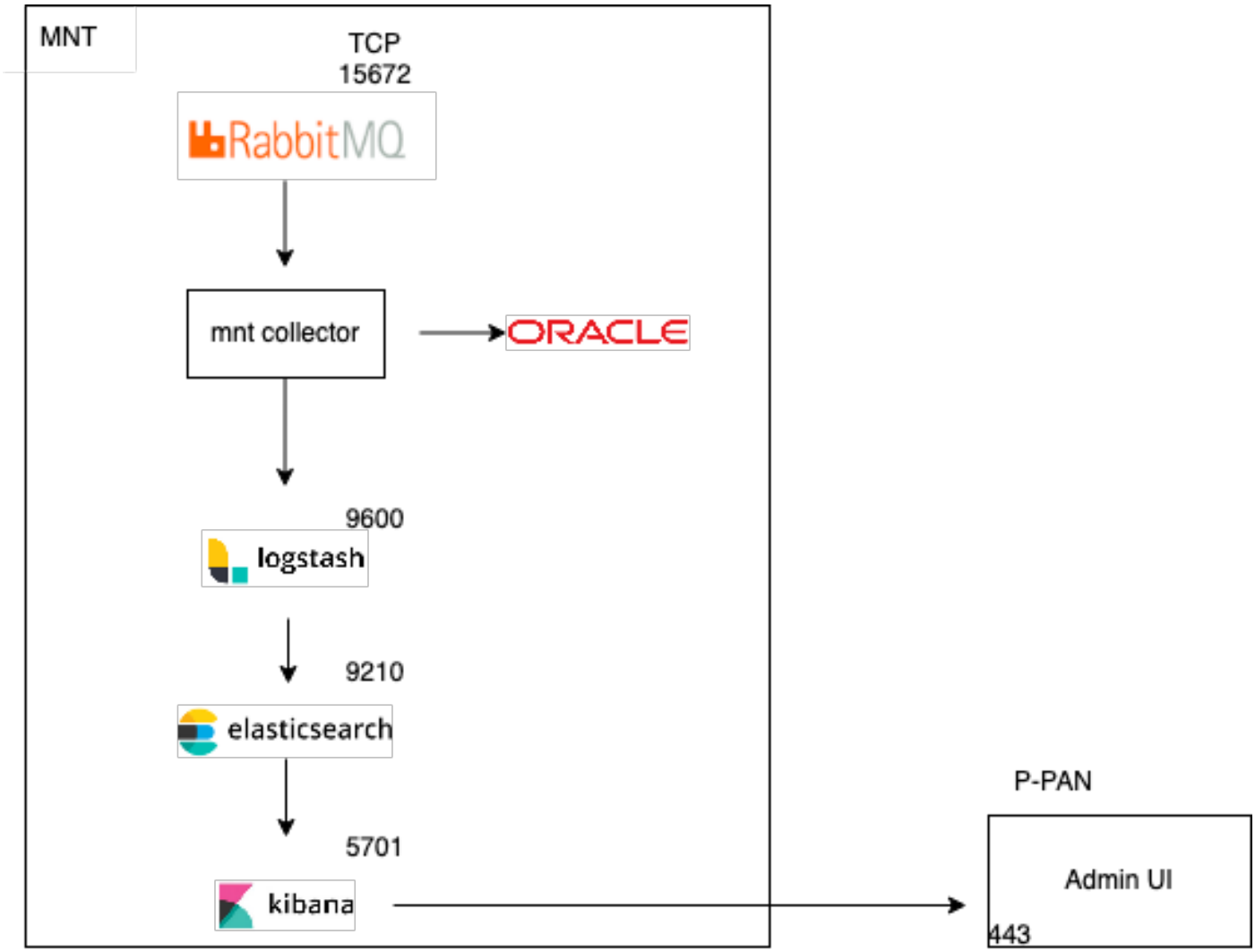


تدفق مكدس ELK

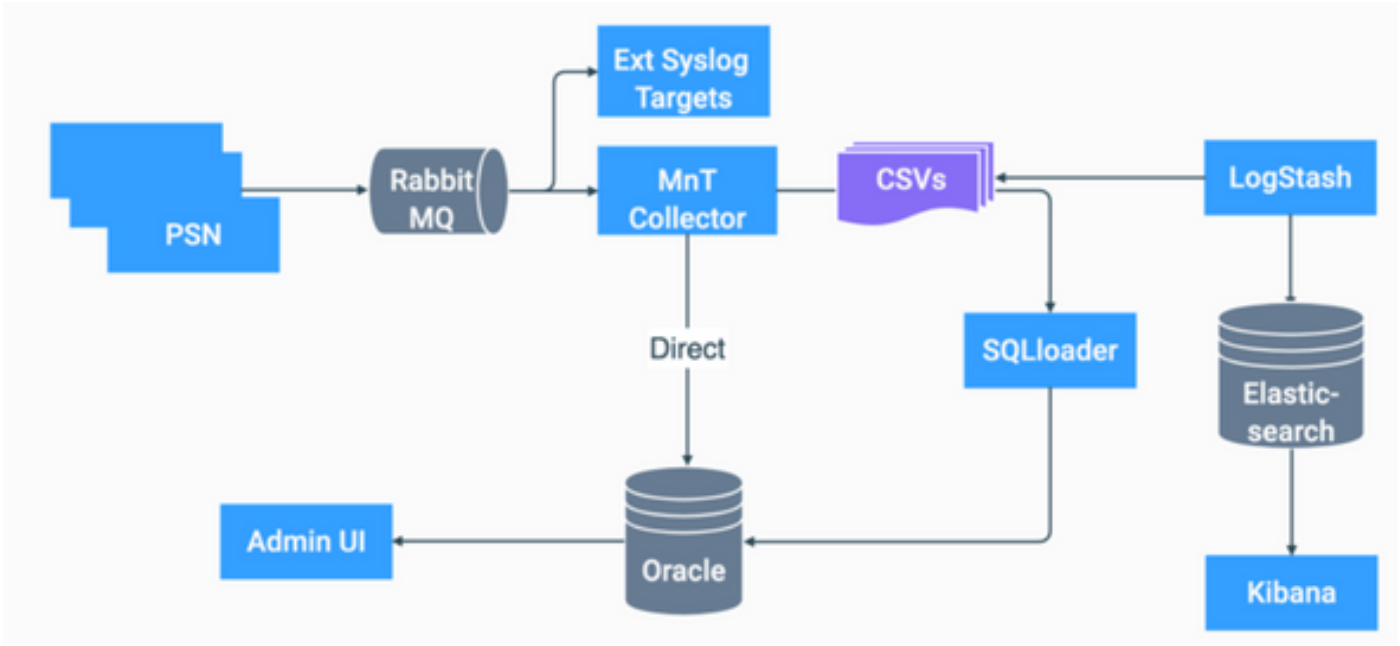
حزمة ELK كتحليلات سجل

- يوجد مثيل منفصل لمكدس FlexibleSearch+LogStash+Kibana قيد التشغيل على عقد MnT فقط.
  - لا يحتوي هذا على أي ارتباط بـ Elasticsearch لـ Context-Visibility.
  - جار ELK 7.17

- وللشبكات المتوسطة والثانوية حالات منفصلة خاصة بها من هذا النوع.
  - لا يتم تمكين Kibana إلا على MNT الثانوي إذا كان متوفرا، مما يعرض البيانات من هذه العقدة فقط.
- تم تعطيل تحليلات السجل بشكل افتراضي.
- يستهلك موارد Oracle.
- تخزين بيانات بحد أقصى 7 أيام.
- يقتصر الحجم الإجمالي للبيانات التي تستهلكها تحليلات السجل على 10 جيجابايت.
  - بمجرد الوصول إلى أي من الحدود، يقوم FlexibleSearch بإزالة البيانات.



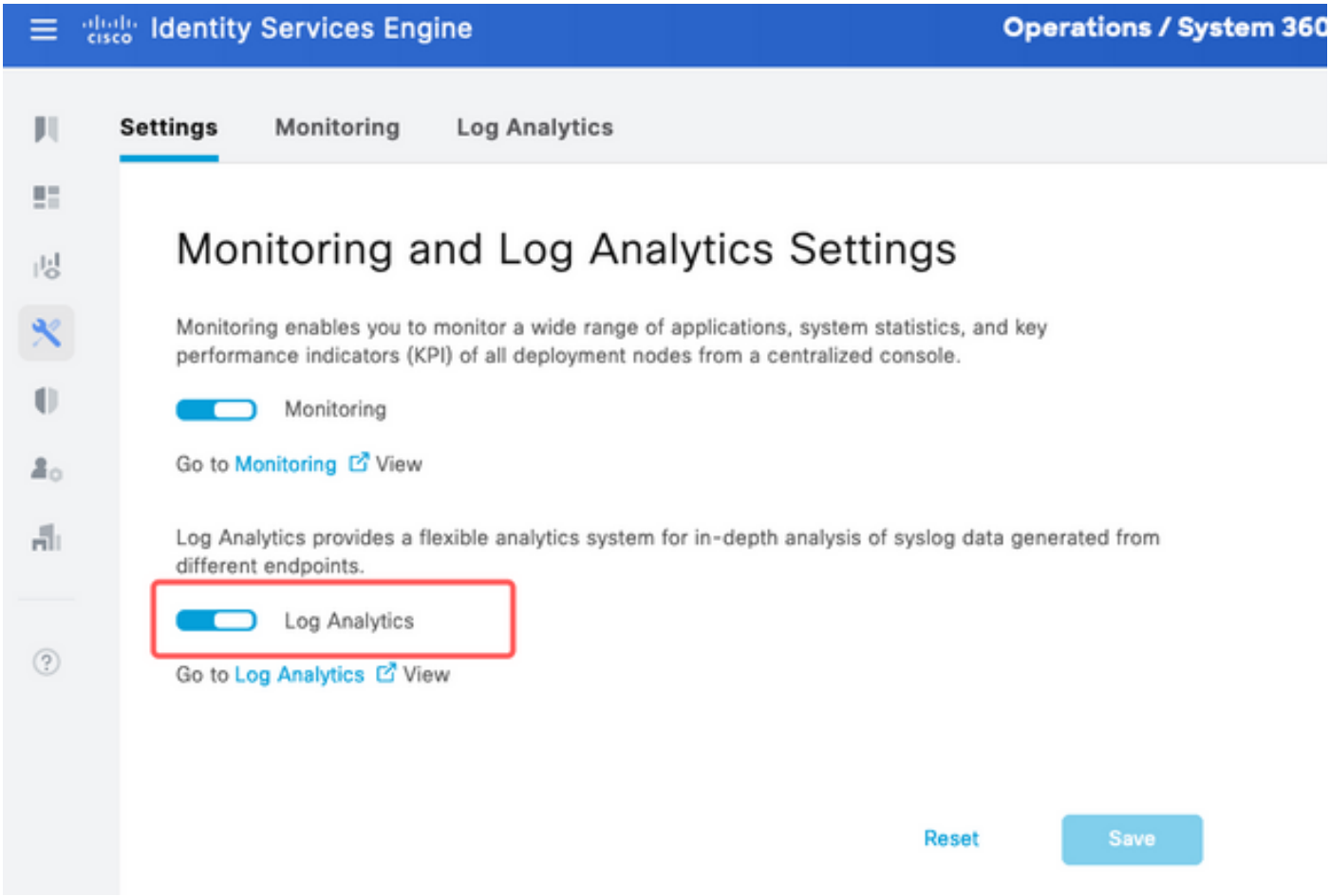
تدفق ELK كتحليلات سجل



مخطط انسيابي ل ELK في ISE

تمكين تحليلات السجل

تم تعطيل تحليلات السجل بشكل افتراضي على ISE. لتمكينها، انتقل إلى Operations > System 360 > Settings كما هو موضح في الصورة.



تمكين تحليلات السجل

يستغرق ISE حوالي دقيقة لتهيئة مكدس ELK، يمكنك التحقق من الحالة باستخدام show app stat ise.

بالإضافة إلى ذلك، يمكنك التحقق من حالة الحاوية من الجذر.

<#root>

admin#show application status ise

```
ISE PROCESS NAME STATE PROCESS ID
--------------------------------------------------------------------
Database Listener running 7708
Database Server running 132 PROCESSES
Application Server running 551493
Profiler Database running 14281
ISE Indexing Engine running 553168
AD Connector running 41413
M&T Session Database running 26017
```

```
M&T Log Processor running 33547
Certificate Authority Service running 41230
EST Service running 659568
SXP Engine Service disabled
TC-NAC Service disabled
PassiveID WMI Service disabled
PassiveID Syslog Service disabled
PassiveID API Service disabled
PassiveID Agent Service disabled
PassiveID Endpoint Service disabled
PassiveID SPAN Service disabled
DHCP Server (dhcpd) disabled
DNS Server (named) disabled
ISE Messaging Service running 10937
ISE API Gateway Database Service running 13294
ISE API Gateway Service running 586762
ISE pxGrid Direct Service running 637606
Segmentation Policy Service disabled
REST Auth Service disabled
SSE Connector disabled
Hermes (pxGrid Cloud Agent) disabled
McTrust (Meraki Sync Service) disabled
ISE Node Exporter running 44422
ISE Prometheus Service running 47890
ISE Grafana Service running 51094
```

ISE MNT LogAnalytics Elasticsearch running 611684

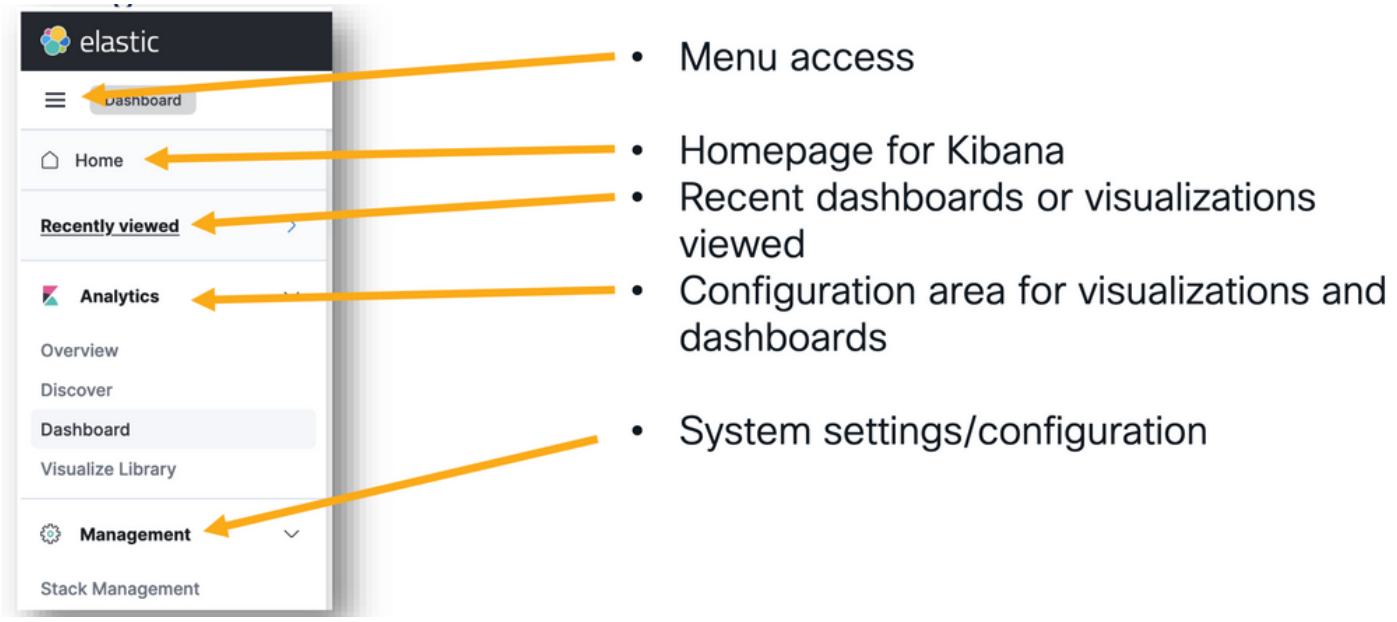
ISE Logstash Service running 614339

ISE Kibana Service running 616064

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

قائمة التنقل

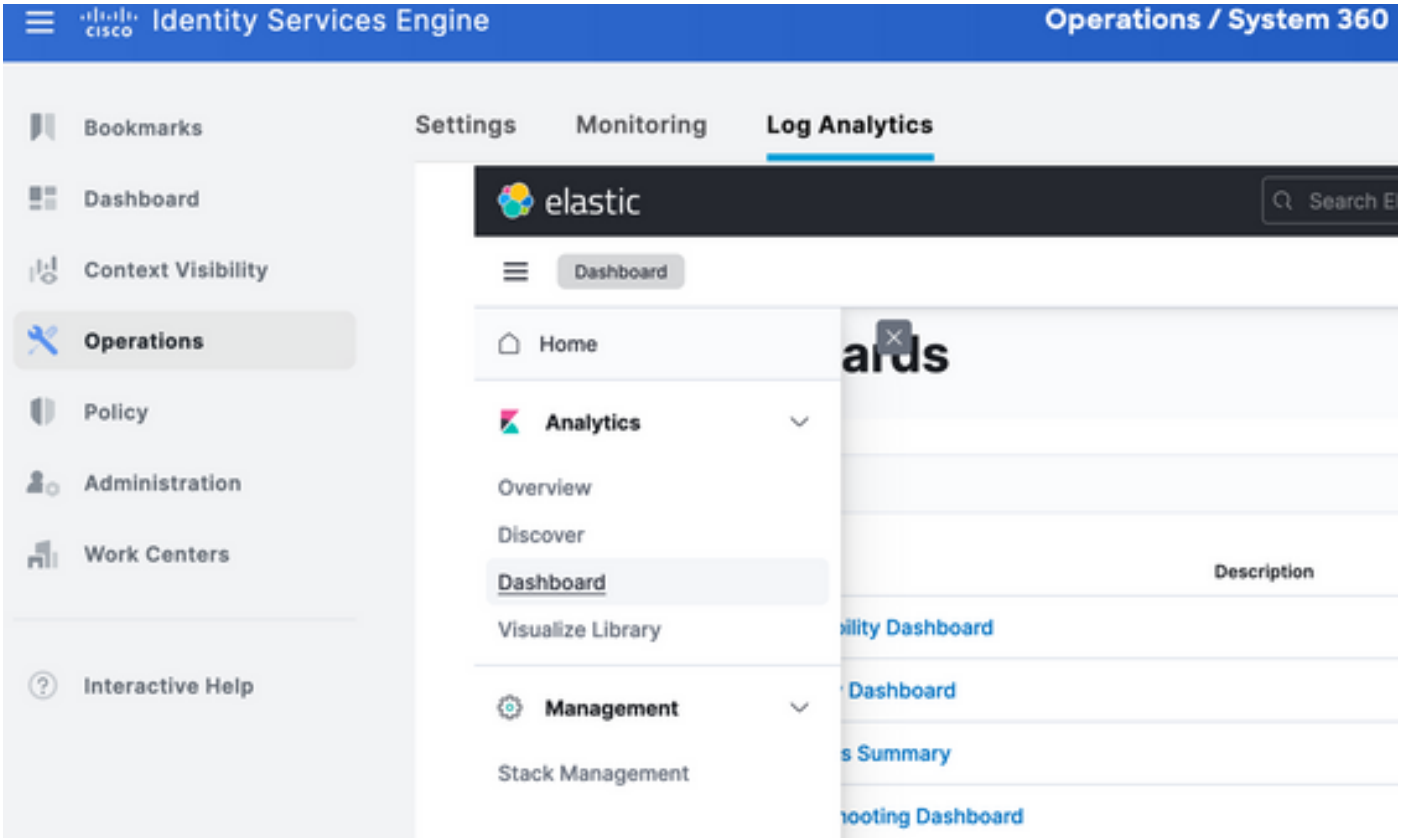
بمجرد بدء تشغيل خدمات ELK، يمكنك الوصول إلى قائمة التنقل المرنة.



قائمة التنقل

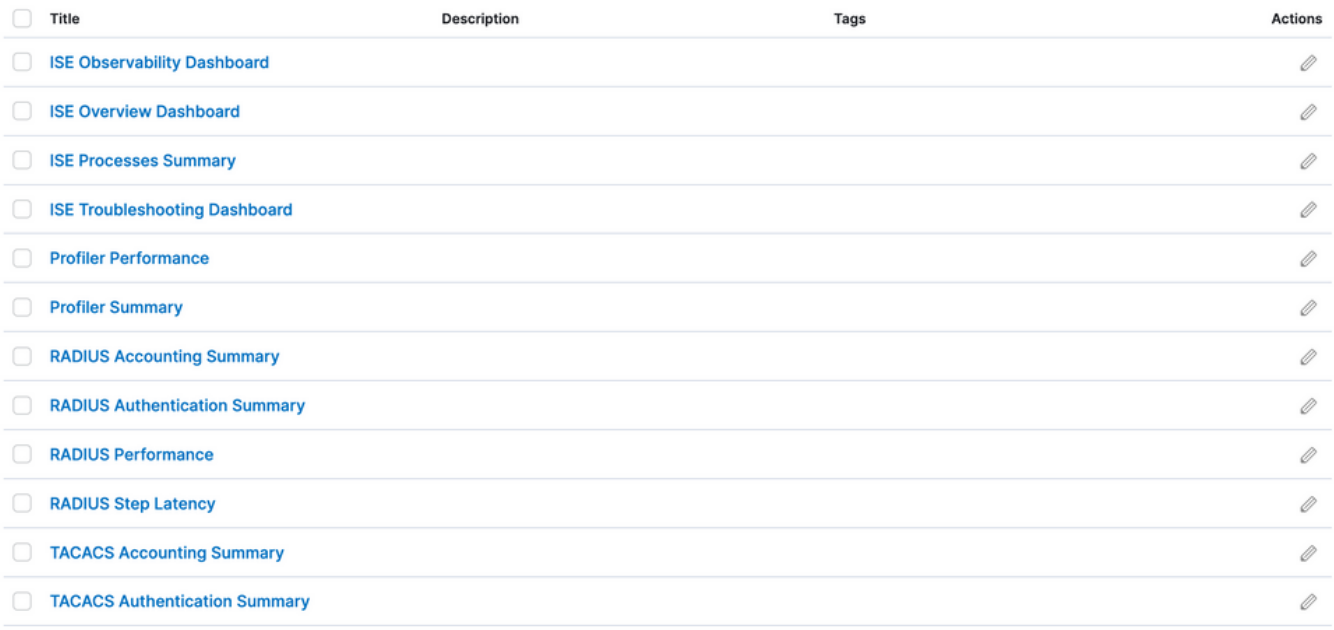
لوحات معلومات مدمجة

- بشكل افتراضي، يحتوي ISE على لوحات معلومات مدمجة تحتوي على بيانات من RADIUS و TACACS وأداء النظام وإمكانية ملاحظة ISE.
- يمكن الوصول إلى لوحات المعلومات هذه من خلال الانتقال إلى Operations > Log Analytics .
  - بمجرد فتح واجهة المستخدم المرنة، انقر فوق Sandwich Menu > Analytics > Dashboards .



لوحات معلومات مدمجة

- لوحات المعلومات المتوفرة على ISE 3.3.



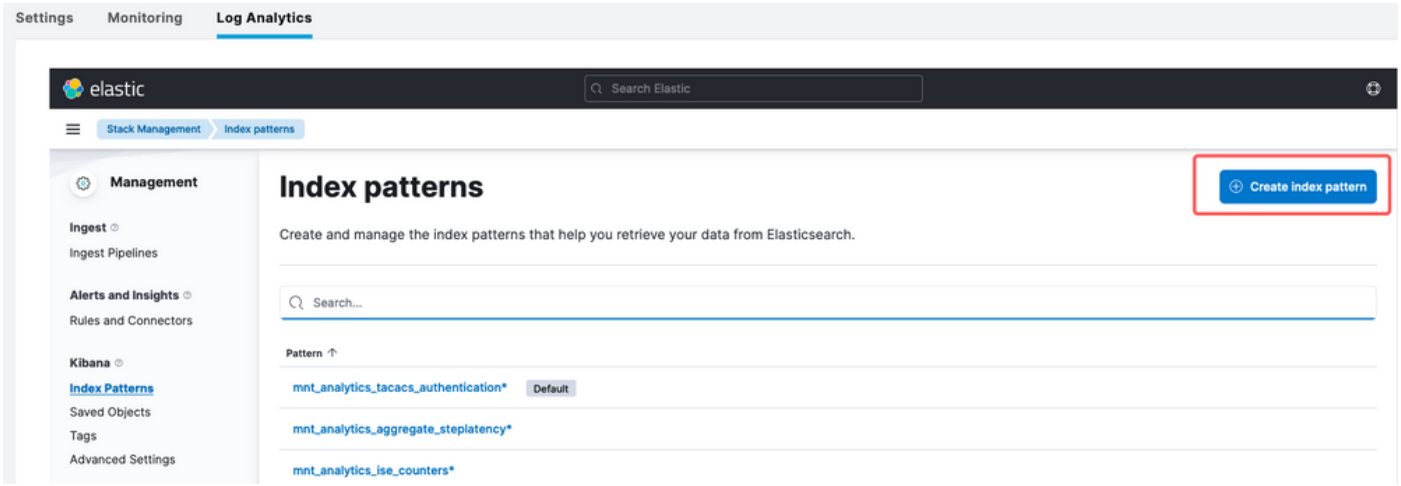
لوحات معلومات تحليلات سجل ISE 3.3

إنشاء لوحات معلومات جديدة

الخطوة 1. إنشاء أنماط فهرس (مصدر بيانات)

وفي كيبانا، فإن "أنماط الفهرسة" هي أشكال تتيح لك تحديد كيفية تفاعل كيبانا مع مؤشر أو أكثر من مؤشرات Elasticsearch.

انتقل إلى Management > Stack Management > Kibana > Index Patterns، ثم انقر Create Index Pattern كما هو موضح في الصورة.



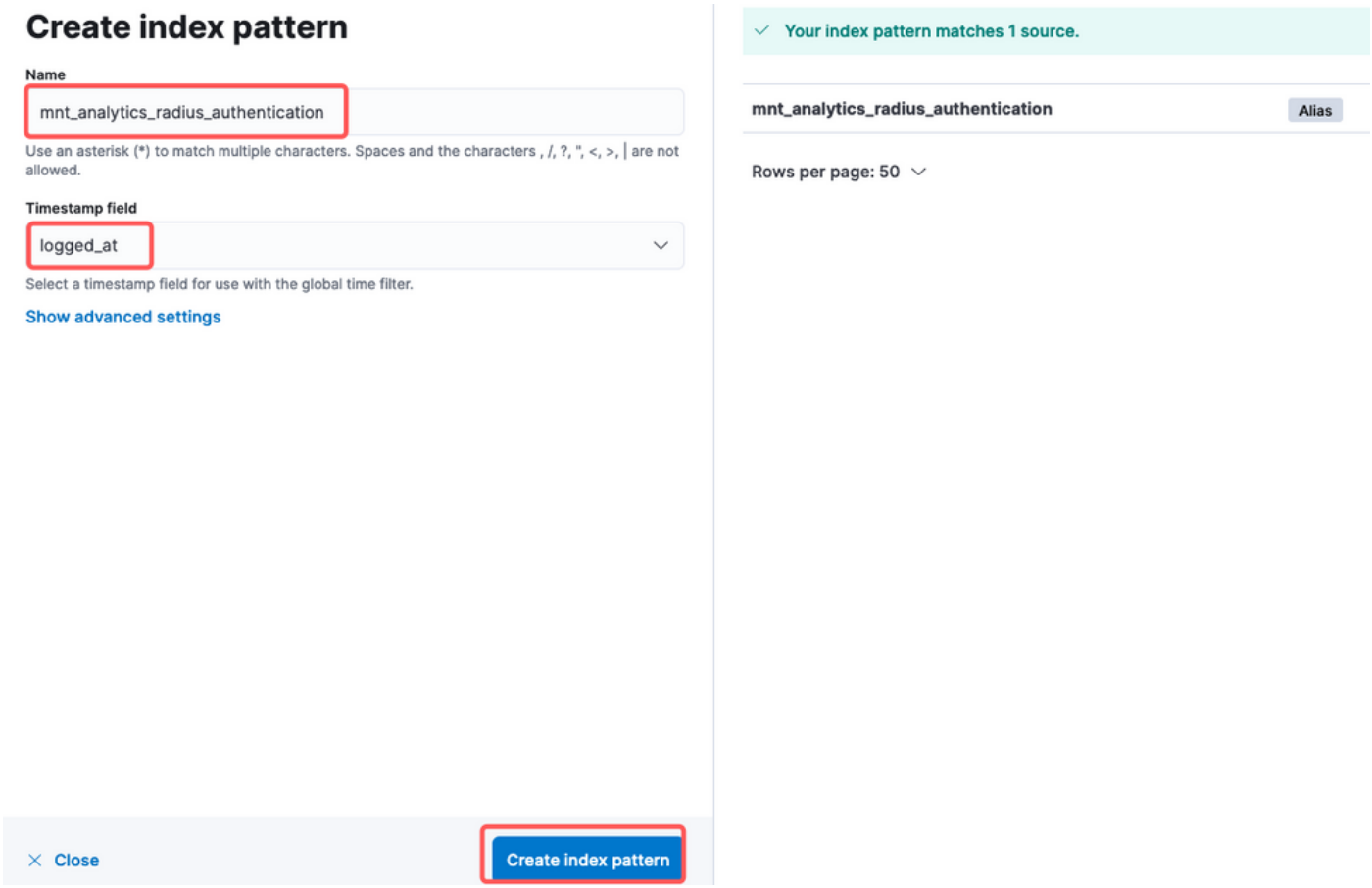
إنشاء نقش فهرس

يظهر الإطار التالي قائمة بكافة الفهارس المتوفرة على ISE.

- اكتب اسم الفهرس الذي تهتم به، ويمكن أن يكون تطابق تام أو حرف بدل باستخدام *.
- حدد حقل الطابع الزمني أو logging_at أو logging_at_timezone أو "لا أريد إستخدام عامل

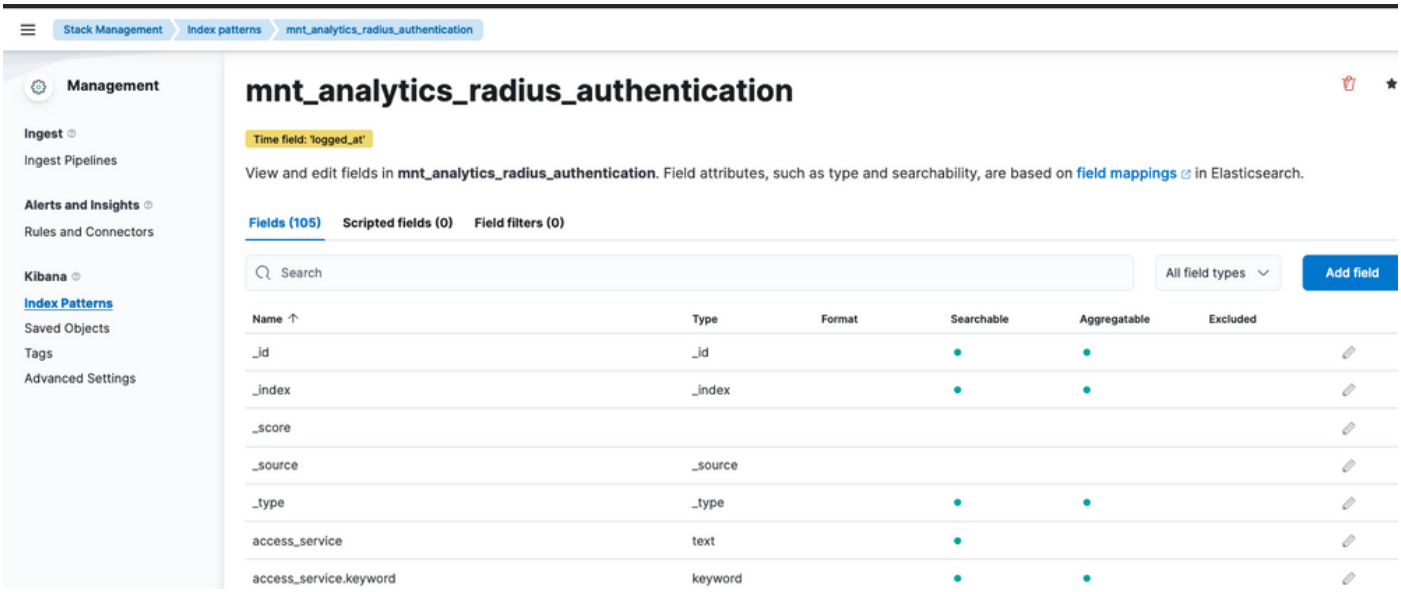
تصفية الوقت".

- ثم انقر Create index pattern.



تحديد فهرس

بمجرد إنشائها، يسرد الفهرس كل المتغيرات المرتبطة التي يمكن إستخدامها لاحقا لإنشاء المرئيات.



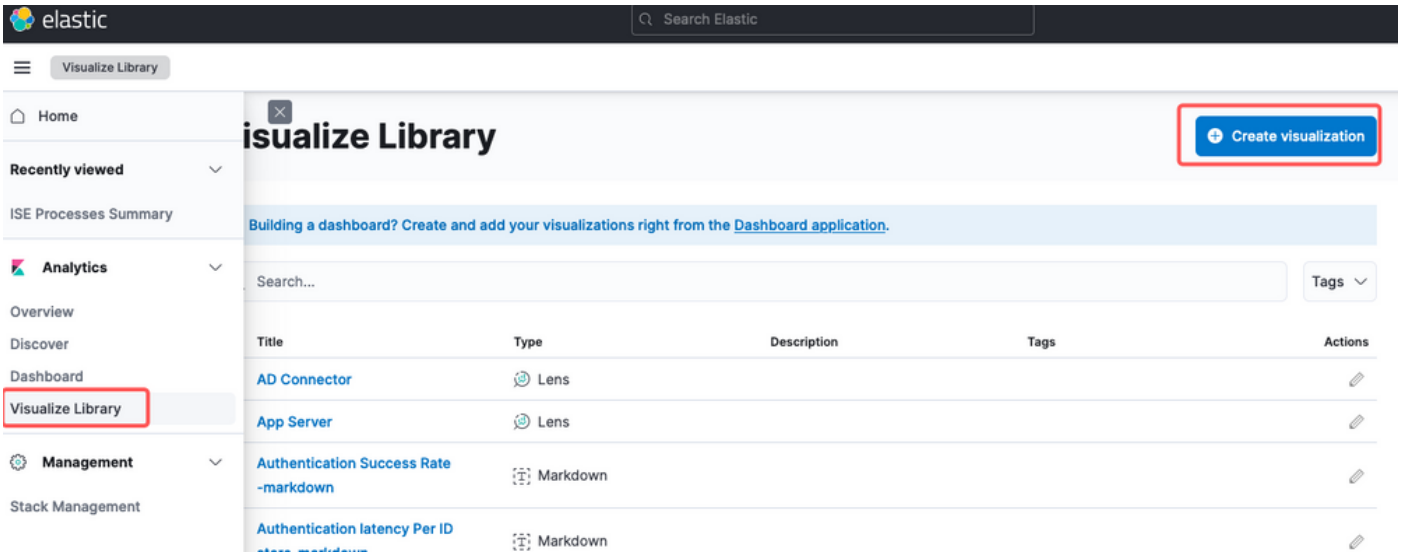
متغيرات الفهرس

الخطوة 2. إنشاء مرئيات

وفي كيبانا، تمثل "المرئيات" تمثيلا رسوميا لبياناتك. إنها تتيح لك أخذ البيانات المخزنة في Elasticsearch وتحويلها إلى مخططات ورسوم بيانية ومخططات ذات معنى لتسهيل الفهم والتحليل. هذه بعض الأنواع الشائعة من المرئيات التي يمكنك إنشاءها:

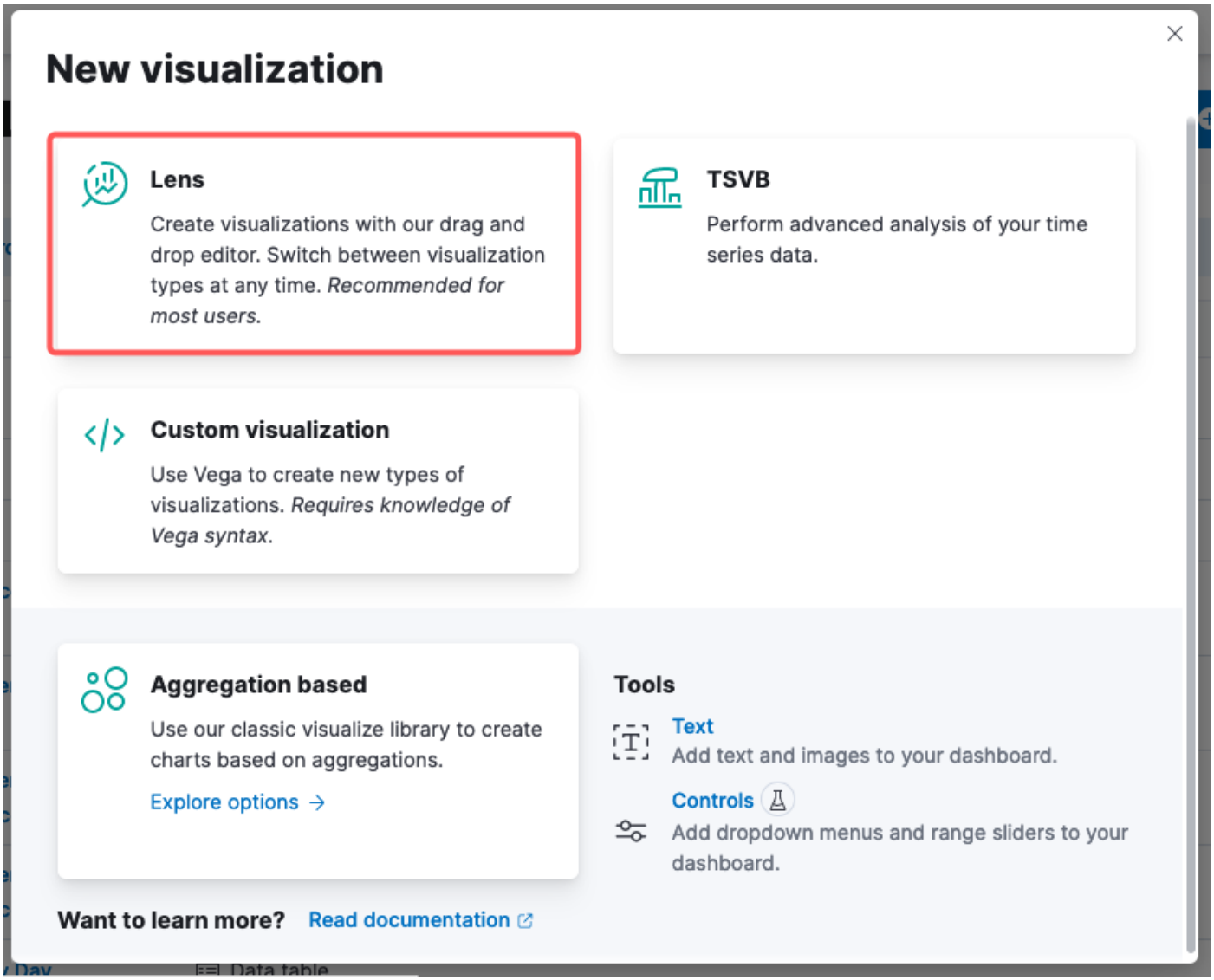
- العدسة: إنشاء مرئيات باستخدام محرر سحب وإفلات. موصى به.
- المخططات الشريطية: تعرض هذه البيانات في أشرطة رأسية، مما يسهل مقارنة القيم عبر الفئات أو الفواصل الزمنية.
- المخططات الخطية: تعرض المخططات الخطية البيانات كسلسلة من نقاط البيانات المتصلة بالخطوط. وهي مفيدة لتصور الاتجاهات بمرور الوقت.
- المخططات الدائرية: تمثل المخططات الدائرية البيانات في رسم بياني دائري، حيث يمثل كل مقطع من المخطط الدائري فئة وحجم المقطع الذي يشير إلى تناسبه.
- المخططات المساحية: على غرار المخططات الخطية، تظهر المخططات المساحية أيضا الاتجاهات بمرور الوقت، ولكنها تملأ المساحة تحت الأسطر، مما يسهل رؤية مقدار التغييرات.
- خرائط الحرارة: تستخدم خرائط الحرارة الألوان لتمثيل قيم البيانات في مصفوفة أو شبكة. وهي مفيدة لإظهار التركيزات أو التباينات في البيانات.
- المرئيات المترية: تعرض هذه المرئيات قيما رقمية مفردة، مثل أعداد الأرقام أو المتوسطات. وغالبا ما تستخدم هذه المؤشرات لإظهار مؤشرات الأداء الرئيسية.
- جداول البيانات: تقدم جداول البيانات بيانات أولية في شكل جدولي، مما يتيح لك مشاهدة معلومات تفصيلية وترتيب البيانات أو تصفيتها.
- الرسوم البيانية: تقسم الرسوم البيانية البيانات إلى سدادات أو فواصل وتعرض تردد أو عدد نقاط البيانات في كل حاوية. وهي مفيدة لفهم عمليات توزيع البيانات.
- خرائط الإحداثيات: تقوم هذه بعرض البيانات الجيوفضائية، مما يتيح لك عرض البيانات على خريطة واستخدام علامات، ألوان، أو أحجام مختلفة لتمثيل خصائص البيانات.
- Tag Cloud: تعرض السحب ذات علامات التمييز ترددات الكلمات، حيث يشير حجم كل كلمة إلى أهميتها أو ترددها في مجموعة بيانات.

انتقل إلى Analytics > Visualize Library، ثم انقر فوق Create Visualization كما هو موضح في الصورة.



إنشاء مرئيات

حدد مرئيات تفضيلاتك، في هذا المثال، يفضل العدسة على الواقعية.



تحديد نوع المرئيات

Kibana Lens، تتألف عناصر التنقل من:

- تحديد مصدر البيانات: في اللوحة اليسرى، يمكنك تحديد مصدر البيانات أو نقش فهرس Elasticsearch الذي تريد إستخدامه لمشاهدتك.
- Visual Canvas: المنطقة المركزية هي المكان الذي تبني فيه تصورك من خلال سحب الحقول وإسقاطها، وتحديد أنواع المخططات، وتكوين إعدادات المخطط.
- شريط أدوات العرض: يمكنك البحث عن شريط أدوات في أعلى اللوحة، يتيح لك تخصيص تصورك، بما في ذلك خيارات لتغيير أنواع المخطط وإضافة مرشحات وتكوين إعدادات المخطط.

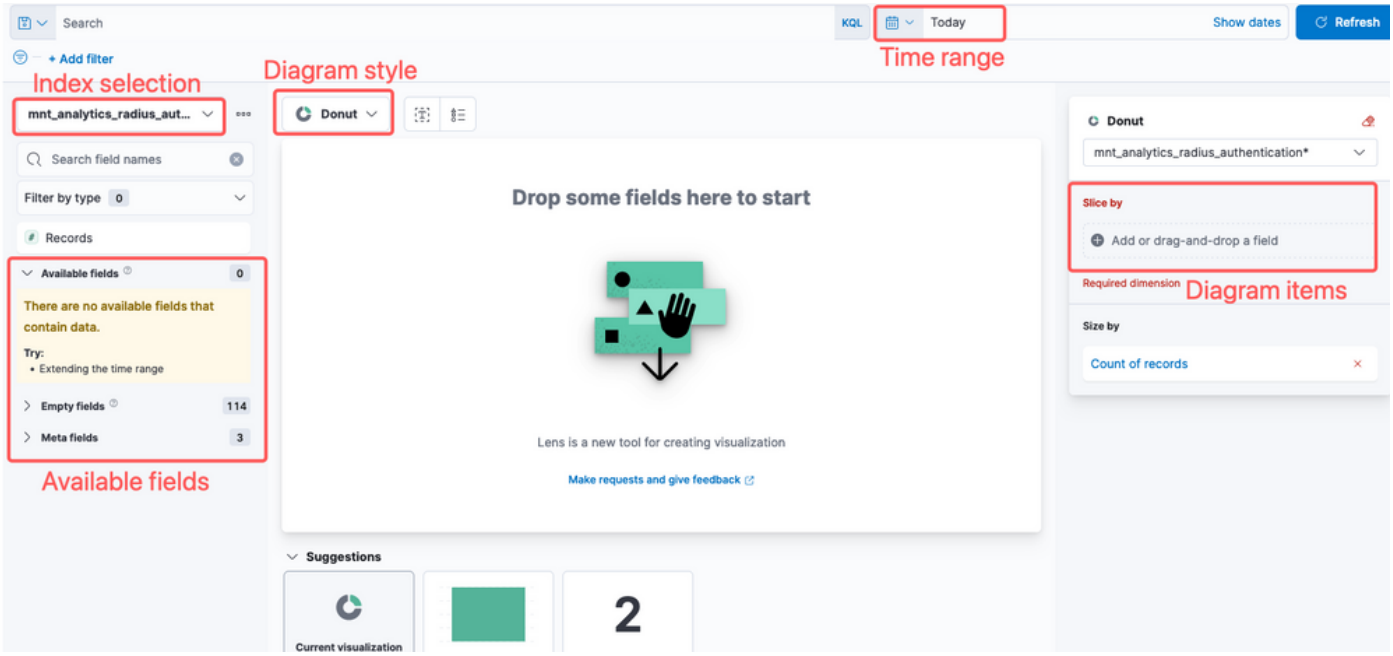
- لوحة البيانات: في الجانب الأيمن، يمكنك الوصول إلى لوحة "البيانات"، والتي تتيح لك إدارة تحويل البيانات، والتجميع، وإعدادات الحقل.

- إدارة الطبقة: طبقا لنوع المرئيات التي تقوم بإنشائها (على سبيل المثال، المخططات ذات الطبقات)، يمكنك الحصول على منطقة إدارة طبقة لتكوين طبقات متعددة في مرآتك.

- معاينة: عند إجراء تغييرات على المرئيات، يتم توفير معاينة في الوقت الحقيقي

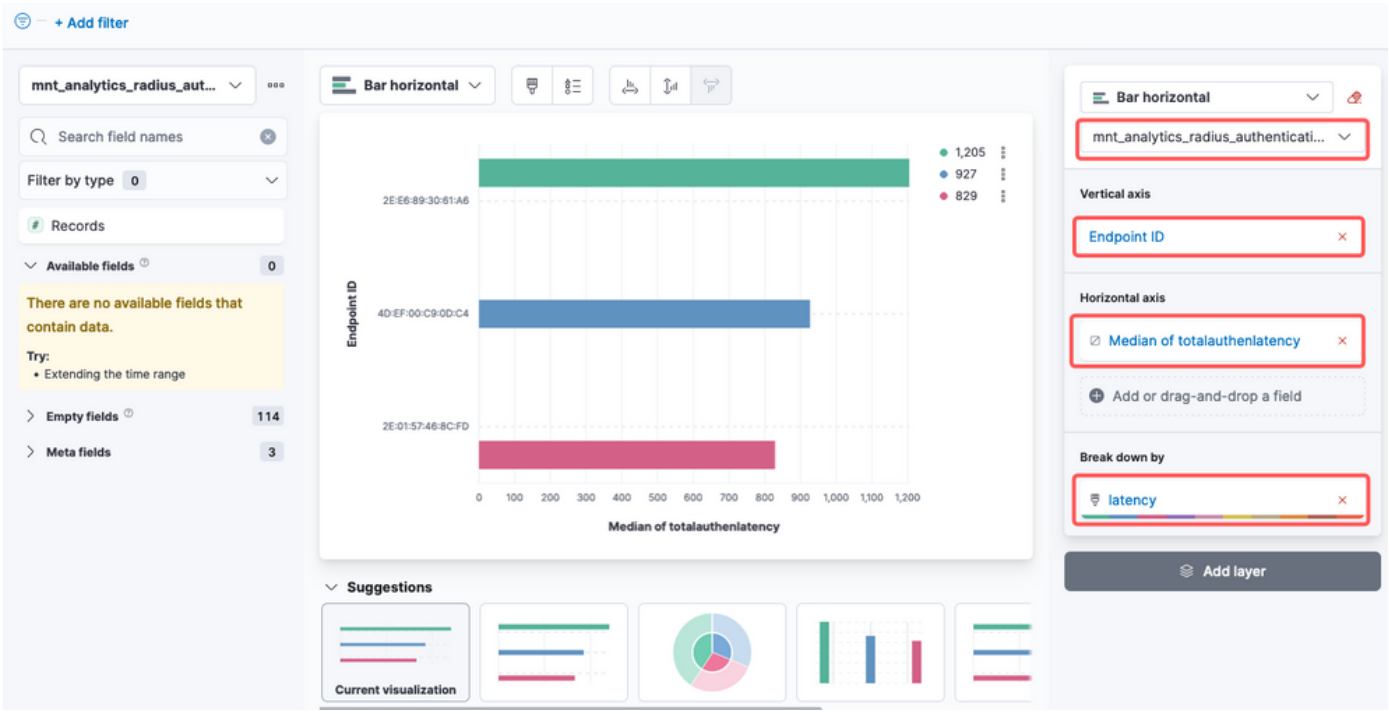
بشكل نموذجي بحيث يمكنك رؤية كيف يبدو المخطط الخاص بك مع الإعدادات الحالية.

- إعدادات المرئيات: على حسب نوع المخطط المحدد، يمكنك الوصول إلى إعدادات معينة لنوع المرئيات هذا، مثل تكوين المحور، أنظمة الألوان، والتسميات.
- إعدادات التفاعلية: يمكنك إضافة تفاعلات وإجراءات إلى المرئيات الخاصة بك، مما يتيح للمستخدمين تصفية البيانات أو التنقل إلى أجزاء أخرى من لوحات المعلومات في الكيبانا.
- حفظ ومشاركة: في أعلى واجهة العدسة، توجد عادة خيارات لحفظ مرآيتك أو إضافتها إلى لوحة معلومات أو مشاركتها مع الآخرين.



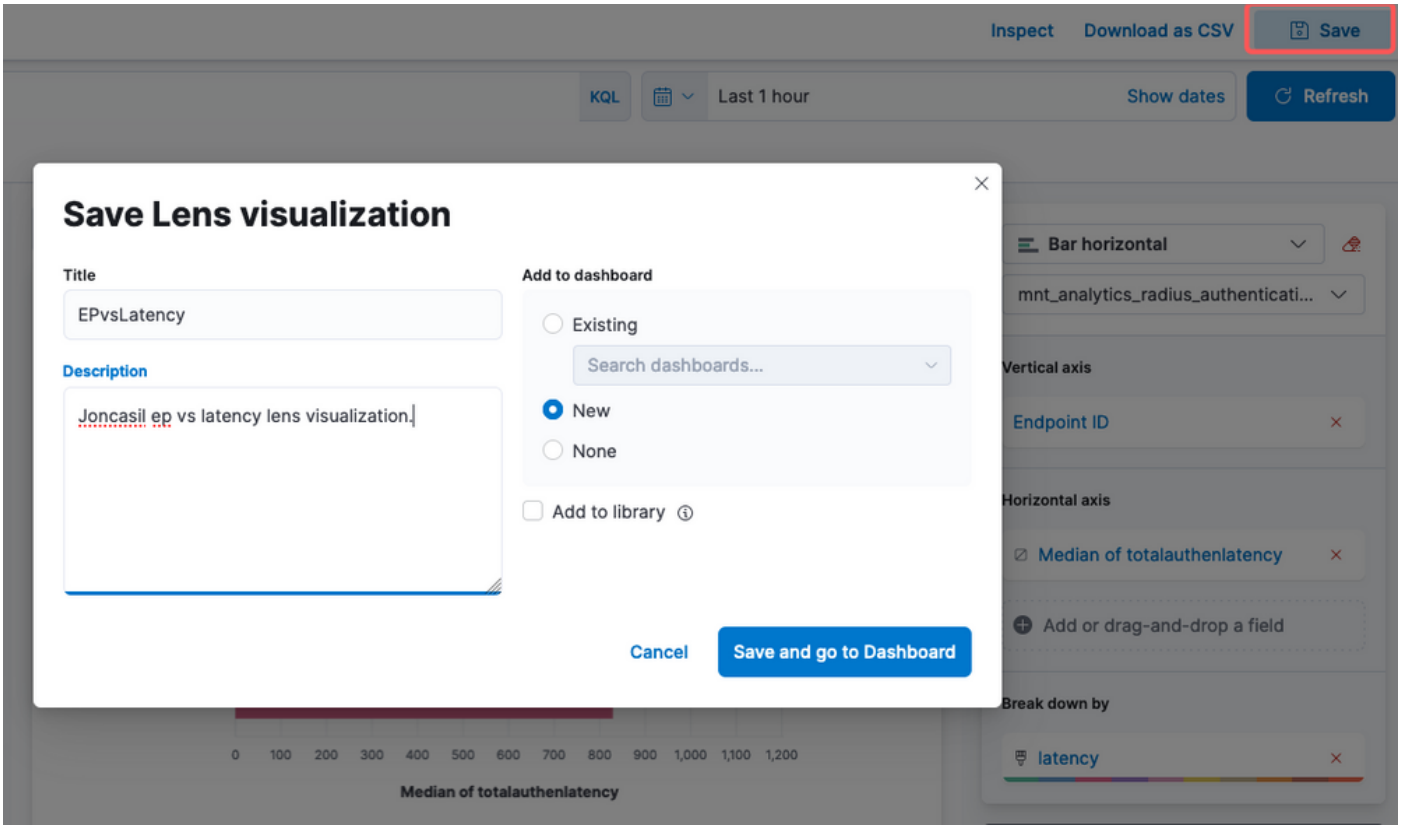
مرئيات العدسات

بسبب معرف تصحيح الأخطاء من Cisco CSCwh48057، لا تظهر اللوحة اليسرى الحقول المتاحة للاستخدام. على أي حال، من الجانب الأيمن، يمكنك تحديد الحقول المطلوبة بالإضافة إلى نمط الرسم التخطيطي. في هذا المثال، نظرا لأن زمن وصول المصادقة هو موضوع يحظى باهتمام مشترك، فقد تم تصميم الرسم البياني لعرض زمن وصول المصادقة مقابل معرف نقطة النهاية.



معرف نقطة النهاية مقابل زمن الوصول

بمجرد الانتهاء، يمكنك النقر فوق Save زر في الزاوية اليمنى كما هو موضح في الصورة.

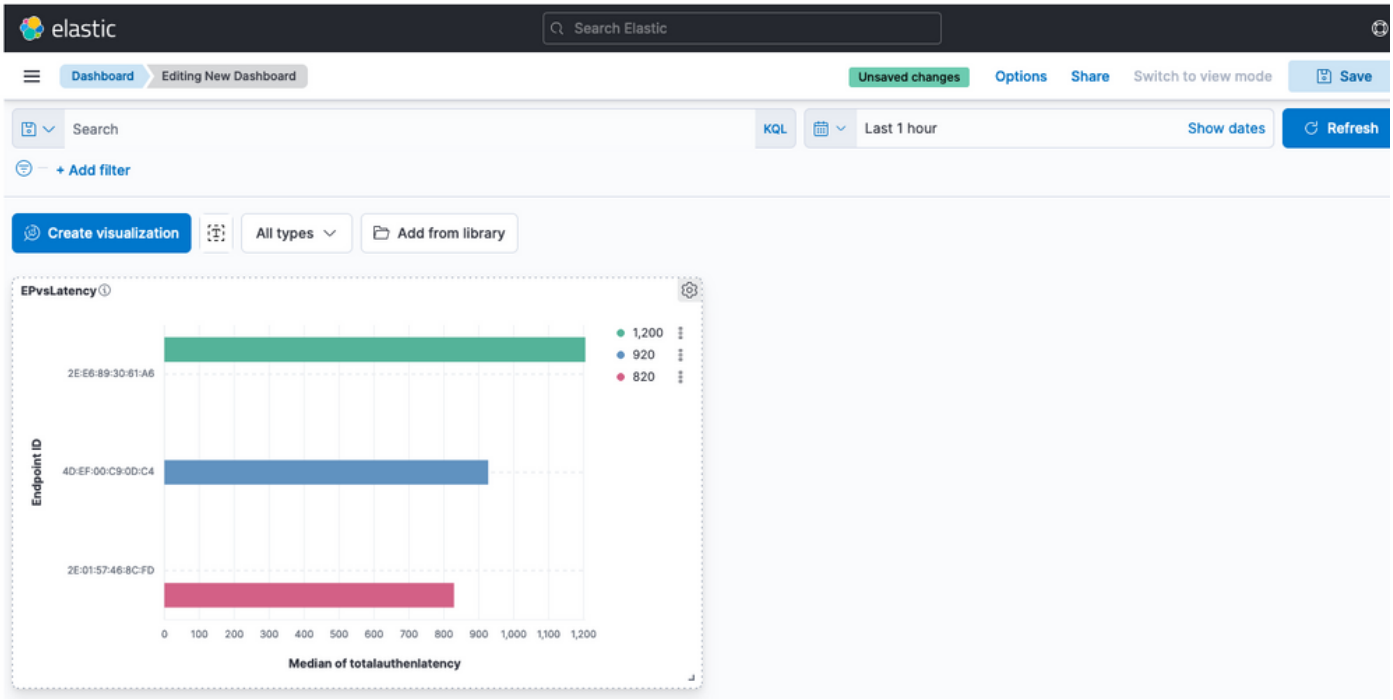


حفظ المرئيات

الخطوة 3. إنشاء لوحة معلومات

وهو يضيف تلقائيا المرئيات الجديدة إلى لوحة معلومات جديدة. ضع في الاعتبار أن لوحات المعلومات في كيبانا تمكن المستخدمين من إنشاء وتخصيص ومشاركة المرئيات

والتقارير التفاعلية المستندة إلى البيانات المخزنة في مؤشرات Elasticsearch.



لوحة معلومات جديدة

استكشاف الأخطاء وإصلاحها

- تحقق من تشغيل خدمات مكدس ELK على MNT.
- وبما أن Kibana، و Logstash، و Elasticsearch تعمل على الحاويات، فقد عثر على السجلات في:

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

معلومات ذات صلة

- دليل مسؤول ISE 3.3
- وثائق كيبانا
- الدعم التقني والتنزيلات من Cisco

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).