Comprendre Log Analytics-ELK Stack sur ISE

Table des matières

Introduction

Ce document décrit les composants de la pile ELK intégrés dans Cisco Identity Services Engine (ISE) 3.3 à System 360 Log Analytics.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco ISE
- Pile ELK

Composants utilisés

Les informations contenues dans ce document sont basées sur Cisco ISE 3.3.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

System 360 inclut la surveillance et l'analyse des journaux.

La fonction Surveillance vous permet de surveiller un large éventail de statistiques d'applications et de systèmes, ainsi que les indicateurs de performance clés (KPI) de tous les noeuds d'un déploiement à partir d'une console centralisée. Les indicateurs de performance clés sont utiles pour obtenir des informations sur l'état général de l'environnement du noeud. Les statistiques offrent une représentation simplifiée des configurations du système et des données spécifiques à l'utilisation.

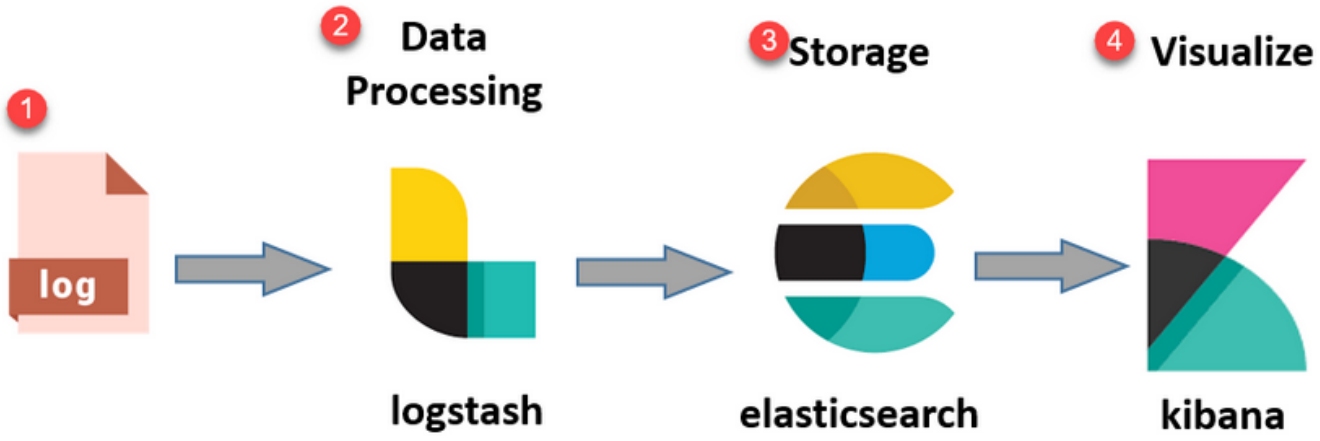
Log Analytics fournit un système d'analyse flexible pour l'analyse approfondie de l'authentification, de l'autorisation et de la comptabilité des terminaux (AAA), et le profilage des données Syslog. Vous pouvez également analyser le résumé de l'état de santé et les états des processus de Cisco ISE. Vous pouvez générer des rapports similaires au rapport Cisco ISE Counters and Health Summary.

Pile ELK

La pile ELK est une pile logicielle open source populaire utilisée pour collecter, traiter et visualiser de grands volumes de données. Il est l'acronyme de Elasticsearch, Logstash et Kibana.

- Elasticsearch : Elasticsearch est un moteur de recherche et d'analyse distribué. Il est conçu pour stocker, rechercher et analyser de grands volumes de données rapidement et quasiment en temps réel. Il utilise un langage de requête JSON et est hautement évolutif.
- Logstash : Logstash est un pipeline de traitement de données qui ingère, traite et transforme des données provenant de plusieurs sources. Il peut analyser et enrichir les données, ce qui les rend plus structurées et adaptées à l'analyse. Logstash prend en charge une large gamme de sources d'entrée et de destinations de sortie.
- Kibana : Kibana est une plate-forme de visualisation de données qui fonctionne avec Elasticsearch. Il permet aux utilisateurs de créer des tableaux de bord, des graphiques, des graphiques et des visualisations interactifs pour explorer et comprendre les données stockées dans Elasticsearch. L'interface de Kibana facilite l'interrogation et la visualisation des données.

Lorsqu'ils sont combinés, ces composants forment une pile puissante pour gérer et analyser divers types de données, des fichiers journaux aux mesures et bien plus encore, tout en fournissant des fonctionnalités de visualisation pour donner un sens aux informations.

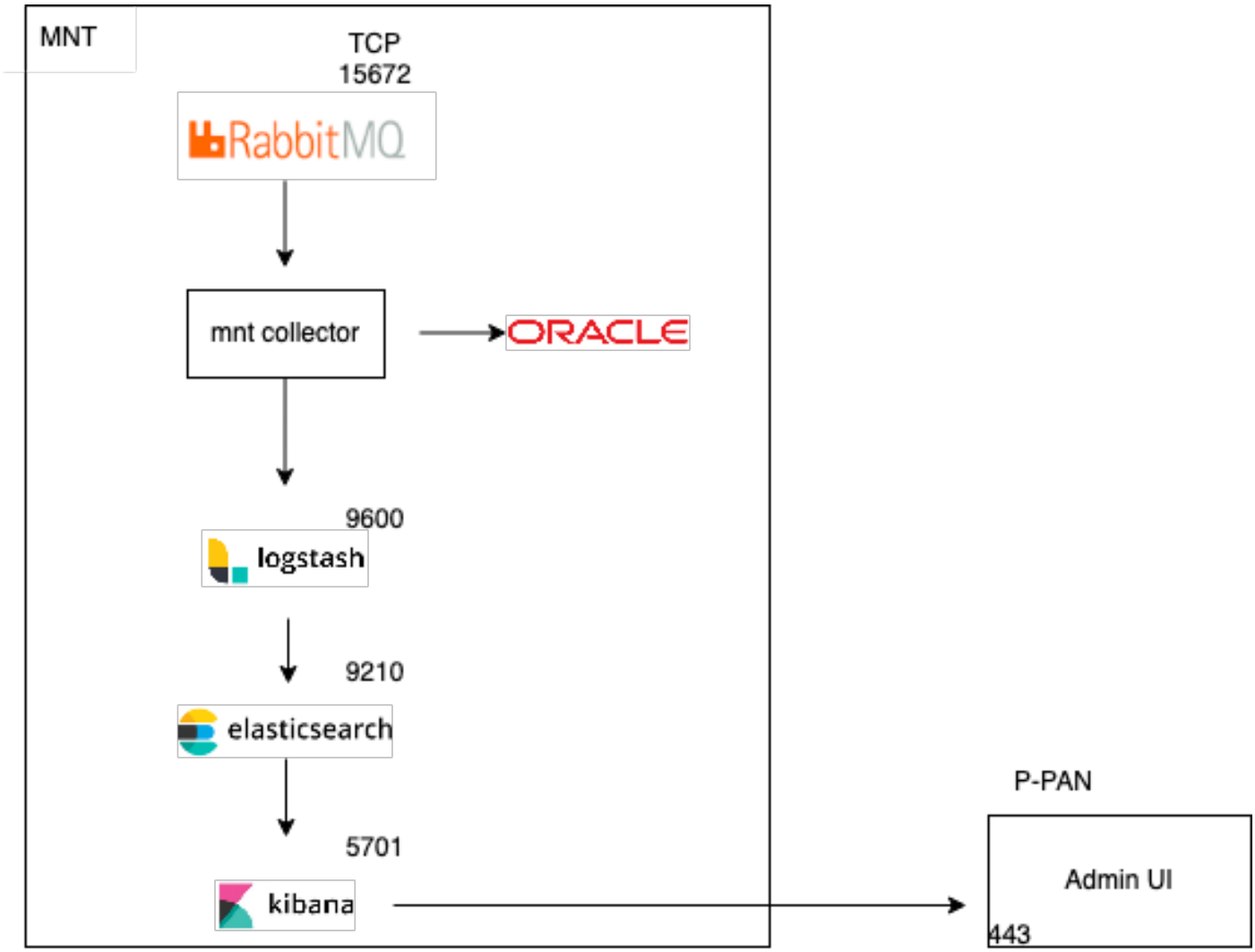


ELK Stack flow

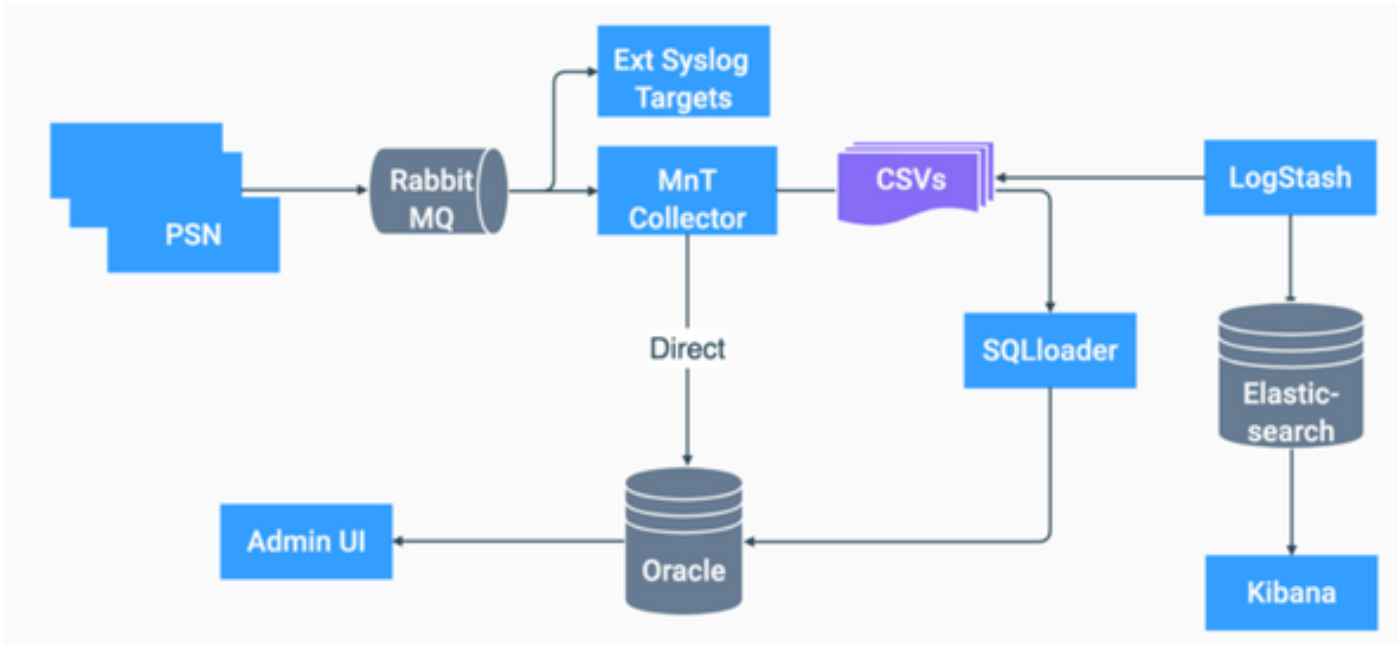
Pile ELK en tant que log Analytics

- Une instance distincte de la pile ElasticSearch+LogStash+Kibana s'exécute sur les noeuds MnT uniquement.
  - Cela n'a aucune corrélation avec la recherche élastique de Context-Visibility.
  - Exécution d'ELK 7.17

- Les MNT primaire et secondaire ont leurs propres instances distinctes d'ELK.
  - Kibana est activé uniquement sur le MNT secondaire s'il est disponible, affichant uniquement les données de ce noeud.
- Log Analytics est désactivé par défaut.
- Consomme des ressources Oracle.
- Stocke un maximum de 7 jours de données.
- La taille totale des données utilisées par Log Analytics est limitée à 10 Go.
  - Une fois que l'une des limites est atteinte, ElasticSearch purge les données.



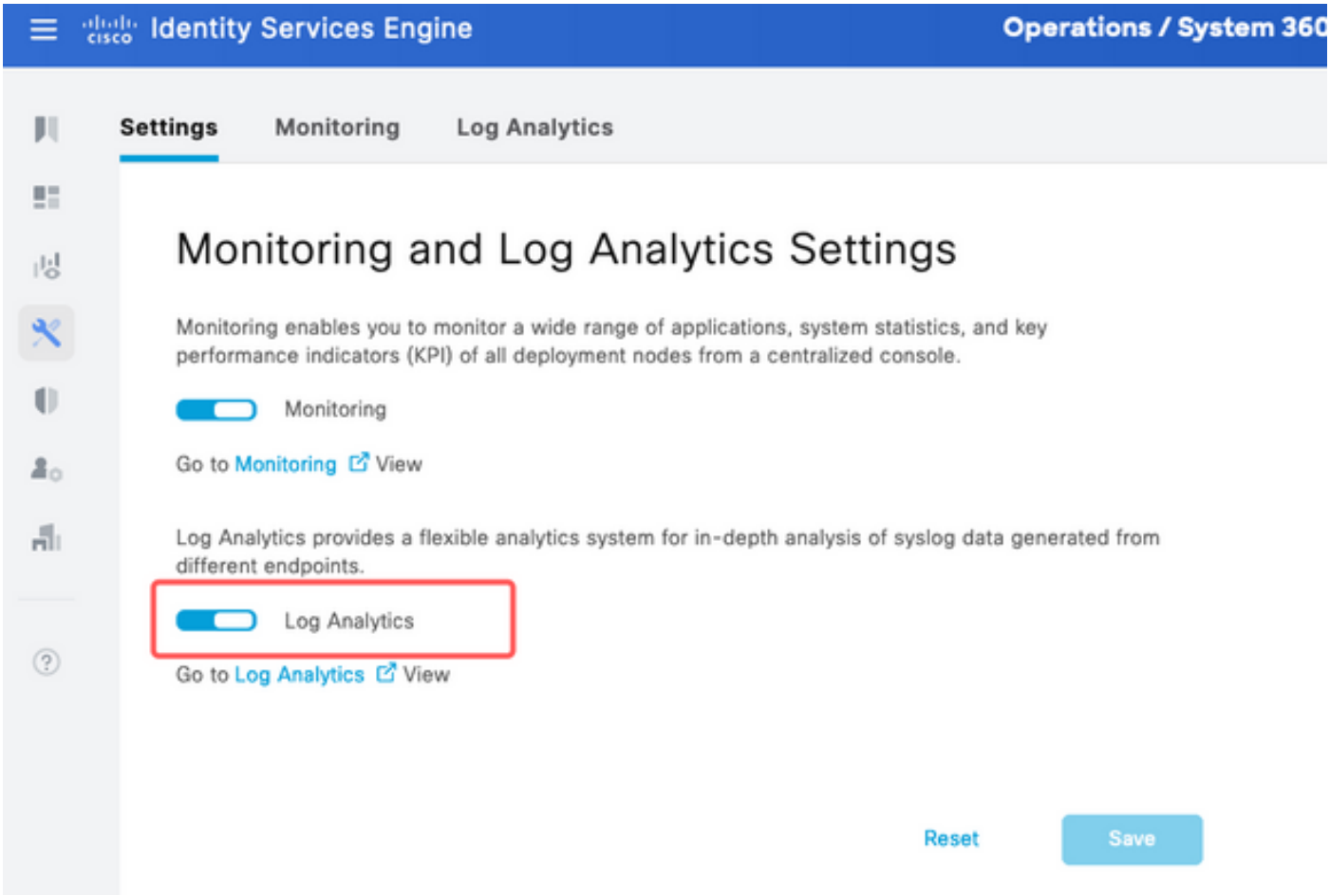
Flux ELK sous Log Analytics



Organigramme de ELK dans ISE

Activer Log Analytics

L'analyse des journaux est désactivée par défaut sur ISE. Pour l'activer, accédez à `Operations > System 360 > Settings` comme illustré dans l'image.



Activer l'analyse des journaux

ISE prend environ une minute pour initialiser la pile ELK, vous pouvez vérifier l'état en utilisant `show app stat ise`.

En outre, vous pouvez vérifier l'état du conteneur à partir de la racine.

<#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

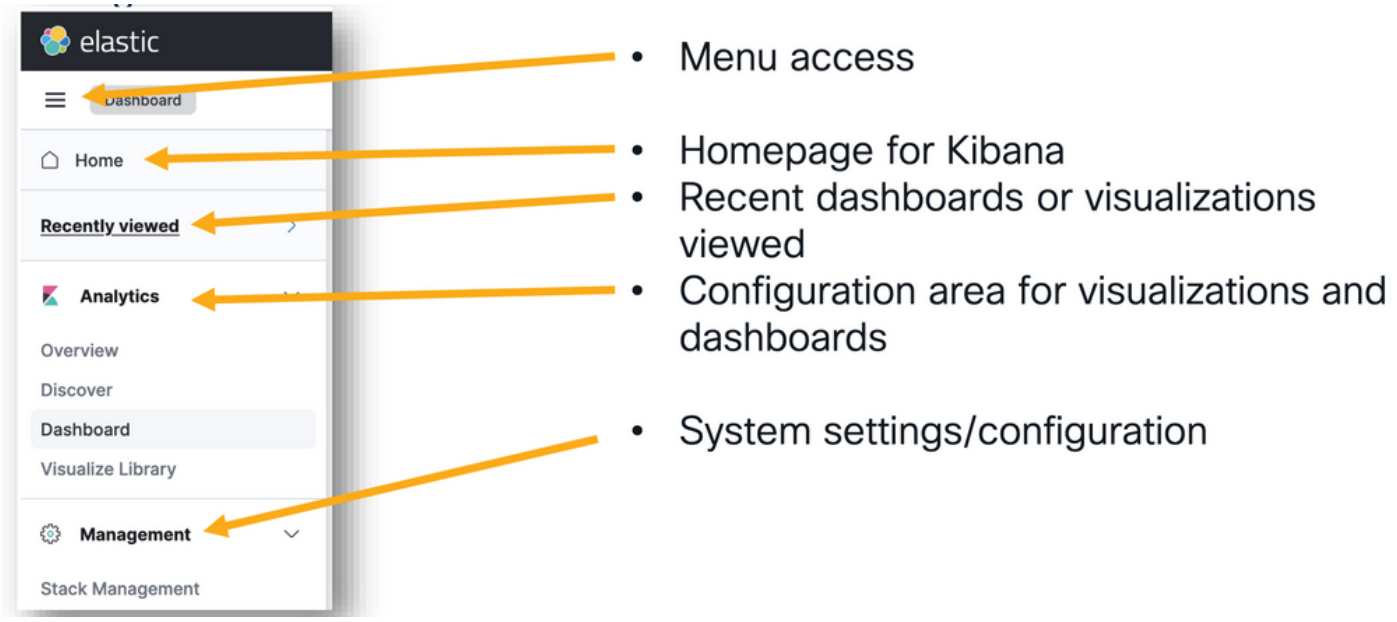
ISE Logstash Service running 614339

ISE Kibana Service running 616064

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

Menu de navigation

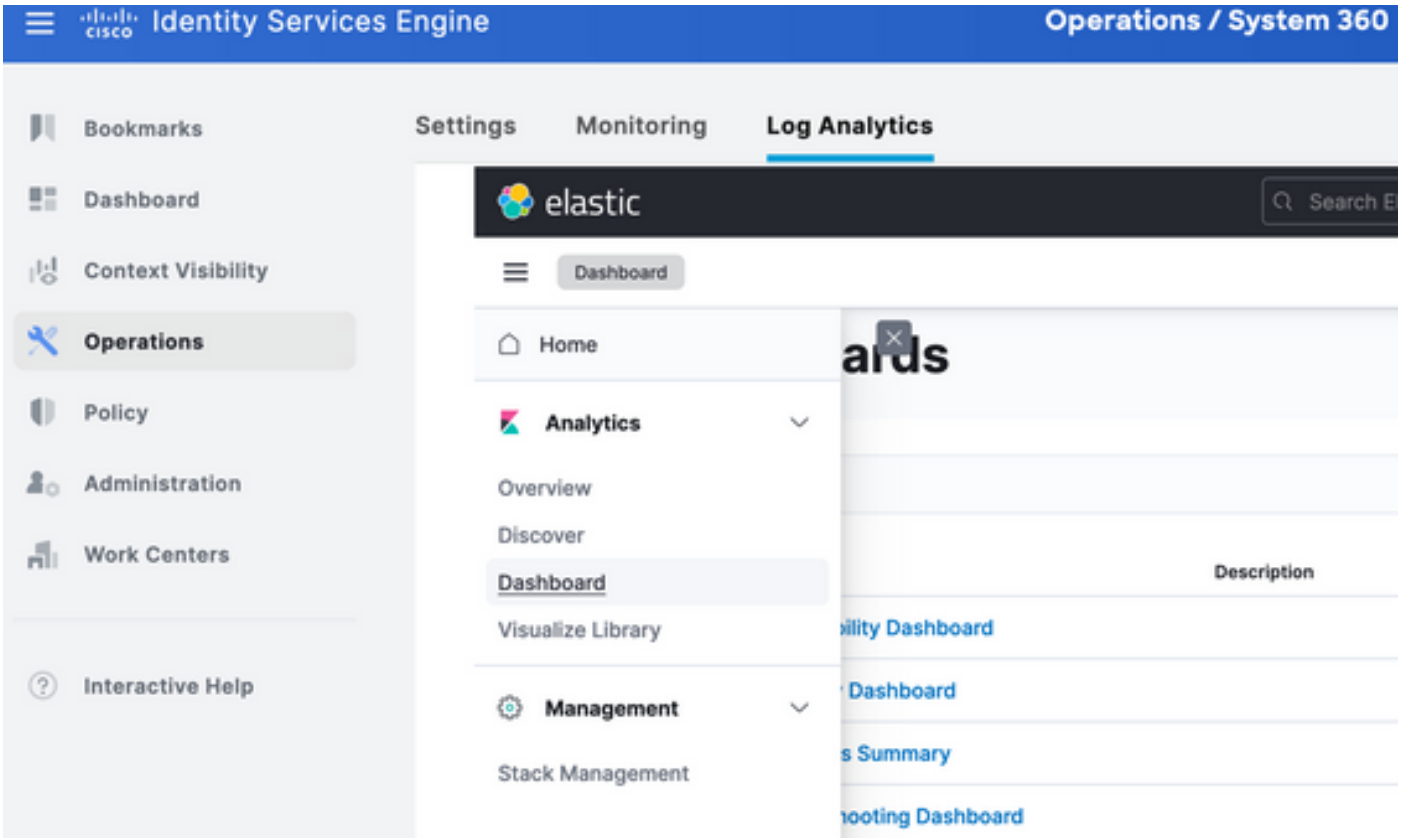
Une fois les services ELK démarrés, vous avez accès au menu de navigation Elastic.



Menu Navigation

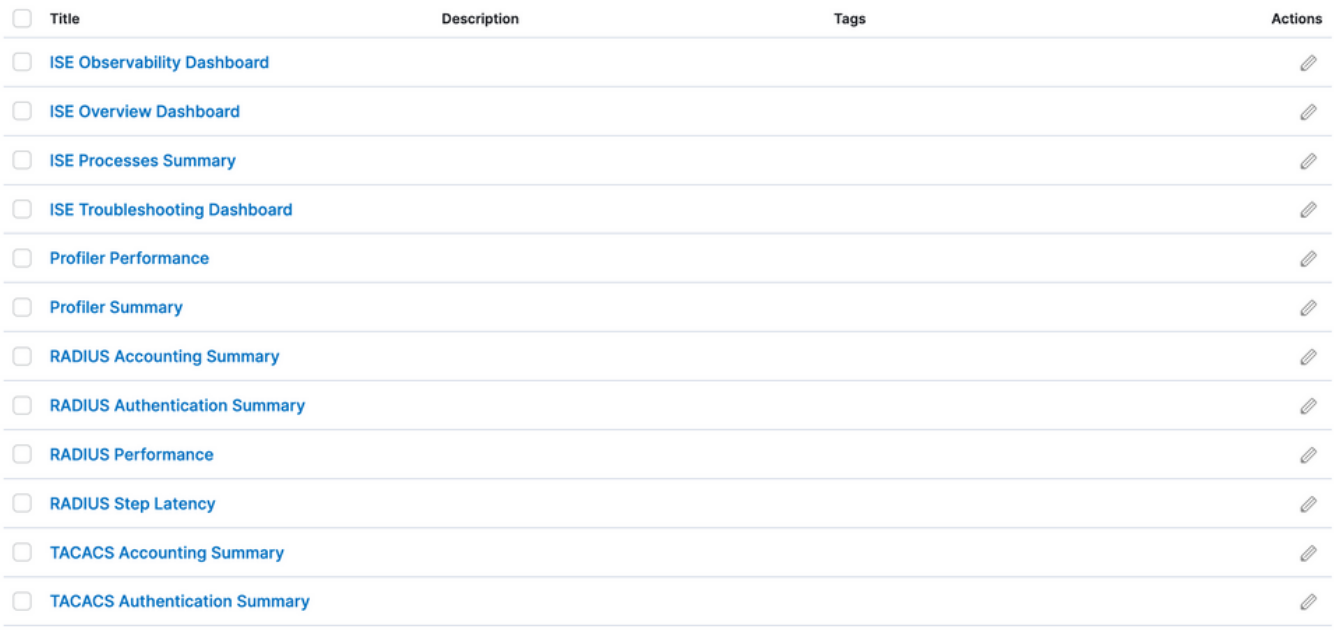
Tableaux de bord intégrés

- ISE intègre par défaut des tableaux de bord avec des données provenant de Radius, TACACS, les performances du système et l'observabilité ISE.
- Vous pouvez accéder à ces tableaux de bord en naviguant jusqu'à Operations > Log Analytics .
  - Une fois l'interface utilisateur élastique ouverte, cliquez sur Sandwich Menu > Analytics > Dashboards .



Tableaux de bord intégrés

- Tableaux de bord disponibles sur ISE 3.3.



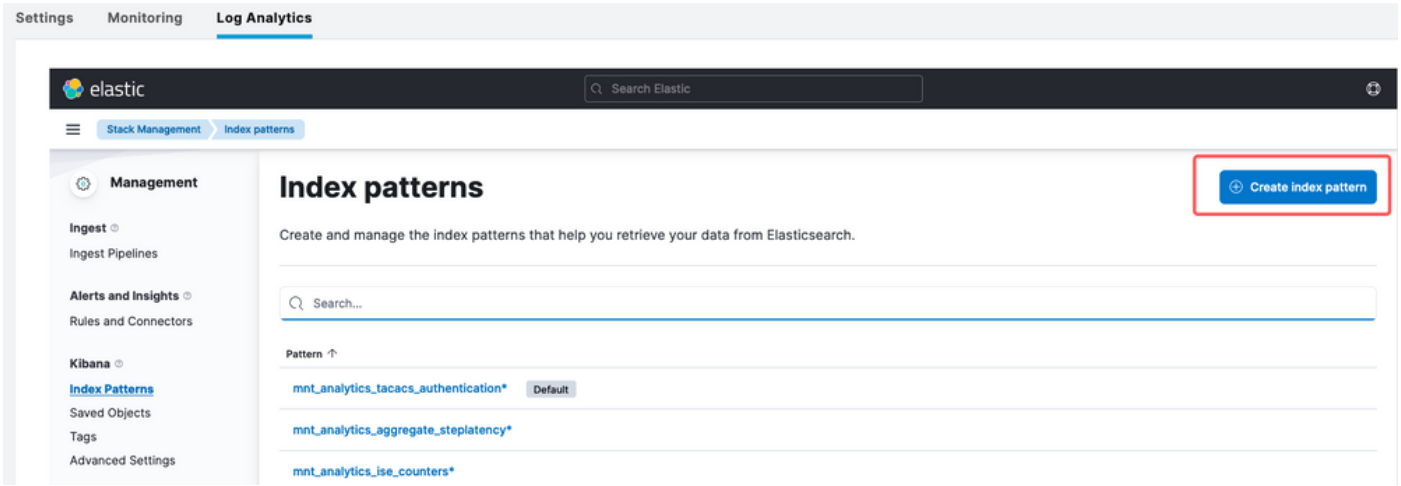
Tableaux de bord d'ISE 3.3 log analytics

Créer de nouveaux tableaux de bord

Étape 1. Créer des modèles d'index (source de données)

Dans Kibana, les "modèles d'index" sont des configurations qui vous permettent de définir comment Kibana interagit avec un ou plusieurs index de recherche élastique.

Naviguez jusqu'à Management > Stack Management > Kibana > Index Patterns, puis cliquez sur Create Index Pattern comme illustré dans l'image.

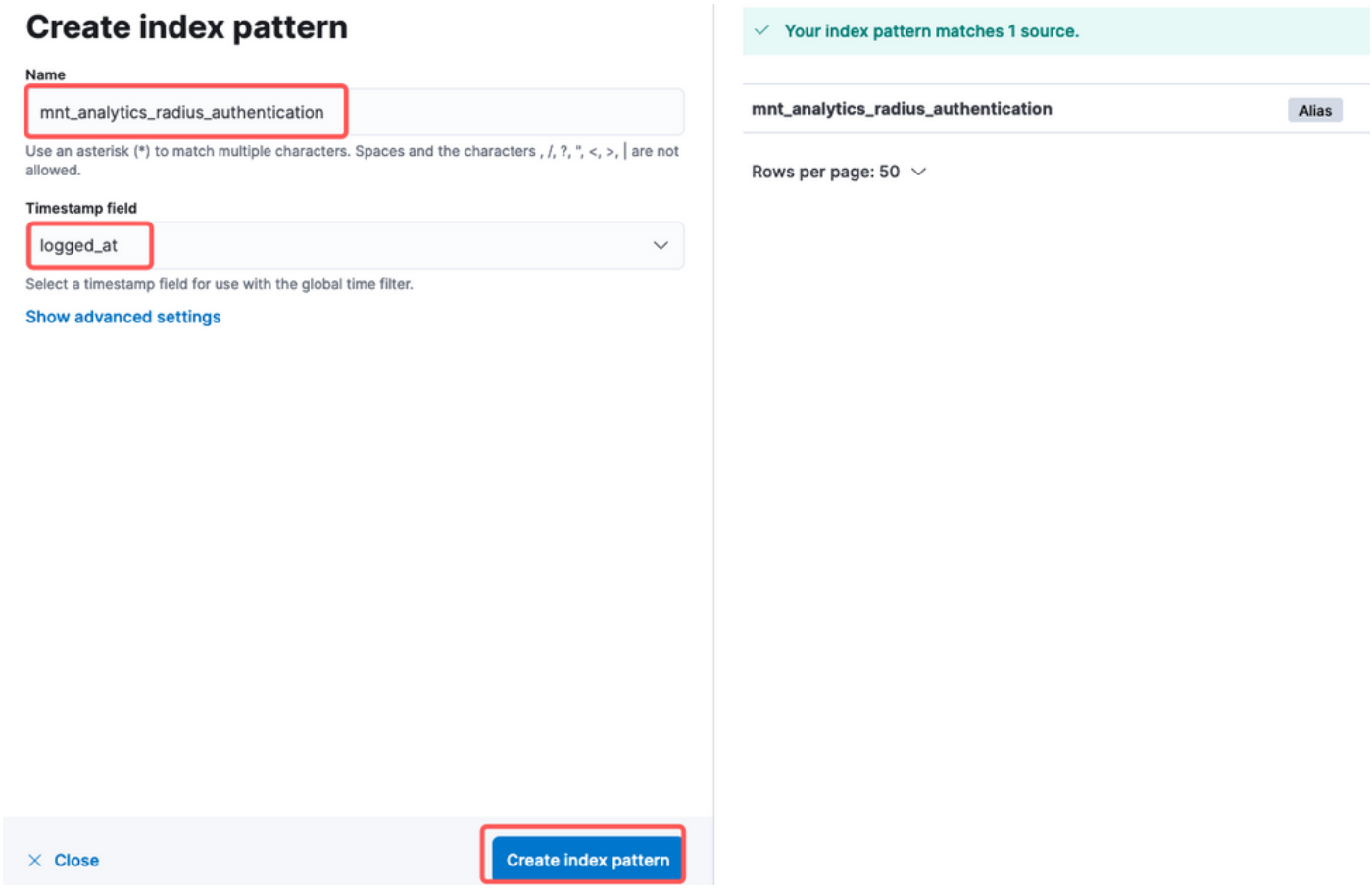


Créer un modèle d'index

La fenêtre suivante affiche la liste de tous les index disponibles sur ISE.

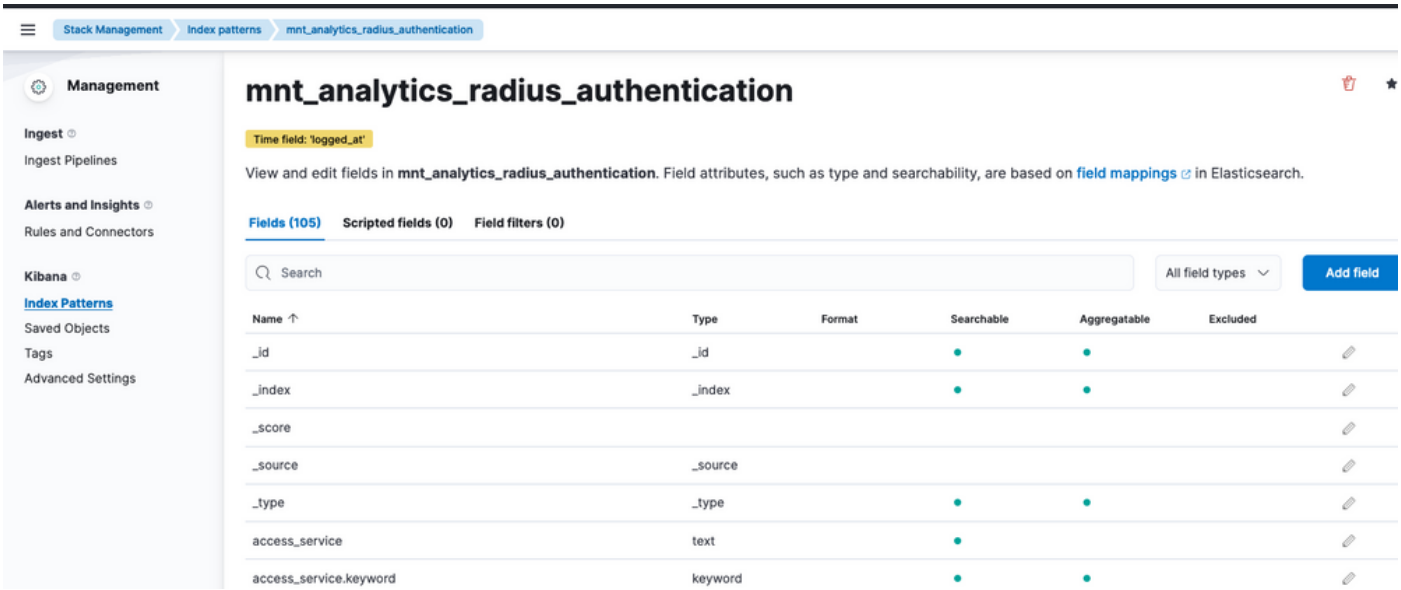
- Tapez le nom de l'index qui vous intéresse, il peut s'agir d'une correspondance exacte ou d'un caractère générique utilisant *.

- Sélectionnez le champ Timestamp, logging_at, logging_at_timezone ou "Je ne veux pas utiliser le filtre d'heure".
- Cliquez ensuite sur Create index pattern.



Sélectionner un index

Une fois créé, l'index répertorie toutes les variables associées qui peuvent être utilisées ultérieurement pour créer des visualisations.



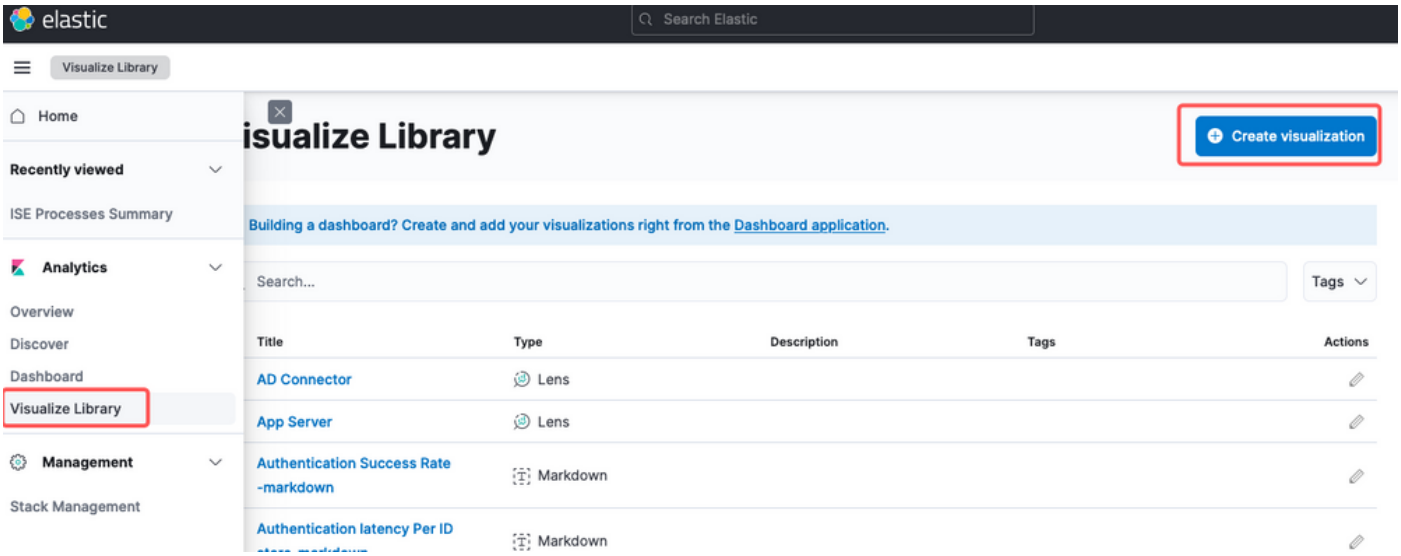
Variables d'index

Étape 2. Créer des visualisations

Dans Kibana, les "visualisations" sont des représentations graphiques de vos données. Ils vous permettent de prendre les données stockées dans Elasticsearch et de les transformer en graphiques, diagrammes et diagrammes significatifs pour une compréhension et une analyse plus faciles. Voici quelques types de visualisations que vous pouvez créer :

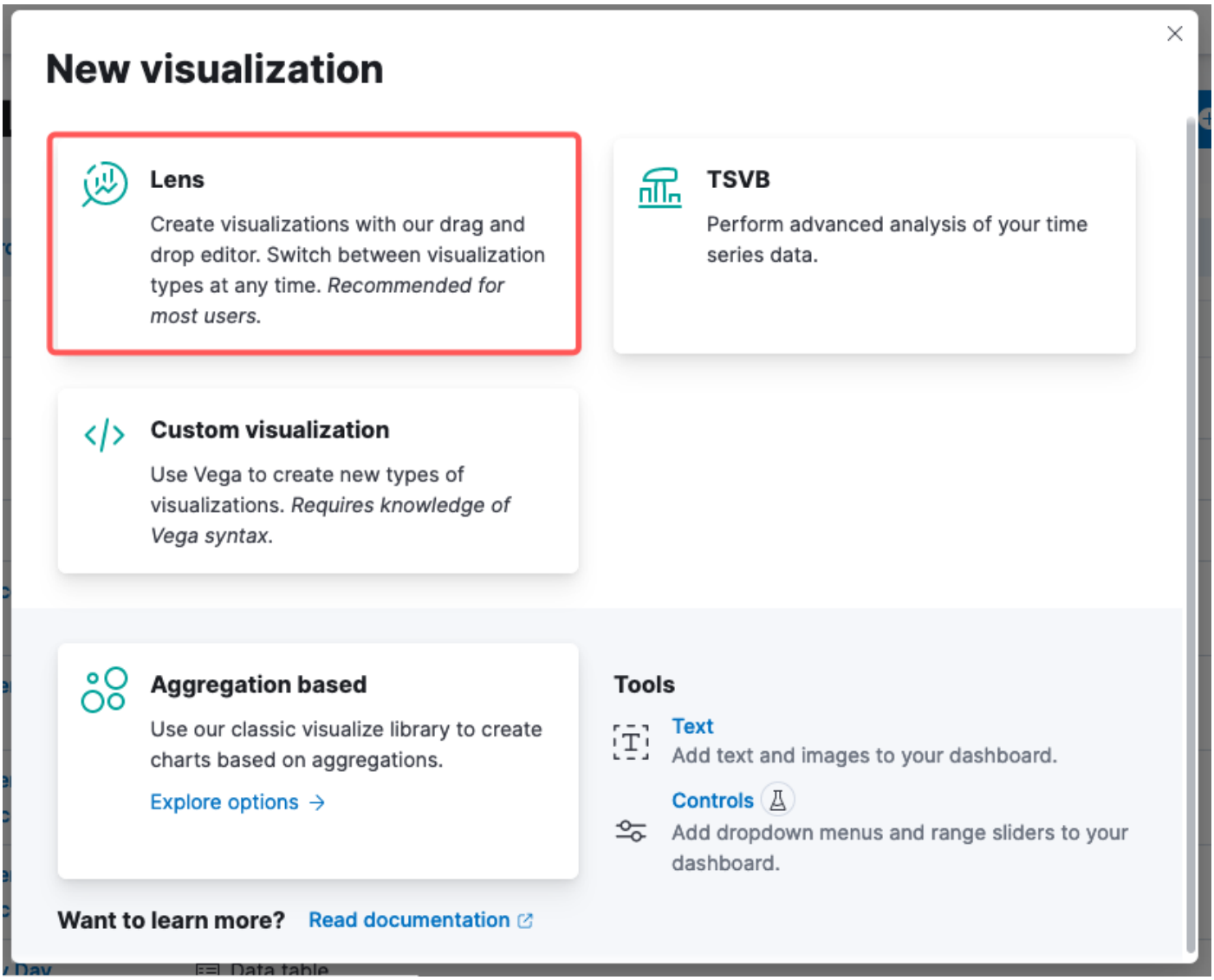
- Objectif : crée la visualisation à l'aide d'un éditeur par glisser-déplacer. Recommandé.
- Graphiques à barres : ils affichent les données sous forme de barres verticales, ce qui facilite la comparaison des valeurs entre les catégories ou les intervalles de temps.
- Graphiques linéaires : les graphiques linéaires affichent les données sous la forme d'une série de points de données reliés par des lignes. Ils sont utiles pour visualiser les tendances dans le temps.
- Graphiques à secteurs : les graphiques à secteurs représentent des données dans un graphique circulaire, chaque segment du secteur représentant une catégorie et la taille du segment indiquant sa proportion.
- Graphiques en aires : comme les graphiques en courbes, les graphiques en aires affichent également des tendances dans le temps, mais ils remplissent la zone située sous les lignes, ce qui facilite la visualisation de l'ampleur des modifications.
- Cartes thermiques : les cartes thermiques utilisent des couleurs pour représenter les valeurs de données dans une matrice ou une grille. Ils sont utiles pour montrer les concentrations ou les variations dans les données.
- Visualisations de mesure : elles affichent des valeurs numériques uniques, telles que des nombres ou des moyennes. Ils sont souvent utilisés pour afficher des indicateurs de performance clés (KPI).
- Tables de données : les tables de données présentent les données brutes sous forme de tableaux, ce qui vous permet de consulter des informations détaillées et de trier ou filtrer les données.
- Histogrammes : les histogrammes divisent les données en cases ou intervalles et affichent la fréquence ou le nombre de points de données dans chaque case. Ils sont utiles pour comprendre les distributions de données.
- Cartes de coordonnées : elles permettent de visualiser des données géospatiales, ce qui vous permet d'afficher des données sur une carte et d'utiliser divers marqueurs, couleurs ou tailles pour représenter des attributs de données.
- Nuages de balises : les nuages de balises affichent la fréquence des mots, la taille de chaque mot indiquant son importance ou sa fréquence dans un jeu de données.

Naviguez jusqu'à Analytics > Visualize Library , puis cliquez sur Create Visualization comme illustré dans l'image.



Créer une visualisation

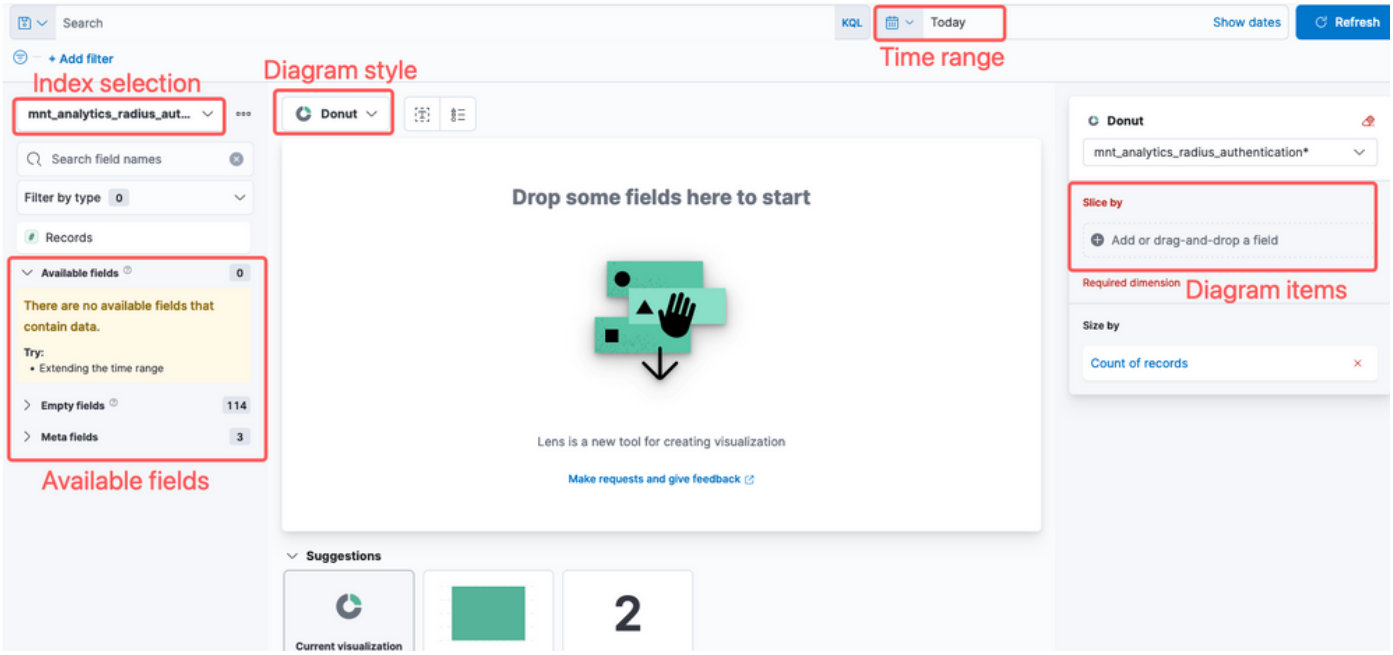
Sélectionnez la visualisation de votre préférence, sur cet exemple Lens est préféré pour des raisons pratiques.



Sélectionner le type de visualisation

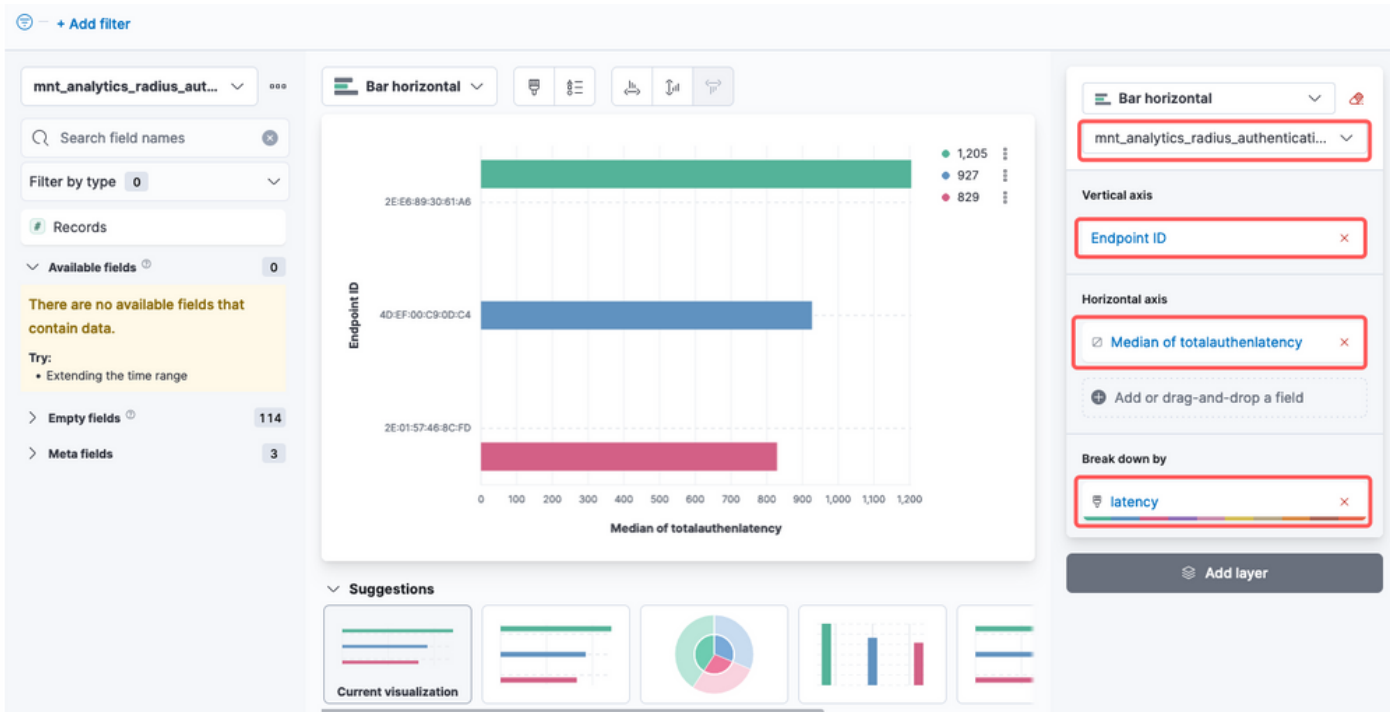
Kibana Lens, les éléments de navigation se composent de :

- Sélection de source de données : dans le panneau de gauche, vous pouvez sélectionner la source de données ou le modèle d'index Elasticsearch que vous souhaitez utiliser pour votre visualisation.
- Toile de visualisation : la zone centrale est l'endroit où vous créez votre visualisation en faisant glisser et en déplaçant des champs, en sélectionnant des types de graphiques et en configurant les paramètres des graphiques.
- Barre d'outils de visualisation : en haut de la zone de travail, vous trouverez une barre d'outils qui vous permet de personnaliser votre visualisation, y compris des options pour modifier les types de graphiques, ajouter des filtres et configurer les paramètres de graphiques.
- Panneau de données : à droite, vous pouvez accéder au panneau « Données », qui vous permet de gérer la transformation de vos données, l'agrégation et les paramètres de champ.
- Gestion des couches : selon le type de visualisation que vous créez (par exemple, des graphiques en couches), vous pouvez disposer d'une zone de gestion des couches pour configurer plusieurs couches dans votre visualisation.
- Aperçu : lorsque vous apportez des modifications à votre visualisation, un aperçu en temps réel est généralement fourni pour vous permettre de voir à quoi ressemble votre graphique avec les paramètres actuels.
- Paramètres de visualisation : selon le type de graphique sélectionné, vous pouvez accéder à des paramètres spécifiques pour ce type de visualisation, tels que la configuration de l'axe, les jeux de couleurs et les étiquettes.
- Paramètres d'interactivité : vous pouvez ajouter des interactions et des actions à votre visualisation, permettant aux utilisateurs de filtrer les données ou de naviguer vers d'autres parties de vos tableaux de bord Kibana.
- Enregistrer et partager : en haut de l'interface de l'objectif, il y a généralement des options pour enregistrer votre visualisation, l'ajouter à un tableau de bord, ou le partager avec d'autres.



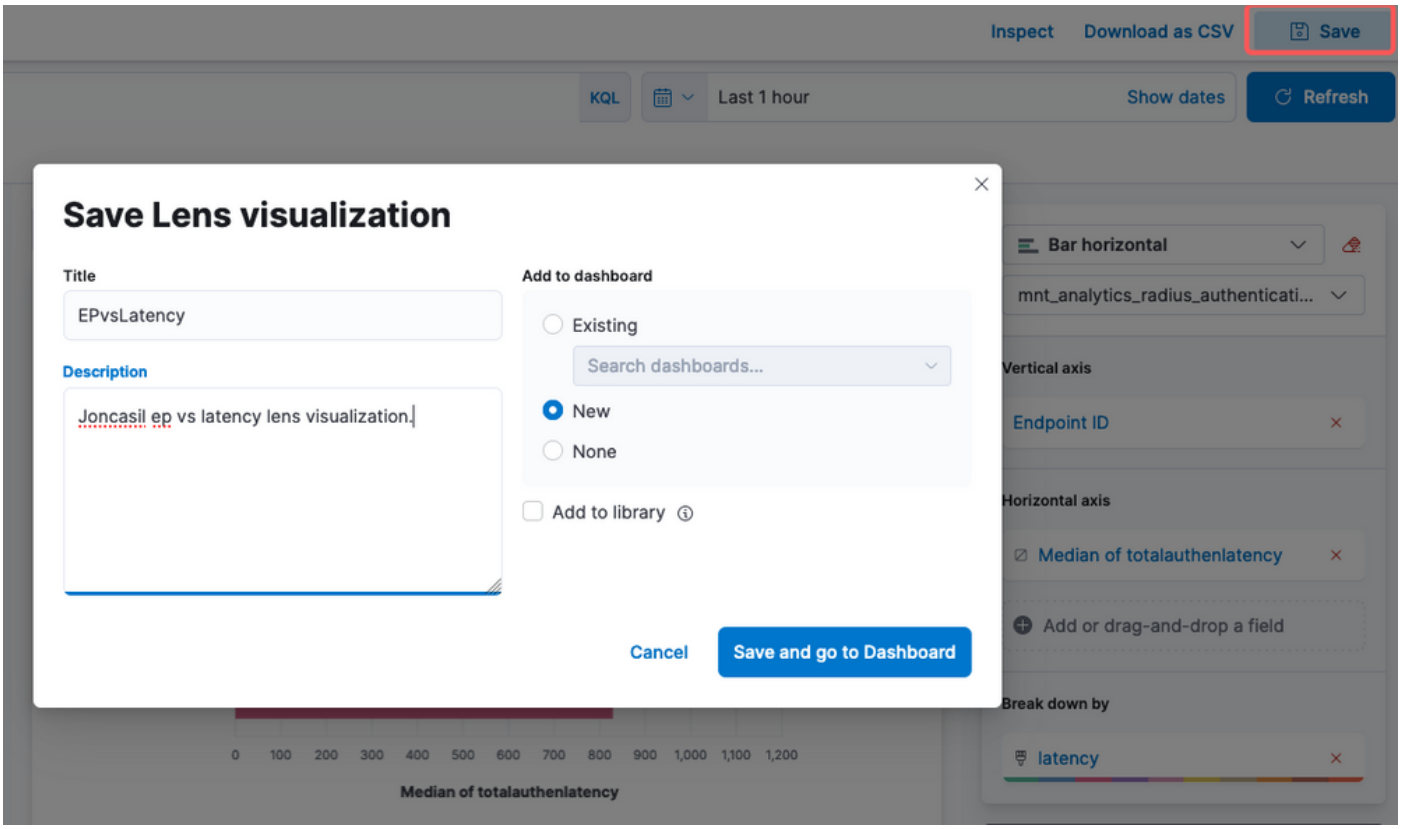
Visualisation de lentille

En raison de l'ID de bogue Cisco [CSCwh48057](), le panneau de gauche n'affiche pas les champs disponibles à utiliser. Cependant, à droite, vous pouvez sélectionner les champs obligatoires ainsi que le style de diagramme. Dans cet exemple, puisque la latence d'authentification est un sujet d'intérêt commun, le graphique est conçu pour visualiser la latence d'authentification par rapport à l'ID de point d'extrémité.



ID de terminal et latence

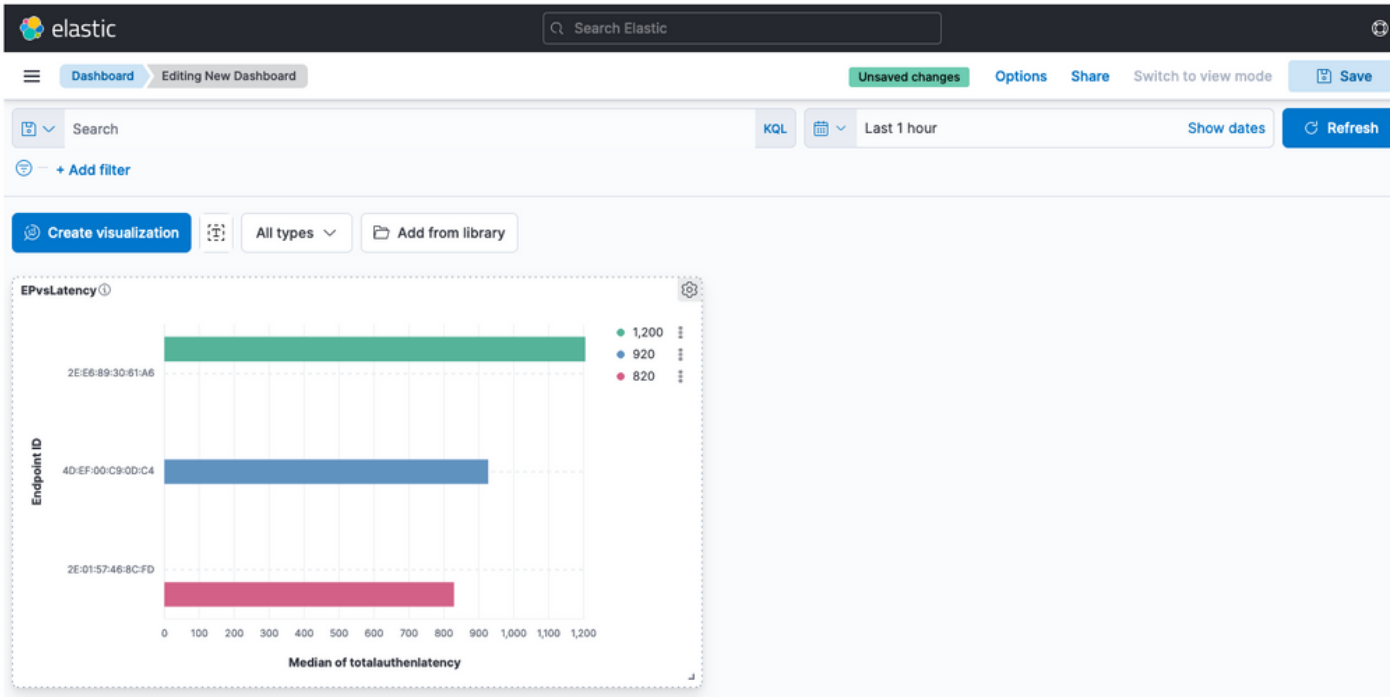
Une fois terminé, vous pouvez cliquer sur le bouton Save dans l'angle droit, comme illustré dans l'image.



Enregistrer la visualisation

Étape 3. Créer un tableau de bord

Il ajoute automatiquement la nouvelle visualisation dans un nouveau tableau de bord. Gardez à l'esprit que les tableaux de bord Kibana permettent aux utilisateurs de créer, personnaliser et partager des visualisations et des rapports interactifs basés sur les données stockées dans les index Elasticsearch.



Nouveau tableau de bord

Dépannage

- Vérifiez que les services de pile ELK sont exécutés sur le MNT.
- Comme Kibana, Logstash et Elasticsearch sont exécutés sur des conteneurs, les journaux sont disponibles à l'adresse suivante :

```
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
```

Informations connexes

- Guide d'administration ISE 3.3
- Documentation Kibana
- Assistance technique et téléchargements Cisco

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.