elastic

Le guide sur Elastic Observability pour AWS

elastic.co/fr →

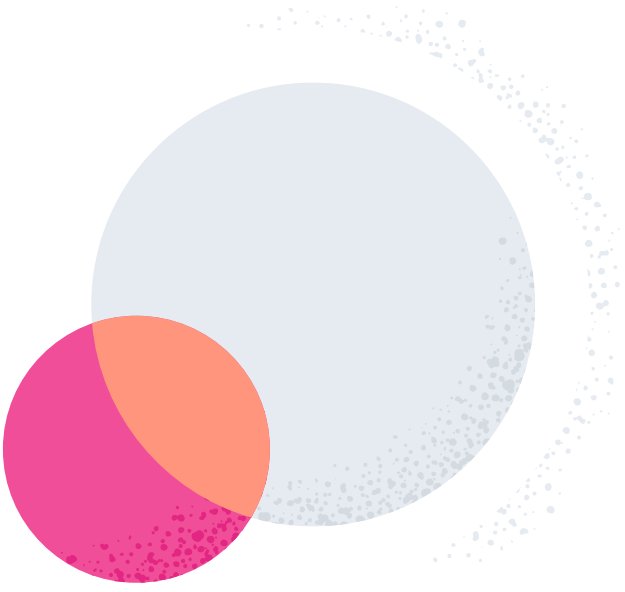
Table des matières

Introduction

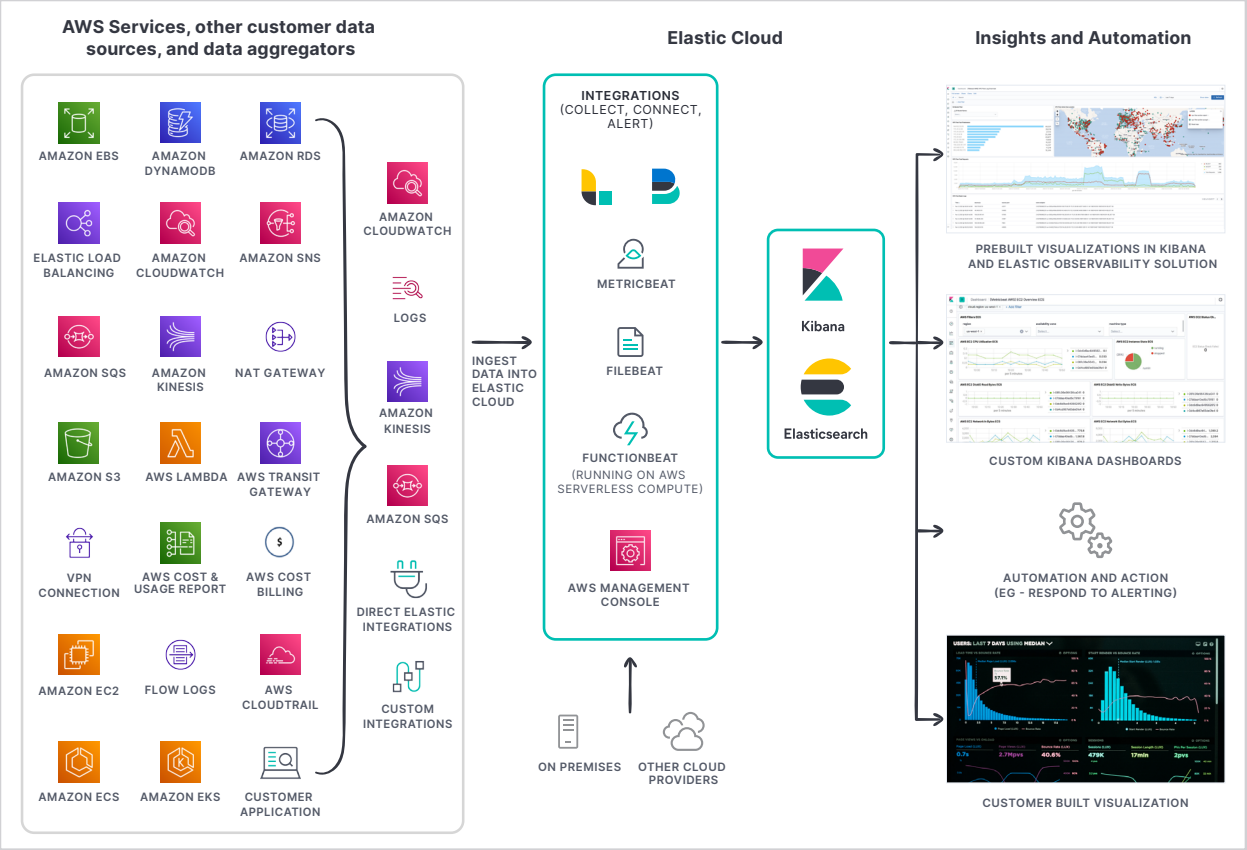
Il est essentiel d'obtenir des informations exploitables et de définir des actions à partir des données afin de tirer pleinement parti de l'agilité et de la flexibilité offertes par le cloud. Grâce à la solution d'Elastic en matière d'observabilité, vous pouvez unifier la visibilité au sein de vos environnements AWS et sur site. Ainsi, vous êtes en mesure de mieux comprendre la disponibilité, la performance et l'état général de vos infrastructures, applications et activités.

AWS vous fournit un vaste éventail de logs et d'indicateurs dans le cadre de ses services cloud, ce qui vous permet de monitorer votre déploiement cloud et de prendre des décisions plus éclairées. Elastic Observability s'intègre à ces sources de données afin d'unifier vos données. De cette manière, vous continuez à obtenir des informations exploitables concernant vos services informatiques, vos opérations et vos activités. Analysez facilement vos données dans des outils et des tableaux de bord prédéfinis ou développez des visualisations personnalisées qui vous aident à réagir rapidement afin de satisfaire vos besoins métier.

Dans ce guide, vous apprendrez à mieux configurer Elastic Observability grâce aux services AWS. Ainsi, vous pourrez plus facilement monitorer les événements et y réagir plus rapidement. Lisez ce guide pour en savoir plus sur ces services AWS, les avantages liés à l'utilisation d'Elastic pour le monitoring et les bonnes pratiques qui peuvent vous aider à optimiser la valeur de vos investissements auprès de ces deux entreprises.



Comment Elastic vous permet de tirer davantage parti de vos données AWS



Monitoring et analyse d'Amazon CloudWatch Logs avec Elastic

Centralisez les logs de vos infrastructures, applications et services AWS que vous utilisez dans un seul service scalable à l'aide d'Amazon CloudWatch.

Grâce à Amazon CloudWatch Logs, vous pouvez facilement et rapidement :

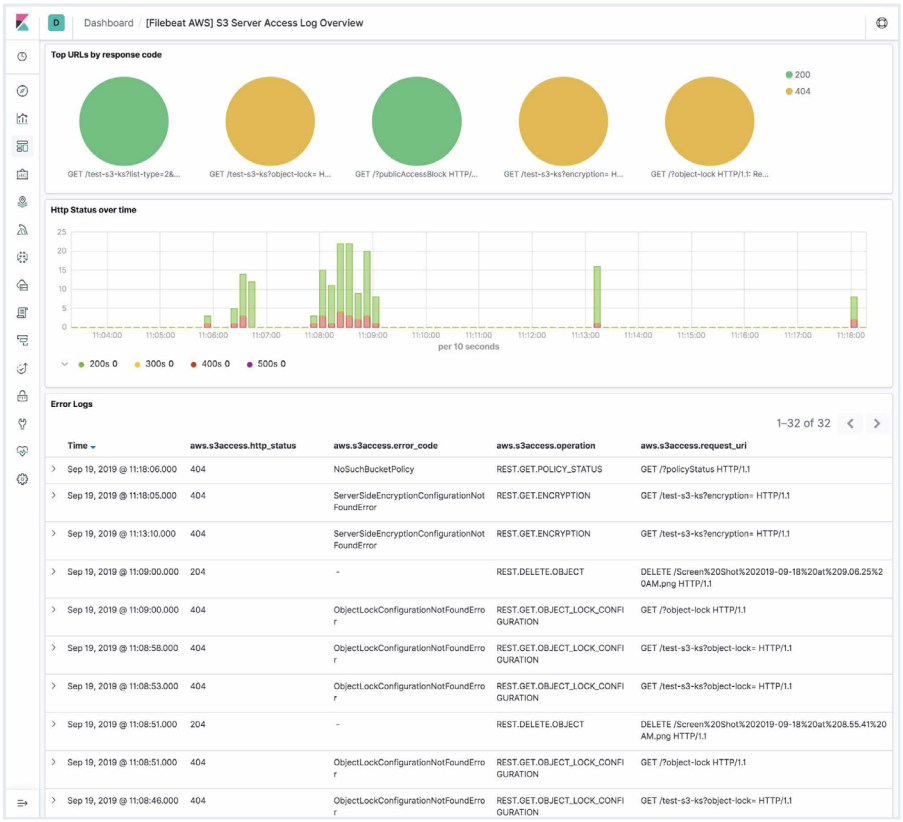
Rassembler, stocker et accéder aux logs à partir de sources diverses.

Monitorer l'état et la performance de vos infrastructures et applications.

Observer Amazon CloudWatch Logs directement dans différents groupes de logs AWS.

elastic

Comment envoyer des Amazon CloudWatch Logs à Elastic



Tout d'abord, vous devez rassembler des informations sur votre environnement AWS et votre déploiement Elastic Cloud. Consultez l'**Annexe A** de ce document pour en savoir plus sur ces prérequis. Pour vous lancer avec Amazon CloudWatch Logs, suivez les étapes décrites dans l'**Annexe B** ci-dessous afin d'obtenir la marche à suivre détaillée concernant notamment les tâches suivantes :

1. Configuration d'un bucket Amazon Simple Storage Service (Amazon S3) et création d'une file d'attente Amazon Simple Queue Service (Amazon SQS)
2. Téléchargement et installation de Filebeat
3. Connexion à la Suite Elastic
4. Configuration de Filebeat pour collecter les Amazon CloudWatch Logs
5. Activation et configuration de vos modules de collecte des données
6. Configuration de vos tableaux de bord Kibana préconfigurés, puis démarrage de Filebeat
7. Analyse des données Amazon CloudWatch dans Kibana

Analyse de l'activité des logs Amazon S3 et monitoring de l'accès avec Elastic

Grâce à Amazon S3, vous pouvez stocker des données, des applications professionnelles et des sites web statiques hôtes. Amazon S3 fournit deux types de workflows à mettre en œuvre, à savoir la collecte des logs personnalisés qu'il stocke, d'une part, et le monitoring des indicateurs et de l'accès à ses services, d'autre part.

Utilisez les solutions d'Elastic avec Amazon S3 pour :

Obtenir des informations sur les requêtes, comme l'adresse IP distante, le demandeur et le nom du bucket, afin de mieux comprendre la nature du trafic par rapport à vos buckets.

Définir des points de comparaison, analyser les modèles d'accès et identifier les tendances dans les tableaux de bord prédéfinis de Kibana.

Détecter les problèmes de sécurité et de conformité, mais aussi mener une analyse de la cause première au sein de votre organisation.

Analyser les logs spécifiques aux applications ou les logs métier personnalisés stockés dans **Amazon S3**.

Comment envoyer des logs d'Amazon S3 à Elastic

Tout d'abord, vous devez rassembler des informations sur votre environnement AWS et votre déploiement Elastic Cloud. Consultez l'**Annexe A** pour en savoir plus sur ces prérequis. Pour vous lancer avec les logs d'Amazon S3, suivez les étapes décrites dans l'**Annexe B** afin d'obtenir la marche à suivre détaillée concernant notamment les tâches suivantes :

1. Configuration d'un bucket Amazon S3 et création d'une file d'attente Amazon SQS
2. Téléchargement et installation de Filebeat
3. Connexion à la Suite Elastic
4. Activation et configuration de vos modules de collecte des données
5. Configuration de Filebeat pour collecter les logs d'Amazon S3
6. Configuration de vos tableaux de bord Kibana préconfigurés et démarrage de Filebeat
7. Analyse des données des logs d'Amazon S3 dans Kibana

Diffusion de données dans Elasticsearch avec Amazon Kinesis

Amazon Kinesis est un service entièrement géré qui fournit en temps réel des sources de données de diffusion à des destinations, comme Amazon S3 et Elastic.

Avec Amazon Kinesis, vous pouvez :

Diffuser des logs en temps réel, puis les analyser à l'aide d'Elasticsearch et de Kibana afin d'obtenir rapidement des informations exploitables et de prendre des décisions plus éclairées.

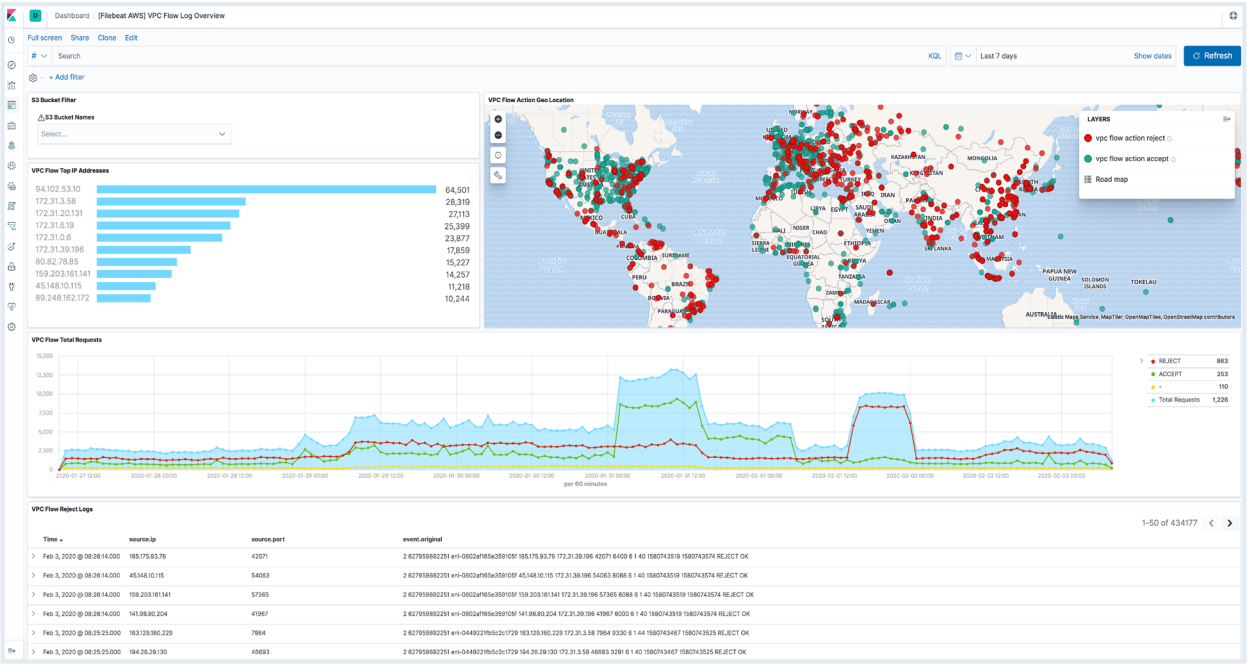
Comprimer, convertir et chiffrer les données en transit afin de diminuer le volume de stockage utilisé tout en renforçant la sécurité.

Comment diffuser des données dans Elastic avec Amazon Kinesis

Vous devez rassembler des informations sur votre environnement AWS et votre déploiement Elastic Cloud avant toute chose. Consultez l'**Annexe A** pour en savoir plus sur ces prérequis. Pour vous lancer avec Amazon Kinesis, suivez les étapes décrites dans l'**Annexe C** afin d'obtenir la marche à suivre détaillée concernant notamment les tâches suivantes :

1. Téléchargement et installation de Metricbeat
2. Connexion à la Suite Elastic
3. Configuration de Metricbeat pour diffuser des données
4. Activation et configuration de vos modules de collecte des données
5. Configuration de vos tableaux de bord Kibana préconfigurés, puis démarrage de Filebeat
6. Analyse des données dans Kibana

Monitoring du trafic réseau à l'aide des logs de flux d'Amazon VPC avec Elastic



Elastic Observability vous permet de rechercher, d'afficher et de filtrer rapidement les logs de flux d'Amazon Virtual Private Cloud (Amazon VPC) pour monitorer le trafic réseau de cette solution à l'aide de Kibana. Avec cette intégration, vous pouvez analyser les données des logs de flux et les comparer à la configuration de vos groupes de sécurité en vue de garantir et d'améliorer la sécurité de votre cloud.

Grâce à l'ingestion des logs de flux d'Amazon VPC, vous pouvez :

Réaliser de meilleures analyses afin de prendre des décisions plus éclairées.

Évaluer les règles des groupes de sécurité et déterminer les lacunes en matière de sécurité.

Définir des alarmes lorsque certains types de trafic sont détectés.

Identifier les problèmes de latence et définir des points de comparaison pour assurer des performances cohérentes.

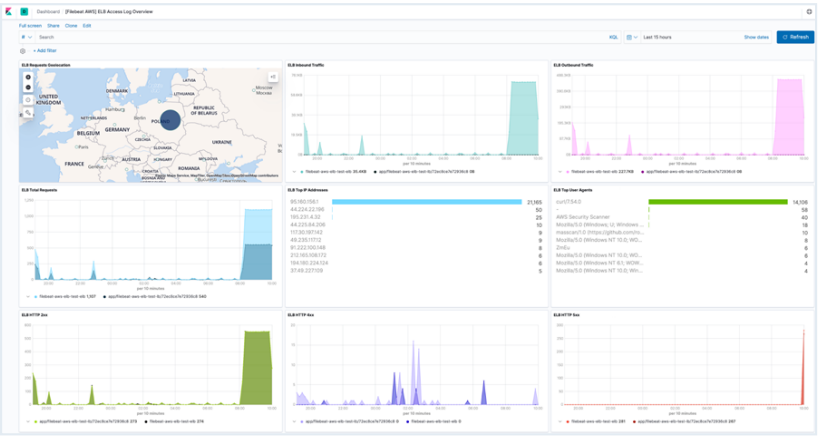
elastic

Comment ingérer les logs d'Amazon VPC dans Elastic

Commencez par rassembler des informations sur votre environnement AWS et votre déploiement Elastic Cloud. Consultez l'**Annexe A** pour en savoir plus sur ces prérequis. Pour vous lancer avec les logs de flux d'Amazon VPC, suivez les étapes décrites dans l'**Annexe B** afin d'obtenir la marche à suivre détaillée concernant notamment les tâches suivantes :

1. Configuration d'un bucket Amazon S3 et création d'une file d'attente Amazon SQS
2. Téléchargement et installation de Filebeat
3. Connexion à la Suite Elastic
4. Configuration de Filebeat pour collecter les logs de flux d'Amazon VPC
5. Activation et configuration de vos modules de collecte des données
6. Configuration de vos tableaux de bord Kibana préconfigurés, puis démarrage de Filebeat
7. Analyse des logs dans Kibana

Observation des opérations d'équilibrage des charges dans Elastic avec Amazon ELB



Le service d'équilibrage des charges Elastic (Elastic Load Balancing ou ELB) proposé sur AWS vous permet d'équilibrer automatiquement le trafic réseau d'un ensemble de ressources cloud.

Quand vous utilisez des logs ELB centralisés, vous pouvez :

Observer des informations détaillées sur les requêtes envoyées par l'équilibreur de charge.

Analyser les tendances du trafic et résoudre les problèmes afin de détecter les défauts de performance

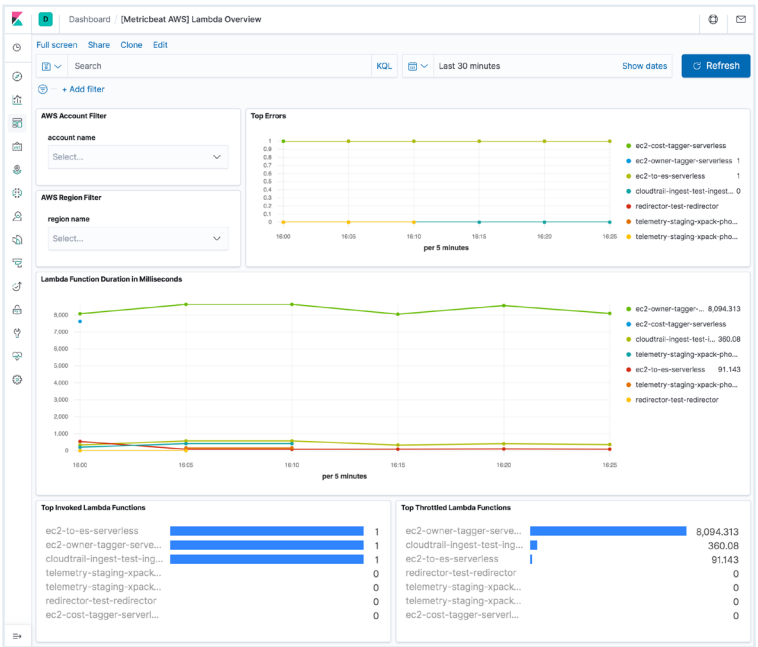
Mener des recherches dans les logs ELB pour identifier les réponses du serveur et autres.

Comment envoyer les données ELB à Elastic

Avant de vous lancer, vous devez rassembler quelques informations sur votre environnement AWS et votre déploiement Elastic Cloud. Consultez l'**Annexe A** pour en savoir plus sur ces prérequis. Pour vous lancer avec l'ELB sur AWS, suivez les étapes décrites dans l'**Annexe B** afin d'obtenir la marche à suivre détaillée concernant notamment les tâches suivantes :

1. Configuration d'un bucket Amazon S3 et création d'une file d'attente Amazon SQS
2. Téléchargement et installation de Filebeat
3. Connexion à la Suite Elastic
4. Configuration de Filebeat pour collecter les logs ELB sur AWS
5. Activation et configuration de vos modules de collecte des données
6. Configuration de vos tableaux de bord Kibana préconfigurés, puis démarrage de Filebeat
7. Analyse des logs ELB dans Kibana

Optimisation des workflows opérationnels à l'aide d'AWS Lambda dans Elastic



Grâce à AWS Lambda, vous bénéficiez d'un service de calcul sans serveur qui permet d'exécuter de manière dynamique du code pour réagir à des événements et optimiser les workflows opérationnels. Réalisez toute tâche informatique, gérez automatiquement vos ressources à l'aide d'un code adapté à toute application et libérez-vous de toute tâche administrative.

elastic

Quand vous utilisez AWS Lambda dans Elastic, vous pouvez :

Monitorer les performances de différentes applications sans serveur.

Traiter les logs et les indicateurs en temps réel.

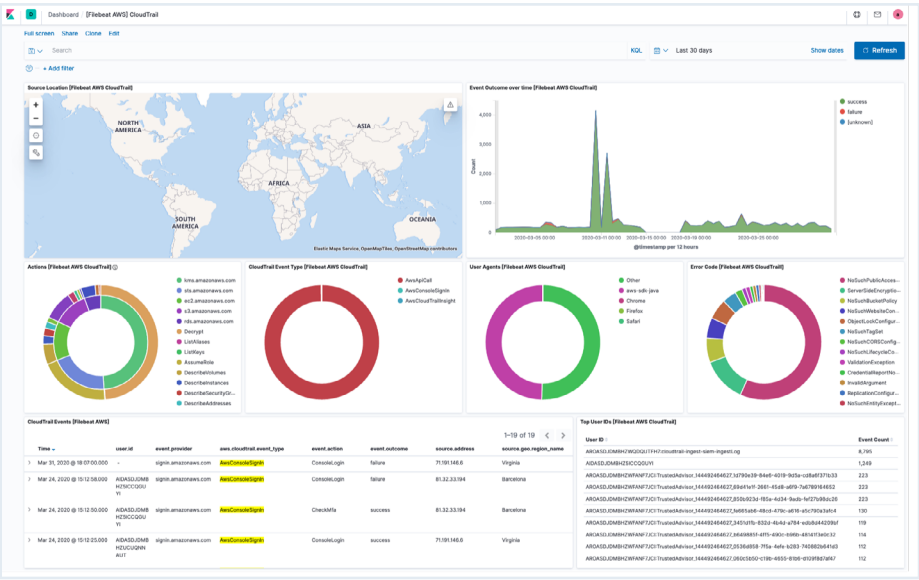
Capturer des données de performances et les mettre en corrélation avec les solutions d'Elastic.

Comment vous lancez avec AWS Lambda dans Elastic

Tout d'abord, rassemblez des informations sur votre environnement AWS et votre déploiement Elastic Cloud. Consultez l'**Annexe A** pour en savoir plus sur ces prérequis. Pour vous lancer avec AWS Lambda, suivez les étapes décrites dans l'**Annexe D** afin d'obtenir la marche à suivre détaillée concernant notamment les tâches suivantes :

1. Téléchargement et installation de Functionbeat
2. Connexion à la Suite Elastic
3. Configuration des fonctions de cloud
4. Activation et configuration des modules de collecte des données
5. Définition de ressources et déploiement de Functionbeat
6. Développement de tableaux de bord Kibana à des fins d'analyse

Respect des normes de gouvernance et de conformité avec AWS CloudTrail dans Elastic



elastic

AWS CloudTrail vous offre des fonctions de gouvernance, de conformité, mais aussi d'audit opérationnel et des risques de votre compte AWS.

Quand vous centralisez les logs d'AWS CloudTrail dans Elastic, vous pouvez facilement :

Visualiser vos logs AWS CloudTrail, mais aussi l'activité des utilisateurs et des comptes, le tout dans les tableaux de bord prédéfinis de Kibana à des fins d'analyse ultérieure.

Consigner des informations sur toutes les actions menées pour suivre les changements et résoudre les problèmes.

Sécuriser et monitorer vos connexions réseau.

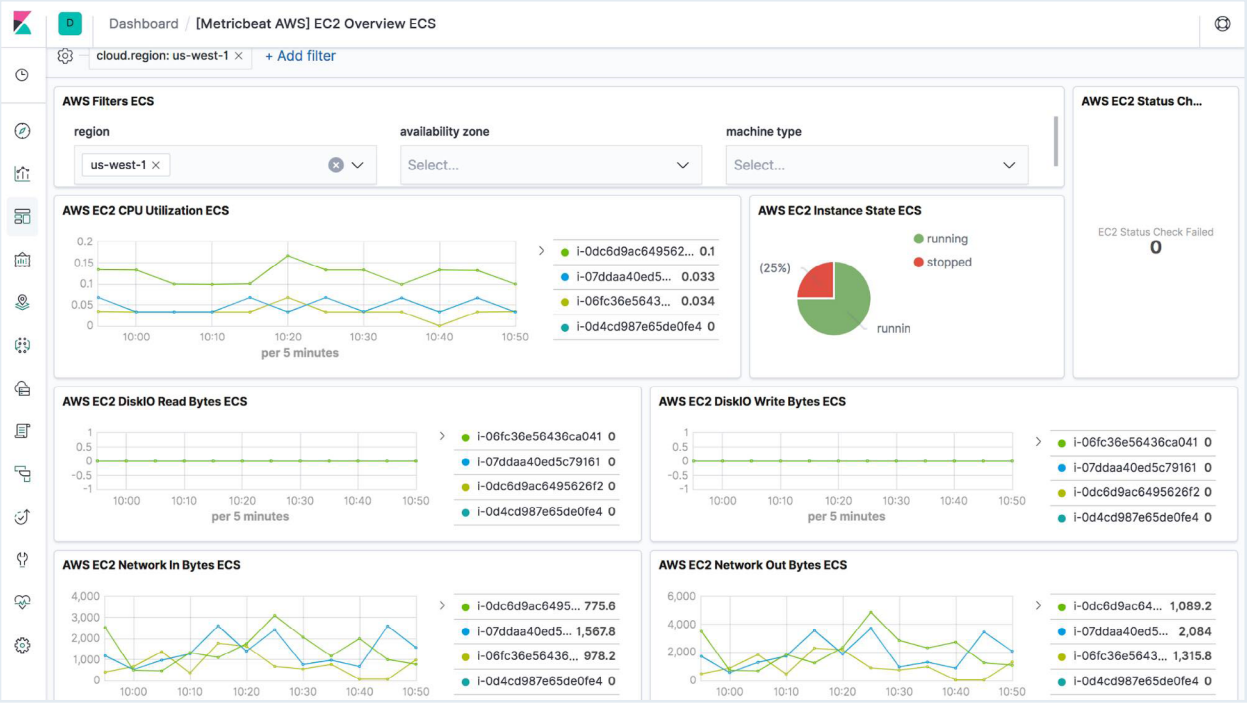
Garantir le respect des politiques et normes réglementaires.

Comment ingérer les données d'AWS CloudTrail dans Elastic

Avant de vous lancer, vous devez rassembler quelques informations sur votre environnement AWS et votre déploiement Elastic Cloud. Consultez l'**Annexe A** pour en savoir plus sur ces prérequis. Pour vous lancer avec AWS CloudTrail, suivez les étapes décrites dans l'**Annexe B** afin d'obtenir la marche à suivre détaillée concernant notamment les tâches suivantes :

1. Configuration d'un bucket Amazon S3 et création d'une file d'attente Amazon SQS
2. Téléchargement et installation de Filebeat
3. Connexion à la Suite Elastic
4. Configuration de Filebeat pour collecter les logs d'AWS CloudTrail
5. Activation et configuration de vos modules de collecte des données
6. Configuration de vos tableaux de bord Kibana préconfigurés et démarrage de Filebeat
7. Analyse des logs d'AWS CloudTrail dans Kibana

Ingestion et unification des indicateurs au sein de votre environnement AWS pour obtenir des informations exploitables exhaustives



Grâce aux intégrations d'Elastic et aux tableaux de bord prédéfinis pour AWS, vous pouvez collecter des indicateurs AWS sur l'utilisation, les performances et la facturation, notamment, afin de déterminer la manière dont chaque signal est mis en corrélation. Ainsi, vous êtes en mesure de prendre des décisions professionnelles plus éclairées.

Grâce à l'analyse et au monitoring permanents de vos indicateurs de données, de réseautage, de stockage et de calcul d'AWS, vous pouvez réagir rapidement en vue de satisfaire vos besoins métier en constante évolution.

- Amazon Relational Database Service (Amazon RDS)
- Amazon Elastic Block Store (Amazon EBS)
- Amazon Elastic Compute Cloud (Amazon EC2)
- Passerelle de traduction d'adresses réseau (NAT) d'Amazon VPC
- Amazon CloudWatch
- Amazon S3
- Amazon DynamoDB
- Amazon Simple Notification Service (SNS)
- Amazon SQS
- Rapport d'utilisation et des coûts d'AWS
- AWS Billing and Cost Management
- AWS Virtual Private Network (AWS VPN)
- AWS Transit Gateway

elastic

Les indicateurs d'AWS vous aident à réaliser des analyses complètes et prendre des décisions plus éclairées. Ainsi, vous pouvez :

Mettre les indicateurs en corrélation dans les services de données, de stockage et de calcul pour résoudre les problèmes de manière unifiée.

Évaluer les contraintes en matière de capacité, de performance et d'utilisation pour prendre des décisions de scaling globales.

Monitorer et assurer la maintenance d'un déploiement cloud optimisé à l'aide d'un alerting et d'une analyse automatisés grâce à un ensemble unifié de données.

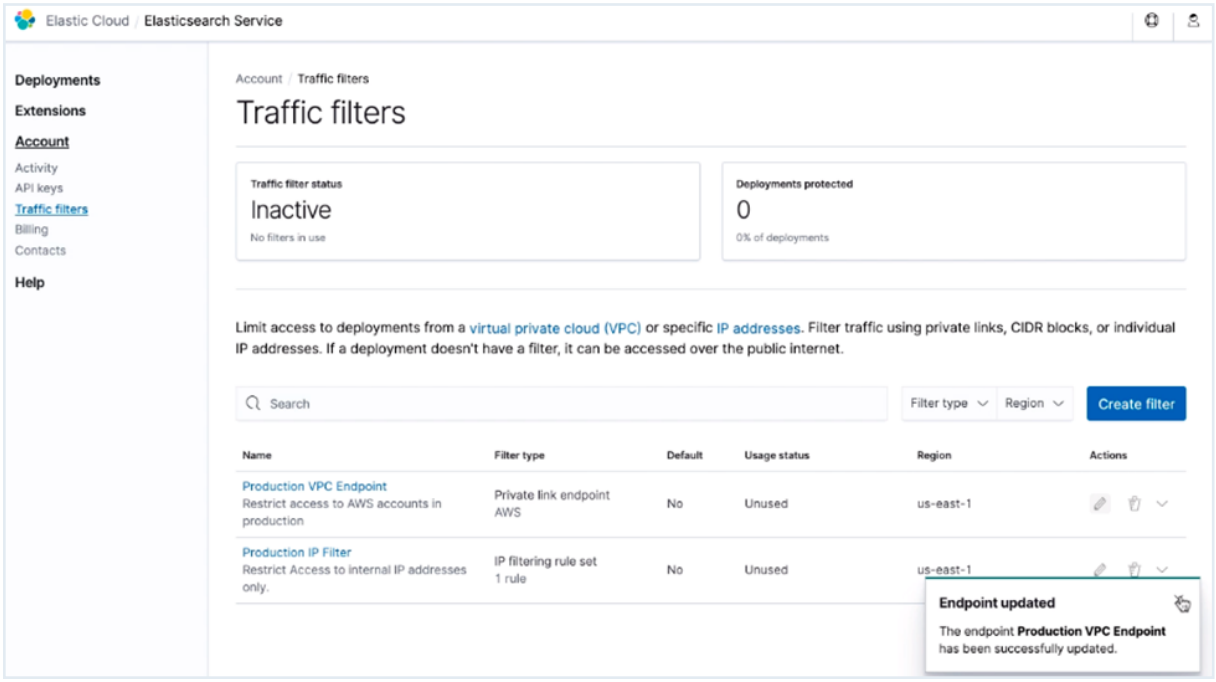
Comment vous lancer et utiliser les tableaux de bord personnalisés et les indicateurs AWS

Vous devez rassembler des informations sur votre environnement AWS et votre déploiement Elastic Cloud avant toute chose. Consultez l'**Annexe A** pour en savoir plus sur ces prérequis. Pour vous lancer dans la création de votre tableau de bord, suivez les étapes décrites dans l'**Annexe C** afin d'obtenir la marche à suivre détaillée concernant notamment les tâches suivantes :

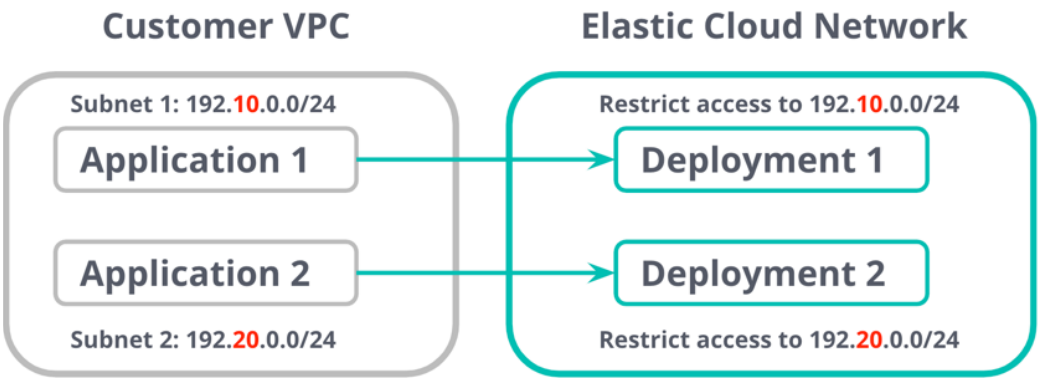
1. Téléchargement et installation de Metricbeat
2. Connexion à la Suite Elastic
3. Configuration de Metricbeat pour collecter des indicateurs
4. Activation et configuration de vos modules de collecte des données
5. Configuration de vos tableaux de bord Kibana préconfigurés et démarrage de Filebeat
6. Analyse de vos indicateurs dans Kibana

Pour apprendre à développer un tableau de bord personnalisé répondant à vos besoins, vous pouvez consulter notre **documentation** et ce **tutoriel vidéo** rapide.

Sécurité et flexibilité accrues offertes par Elastic grâce à AWS PrivateLink



AWS PrivateLink fournit une connectivité sécurisée entre vos Amazon VPC, vos ressources AWS supplémentaires et vos applications sur site. Vous pouvez ainsi sécuriser facilement la connexion réseau entre vos applications et votre déploiement Elastic. Le trafic entre le réseau virtuel et votre déploiement Elastic utilise le réseau AWS au lieu de l'Internet public, ce qui évite les risques d'exposition des données et vous fournit une sécurité accrue.



elastic

Grâce à AWS PrivateLink, vous pouvez :

Créer des points de terminaison à l'aide d'adresses IP. Ainsi, les charges de travail semblent s'exécuter au sein de votre réseau.

Vérifier que l'ensemble du trafic reste sur le réseau d'Amazon et ne s'en échappe pas.

Bénéficier d'une gestion simplifiée du réseau. Vous n'avez plus besoin d'assurer la maintenance d'une infrastructure complexe (passerelles NAT, contrôles des accès).

Restreindre le trafic provenant de réseaux virtuels de clients aux points de terminaison. (Le trafic d'AWS PrivateLink est unidirectionnel, alors que celui dans le peering d'Amazon VPC est bidirectionnel.)

Comment vous lancer avec AWS PrivateLink

Consultez notre **documentation** pour obtenir des instructions détaillées.

Pourquoi choisir Elastic ?

Déployez Elastic pour apporter un ensemble de fonctionnalités complémentaires au cloud et ainsi optimiser la valeur de vos investissements AWS.

Comment Elastic Observability et les fonctionnalités de sa plateforme de recherche sous-jacente alimentent les innovations en matière d'infrastructure cloud

Depuis sa création, Elastic a fourni un flux constant d'innovations en matière d'analyse des données et de recherche, mais aussi a redéfini la valeur de cette dernière. Elastic, l'entreprise qui a créé Elasticsearch et Kibana, ajoute en permanence de nouvelles fonctionnalités, mises à jour de sécurité et améliorations de performance à ces produits. Les innovations d'Elastic en matière de recherche au niveau des applications logicielles viennent en complément de celles d'AWS dans l'infrastructure du cloud. Ainsi, vous pouvez rapidement réagir aux données opérationnelles et métier, ce qui vous aide à rendre votre entreprise plus agile et orientée vers les données.

Choix et flexibilité entre les fournisseurs cloud et les solutions sur site

La plateforme de recherche d'Elastic est conçue pour conférer aux développeurs et aux clients une flexibilité d'exécution à partir de l'emplacement de leur choix. De solides investissements permettent de développer des fonctionnalités essentielles au sein de la plateforme en parallèle d'intégrations poussées dans le cloud. La plateforme de recherche d'Elastic offre aussi une expérience cohérente dans le cloud et sur site. Cette cohérence hybride est précieuse à mesure que vous augmentez l'utilisation de votre cloud, un processus qui peut prendre des années dans les grandes entreprises.

La cohérence entre plusieurs clouds peut également faciliter l'élargissement de votre solution si vous choisissez d'étendre l'utilisation de votre cloud afin d'ajouter les meilleurs services fournis par les fournisseurs cloud. Cela est particulièrement important pour les cas d'utilisation de sécurité et d'observabilité : grâce à une vue unifiée des différents emplacements, les clients accélèrent le dépannage et diminuent les risques.

Solutions prêtes à l'emploi pour Enterprise Search, Observability et Security

Elastic fournit des applications prédéfinies et prêtes à l'emploi pour les cas d'utilisation d'Enterprise Search, y compris Workplace Search, App Search et Site Search, ceux d'Observability, dont le logging et le monitoring des performances applicatives, mais aussi ceux de Security, notamment le SIEM et la protection aux points de terminaison.

Toutes les fonctionnalités et les intégrations externes sur lesquelles reposent ces applications spécialement conçues pour les solutions sont intégrées à la plateforme de recherche d'Elastic et disponibles pour les clients qui souhaitent développer leurs propres applications personnalisées afin de répondre à leurs besoins. Il s'agit notamment des vastes intégrations conçues afin d'ingérer les données requises pour les solutions Observability et Security dans AWS.

Communauté et talents techniques

La plateforme de recherche d'Elastic est de facto une norme relative aux solutions optimisées pour la recherche. La communauté GitHub d'Elasticsearch comprend plus de 1 500 membres. En outre, les compétences relatives à Elasticsearch et à Kibana sont bien établies au sein du secteur. Elasticsearch inclut également des intégrations immédiatement disponibles pour les sources de données et les applications adjacentes couramment utilisées. En exploitant Elastic Observability avec AWS, vous pouvez utiliser ces ressources (ensemble de talents, intégrations et communauté collaborative d'Elasticsearch) à mesure de l'évolution de vos solutions optimisées pour la recherche.

Échanges avec la communauté Elastic

Forums de discussion

Obtenez des conseils ou prêtez main forte. Posez toutes vos questions concernant Elastic et faites profiter d'autres utilisateurs de votre savoir sur nos **forums de discussion**, qui sont également disponibles dans votre langue natale.

Communautés Slack et locales

Inscrivez-vous à notre équipe **Elastic Slack** afin de discuter avec d'autres utilisateurs et de demander des conseils dans différents canaux, comme #elasticsearch, #kubernetes et #kibana-development dédié au développement de Kibana.

En outre, de nombreuses **autres communautés en ligne** ont vu le jour un peu partout dans le monde. Rejoignez l'une d'entre elles dans votre région pour parler de votre expérience avec Elastic à la communauté locale.

Apprentissage continu

Vous découvrez la Suite Elastic ou vous explorez nos solutions plus en profondeur ? Obtenez des informations pratiques à l'aide du **référentiel d'exemples Elastic**, découvrez des ensembles de données conçus avec soin et bénéficiez d'instructions détaillées. En outre, lisez notre **newsletter de la communauté** pour savoir sur quoi travaille notre équipe de développement.

Vos commentaires

Elastic évolue au rythme des innovations technologiques. Dans cette optique, l'avis de notre communauté est précieux. Nous vous encourageons donc à **nous contacter** pour nous parler de votre expérience Elastic.

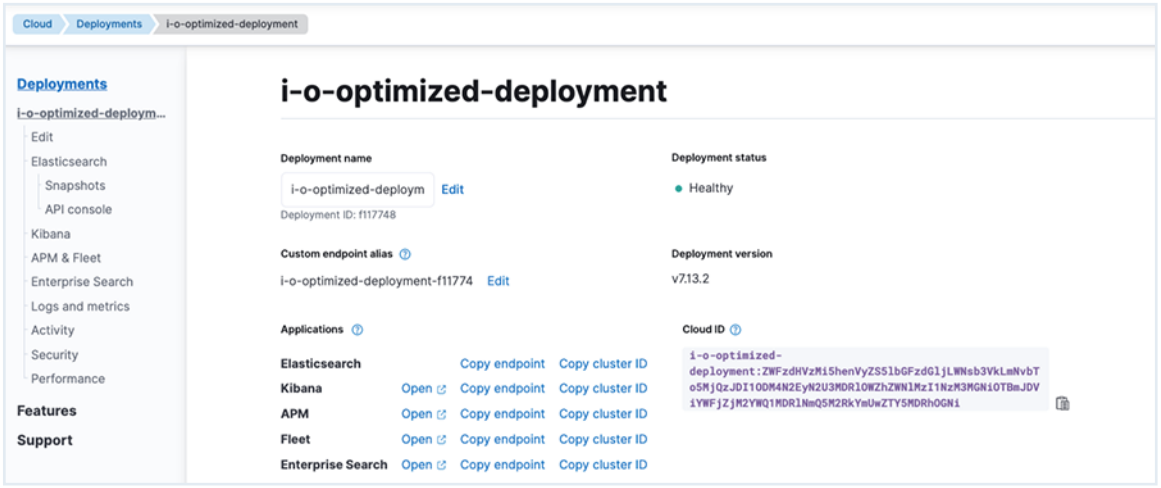
Annexe A – prérequis pour se lancer

Suivez les instructions ci-dessous pour obtenir les informations suivantes avant de commencer à ingérer vos données AWS :

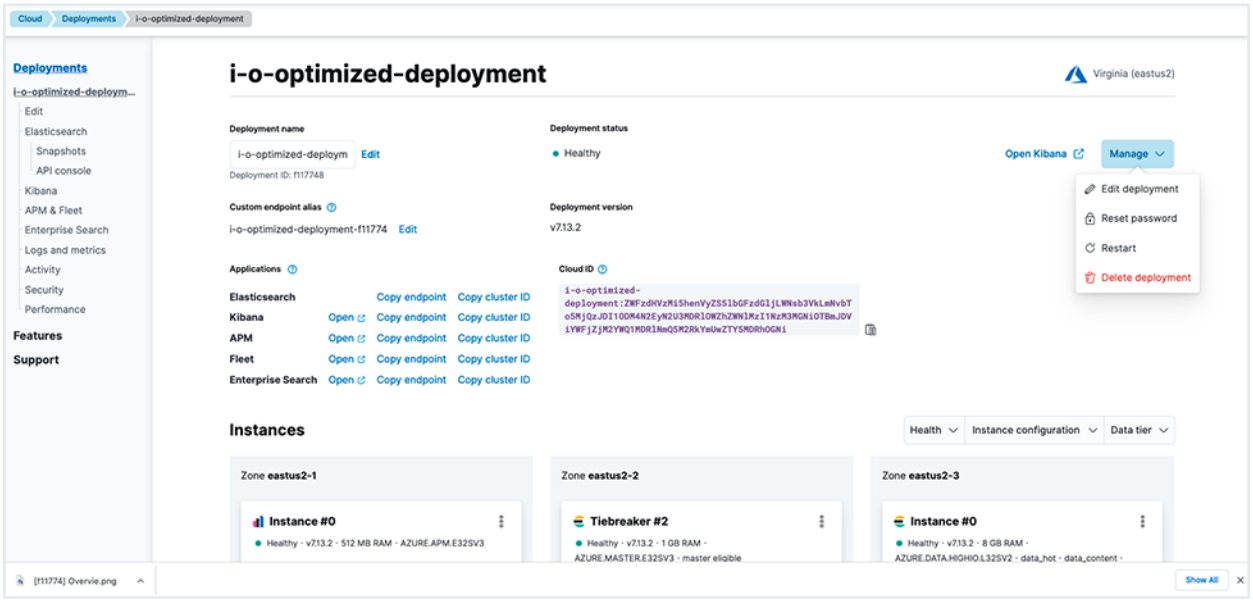
- Localisez l'identifiant du cloud.
- Obtenez les identifiants de connexion.
- Créez la clé d'accès AWS et son identifiant.

Localisation de l'identifiant du cloud

Pour trouver l'identifiant de votre cloud, accédez à la page cloud.elastic.co et sélectionnez le déploiement concerné.



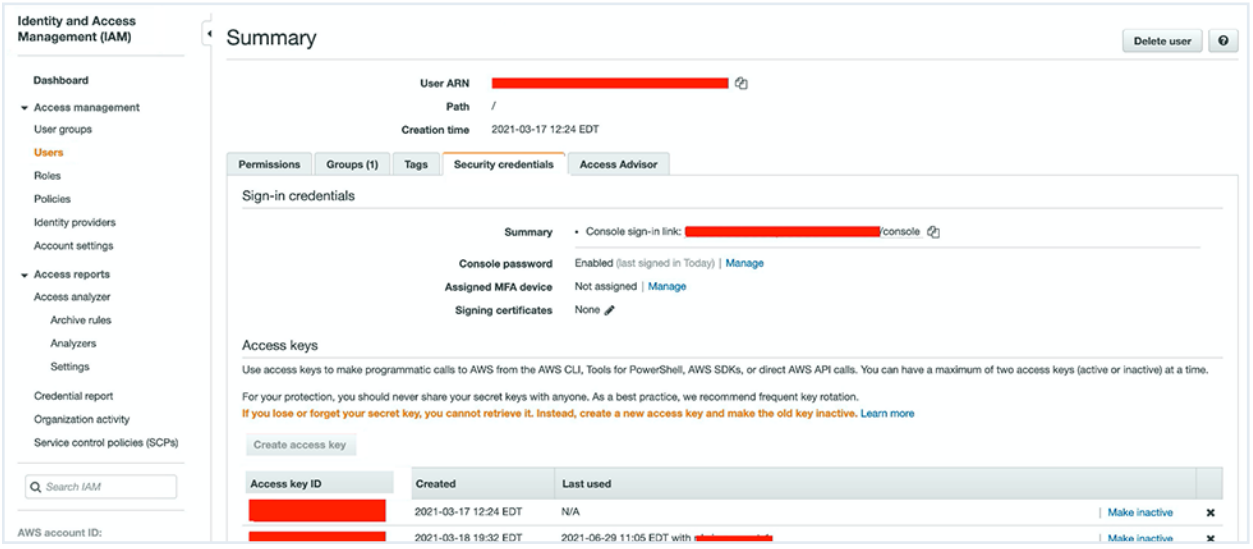
Obtention des identifiants de connexion



Lorsque vous envoyez des données à Elasticsearch, vous pouvez utiliser le nom d'utilisateur par défaut, à savoir "Elastic", et le mot de passe que vous avez obtenu à la création du cluster. Autre solution, vous pouvez configurer des utilisateurs et des rôles dédiés dotés des privilèges minimaux requis pour réaliser ces tâches. Dans cet exemple, nous utilisons le nom d'utilisateur "Elastic" et le mot de passe fourni.

Si vous n'avez pas téléchargé pas ce mot de passe ou l'avez oublié, accédez à la page cloud.elastic.co et réinitialisez le mot de passe en cliquant sur "Manage" (Gérer).

Création de la clé d'accès AWS et de son identifiant



La clé d'accès AWS et son identifiant permettent de signer vos requêtes programmatiques auprès d'AWS. Pour obtenir ces informations :

- Connectez-vous à AWS Identity and Access Management et accédez à la console IAM sur la page **https://console.aws.amazon.com/iam/**.
- Sélectionnez "Users" (Utilisateurs) dans le volet de navigation.
- Choisissez l'utilisateur de votre choix, puis sélectionnez l'onglet "Security credentials" (Identifiants de sécurité).
- Dans la section "Access Keys" (Clés d'accès), cliquez sur "Create access key" (Créer une clé d'accès). Pour voir la paire de clés d'accès, sélectionnez "Show" (Afficher), puis copiez les données et enregistrez-les afin de configurer Filebeat et Metricbeat.

Annexe B – configuration de Filebeat

Vous trouverez ci-dessous des instructions détaillées concernant l'installation de Filebeat etl'activation des modules AWS. Veuillez procéder comme suit :

1. Configuration d'un bucket Amazon S3 et création d'une file d'attente Amazon SQS
2. Téléchargement et installation de Filebeat
3. Connexion à la Suite Elastic
    - À cette étape, vous avez besoin de l'identifiant et du mot de passe de votre cloud pour votre déploiement Elastic.
4. Activation et configuration de votre module Filebeat
5. Configuration de Filebeat pour collecter vos logs AWS
    - À cette étape, vous avez besoin du code de votre module AWS, mais aussi de la clé d'accès AWS et de son identifiant.
6. Configuration de vos tableaux de bord Kibana préconfigurés et démarrage de Filebeat
7. Affichage et visualisation des données dans Kibana

1ère étape : configuration d'un bucket Amazon S3 et création d'une file d'attente Amazon SQS

Pour éviter tout retard important lors de l'interrogation de l'ensemble des fichiers de logs provenant de chaque bucket Amazon S3, Filebeat associe la notification à l'interrogation en utilisant Amazon SQS pour la notification Amazon S3 lors de la création d'un nouvel objet Amazon S3. Lisez l'article intitulé **Configuration des notifications des événements S3 à l'aide d'Amazon SQS** pour savoir comment configurer votre bucket Amazon S3 et votre file d'attente Amazon SQS.

2e étape : téléchargement et installation de Filebeat

Téléchargez et installez Filebeat. Utilisez les commandes adaptées à votre système.

- Dans cet exemple, nous utilisons les commandes Linux. Pour trouver la dernière version, accédez à la **documentation de Filebeat**, puis sélectionnez "Quick start: installation and configuration" (Démarrage rapide : installation et configuration). Vous trouverez également les commandes d'autres systèmes d'exploitation.

```
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
```

3e étape : connexion à la Suite Elastic

Pour configurer Filebeat, il faut se connecter à Elasticsearch et à Kibana. Vous devrez modifier le fichier de configuration intitulé filebeat.yml.

À cette étape, vous devez utiliser l'identifiant et le mot de passe de votre cloud que vous avez obtenus. Indiquez l'**cloud.id** de votre Elasticsearch Service, puis configurez **cloud.auth** (nom d'utilisateur : mot de passe) pour un utilisateur autorisé à configurer Filebeat. Par exemple :

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

Pour bénéficier d'une sécurité accrue, vous pouvez exploiter le **magasin de clés de Filebeat** afin de masquer les identifiants (nom d'utilisateur, mot de passe, cloud.id, etc.). Ensuite, créez des rôles et utilisateurs dédiés dotés des autorisations minimales requises pour la tâche concernée. Dans cet exemple, nous utilisons le nom d'utilisateur et le mot de passe par défaut que vous avez obtenus à la création de votre déploiement. En outre, vous utilisez le superutilisateur par défaut comme exemple. Pour la mise en production, configurez des rôles et des utilisateurs dotés des **privilèges minium nécessaires** pour réaliser la tâche concernée.

Assurez-vous de créer un rôle personnalisé pour la fonction déployée. Par exemple :

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

Vérifiez que le rôle personnalisé est doté des autorisations requises pour exécuter la fonction.
Pour en savoir plus, consultez les **autorisations IAM requises pour le déploiement**.

4e étape : activation et configuration des modules de collecte des données

Pour activer le module AWS, accédez au répertoire de Filebeat et saisissez la commande suivante :

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

5e étape : configuration de Filebeat pour collecter vos indicateurs AWS

Accédez aux configurations du module AWS dans le répertoire modules.d du fichier aws.yml. Si vous ne détenez pas le code pour l'intégration recherchée, vous le trouverez dans l'**Annexe E**.

Vous avez aussi besoin des identifiants AWS que vous avez obtenus à l'Annexe A afin d'ajouter le fichier aws.yml au début :

- access_key_id: "VOTRE CLÉ D'ACCÈS SECRÈTE AWS"
- secret_access_key: "VOTRE CLÉ D'ACCÈS AWS"

Si vous préférez utiliser une autre méthode d'authentification, consultez les **options d'identifiants AWS** pour en savoir plus.

Veuillez consulter l'exemple ci-dessous pour ajouter votre clé d'accès AWS et son identifiant :

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

Veuillez consulter l'exemple ci-dessous pour ajouter votre rôle IAM :

```
module: aws
#AWS IAM Role to assume
var.role_arn: arniam::123456789012:role/test-mb
```

Remarque : vous pouvez utiliser le **magasin de clés de Filebeat** pour masquer votre clé d'accès AWS et son identifiant.

6e étape : configuration de vos tableaux de bord Kibana préconfigurés et démarrage de Filebeat

Filebeat est doté de ressources prédéfinies pour l'analyse, l'indexation et la visualisation de vos données. Pour charger ces ressources :

- Assurez-vous que l'utilisateur indiqué dans le fichier filebeat.yml est **autorisé à configurer Filebeat** si vous n'utilisez pas l'utilisateur "elastic" (par défaut).
- Pour le répertoire d'installation, exécutez la commande suivante :

  ```
  ./filebeat setup -e
  ```

Avant de lancer Filebeat, modifiez les identifiants d'utilisateur dans le fichier filebeat.yml et indiquez un utilisateur autorisé à publier des événements.

Pour démarrer Filebeat, utilisez les commandes suivantes :

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

7e étape : affichage et visualisation des données dans Kibana

Filebeat est doté de tableaux de bord Kibana prédéfinis, d'une application Logs dédiée pour visualiser, rechercher et filtrer des données de logs, mais aussi de la détection des anomalies facile à configurer. Lorsque vous avez exécuté la commande de configuration, vous avez chargé les tableaux de bord.

Pour lancer Kibana :

- **Connectez-vous** à votre compte Elastic Cloud.
- Accédez au point de terminaison Kibana dans votre déploiement pour consulter et analyser vos données.

Annexe C – configuration de Metricbeat

Vous trouverez ci-dessous des instructions détaillées concernant l'installation de Metricbeat et l'activation des modules AWS. Veuillez procéder comme suit :

1. Téléchargement et installation de Metricbeat
2. Connexion à la Suite Elastic
   - À cette étape, vous avez besoin de l'identifiant et du mot de passe de votre cloud pour votre déploiement Elastic.
3. Activation et configuration des modules de collecte des données
4. Configuration de Filebeat pour collecter vos indicateurs AWS
   - À cette étape, vous avez besoin du code de votre module AWS, mais aussi de la clé d'accès AWS et de son identifiant.
5. Configuration de vos tableaux de bord Kibana préconfigurés et démarrage de Metricbeat
6. Affichage et visualisation des données dans Kibana

1ère étape : téléchargement et installation de Metricbeat

Téléchargez et installez Metricbeat. Utilisez les commandes adaptées à votre système.

Dans cet exemple, nous utilisons les commandes Linux. Pour trouver la dernière version, accédez à la **documentation de Metricbeat**, puis sélectionnez "Quick start: installation and configuration" (Démarrage rapide : installation et configuration). Vous trouverez également les commandes d'autres systèmes d'exploitation.

```
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
```

2e étape : connexion à la Suite Elastic

Lors de la configuration de Metricbeat, vous devez modifier le fichier de configuration metricbeat.yml.

À cette étape, vous devez utiliser l'identifiant et le mot de passe de votre cloud que vous avez obtenus. Indiquez l'**cloud.id** de votre Elasticsearch Service, puis configurez **cloud.auth** (nom d'utilisateur : mot de passe) pour un utilisateur autorisé à configurer Metricbeat. Par exemple :

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

Pour bénéficier d'une sécurité accrue, vous pouvez exploiter le **magasin de clés de Metricbeat** afin de masquer les identifiants (nom d'utilisateur, mot de passe, cloud.id, etc.). Ensuite, créez des rôles et utilisateurs dédiés dotés des autorisations minimales requises pour la tâche concernée. Dans cet exemple, nous utilisons le nom d'utilisateur et le mot de passe par défaut que vous avez obtenus à la création de votre déploiement. En outre, vous utilisez le superutilisateur par défaut comme exemple. Pour la mise en production, configurez des rôles et des utilisateurs dotés des **privilèges minium nécessaires** pour réaliser la tâche concernée.

Assurez-vous de créer un rôle personnalisé pour la fonction déployée. Par exemple :

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

Vérifiez que le rôle personnalisé est doté des autorisations requises pour exécuter la fonction. Pour en savoir plus, consultez les **autorisations IAM requises pour le déploiement**.

3e étape : activation et configuration des modules de collecte des données

Lors de la configuration de Metricbeat, vous devez indiquer les modules à exécuter. Metricbeat utilise des modules pour collecter des indicateurs. Pour activer la configuration aws dans le répertoire modules.d, saisissez la commande suivante :

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

4e étape : configuration de Metricbeat pour collecter vos indicateurs AWS

Accédez aux configurations du module AWS dans le répertoire modules.d du fichier aws.yml. Si vous ne détenez pas le code pour l'intégration recherchée, vous le trouverez dans l'**Annexe E**.

Vous avez aussi besoin de vos identifiants AWS afin d'ajouter le fichier aws.yml au début :

- access_key_id: "VOTRE CLÉ D'ACCÈS SECRÈTE AWS"
- secret_access_key: "VOTRE CLÉ D'ACCÈS AWS"

Si vous préférez utiliser une autre méthode d'authentification, consultez les **options d'identifiants AWS** pour en savoir plus.

Veuillez consulter l'exemple ci-dessous pour ajouter votre clé d'accès AWS et son identifiant :

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

Veuillez consulter l'exemple ci-dessous pour ajouter votre rôle IAM :

```
module: aws
#AWS IAM Role to assume
role_arn: arniam::123456789012:role/test-mb
```

Remarque : vous pouvez utiliser le **magasin de clés de Metricbeat** pour masquer votre clé d'accès AWS et son identifiant.

5e étape : configuration de vos tableaux de bord Kibana préconfigurés et démarrage de Metricbeat

Metricbeat est doté d'exemples de tableaux de bord Kibana, de visualisations et de recherches pour afficher les données des indicateurs AWS dans Kibana, mais aussi de l'alerting et de la détection des anomalies faciles à configurer.

- Assurez-vous que l'utilisateur indiqué dans le fichier metricbeat.yml est **autorisé à configurer Metricbeat** si vous ne vous servez pas de l'utilisateur "elastic" (par défaut).
- Pour le répertoire d'installation, exécutez la commande suivante :

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

Pour démarrer Metricbeat, utilisez les commandes suivantes :

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

6e étape : affichage et visualisation des données dans Kibana

Metricbeat est doté de tableaux de bord Kibana prédéfinis et d'une application dédiée à la visualisation des données des indicateurs. Lorsque vous avez exécuté la commande de configuration, vous avez chargé les tableaux de bord.

Pour lancer Kibana :

- **Connectez-vous** à votre compte Elastic Cloud.
- Accédez au point de terminaison Kibana dans votre déploiement.

Annexe D – configuration de Functionbeat

Vous trouverez ci-dessous des instructions détaillées concernant l'installation de Functionbeat et l'activation des modules AWS. Veuillez procéder comme suit :

1. Téléchargement et installation de Functionbeat
2. Connexion à la Suite Elastic
   - À cette étape, vous avez besoin de l'identifiant et du mot de passe de votre cloud pour votre déploiement Elastic.
3. Configuration des fonctions de cloud
   - À cette étape, vous avez besoin du code de votre module AWS, mais aussi de la clé d'accès AWS et de son identifiant.
4. Configuration des ressources et déploiement de Functionbeat
5. Développement de vos tableaux de bord Kibana à des fins d'analyse

1ère étape : téléchargement et installation de Functionbeat

Téléchargez et installez Metricbeat. Utilisez les commandes adaptées à votre système.

- Dans cet exemple, nous utilisons les commandes Linux. Consultez notre **documentation** pour les commandes d'autres systèmes d'exploitation.

```
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
```

2e étape : connexion à la Suite Elastic

Pour configurer Filebeat, il faut se connecter à Elasticsearch et à Kibana. Vous devrez modifier le fichier de configuration functionbeat.yml.

À cette étape, vous devez utiliser l'identifiant et le mot de passe de votre cloud que vous avez obtenus. Indiquez l'**cloud.id** de votre Elasticsearch Service, puis configurez **cloud.auth** (mot de passe) pour un utilisateur autorisé à configurer Functionbeat. Par exemple :

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

Assurez-vous de créer un rôle personnalisé pour la fonction déployée. Par exemple :

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

Vérifiez que le rôle personnalisé est doté des autorisations requises pour exécuter la fonction.
Pour en savoir plus, consultez les **autorisations IAM requises pour le déploiement**.

3e étape : configuration de vos fonctions de cloud

Avant de déployer Functionbeat sur AWS, vous devez fournir les informations sur les fonctions du cloud que vous souhaitez déployer, comme leur nom et leur type, mais aussi les déclencheurs de l'exécution des fonctions.

Dans le fichier functionbeat.yml, configurez les fonctions que vous souhaitez déployer. Les paramètres de configuration dépendent du type de fonction et de fournisseur cloud auquel vous faites appel. Si vous ne détenez pas le code pour l'intégration recherchée, vous le trouverez dans l'**Annexe E**. Cette section présente un exemple de configuration.

```
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
```

Vous avez aussi besoin de vos identifiants AWS. Configurez-les au début du fichier functionbeat.yml :

- access_key_id: "VOTRE CLÉ D'ACCÈS SECRÈTE AWS"
- secret_access_key: "VOTRE CLÉ D'ACCÈS AWS"

Si vous préférez utiliser une autre méthode d'authentification, consultez les **options d'identifiants AWS** pour en savoir plus.

Veuillez consulter l'exemple ci-dessous :

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

4e étape : configuration des ressources et déploiement de Functionbeat

Functionbeat est doté de ressources prédéfinies pour l'analyse, l'indexation et la visualisation de vos données. Pour charger ces ressources :

Vérifiez que l'utilisateur indiqué dans functionbeat.yml est **autorisé à configurer Functionbeat**.
Pour le répertoire d'installation, exécutez la commande suivante :

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

Pour déployer les fonctions de cloud, utilisez les commandes suivantes :

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

La fonction est déployée dans AWS et peut envoyer des événements de logs à la sortie configurée.

5e étape : développement de vos tableaux de bord Kibana à des fins d'analyse

Maintenant, vous pouvez développer vos tableaux de bord dans Kibana. Pour apprendre à afficher et à explorer vos données, consultez le **guide d'utilisateur de Kibana**. Pour lancer Kibana :

- **Connectez-vous** à votre compte Elastic Cloud.
- Accédez au point de terminaison Kibana dans votre déploiement.

Annexe E – pour aller plus loin

Pour les configurations AWS avancées, consultez ces documents dédiés :

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

elastic

Search. Observe. Protect.

Elastic garantit des données exploitables en temps réel et à grande échelle pour les tâches de recherche d'entreprise, d'observabilité et de sécurité. Ses solutions, déployables partout, se fondent sur une seule pile technologique gratuite et ouverte. Vous bénéficiez alors instantanément de données exploitables (recherches de documents, monitoring d'infrastructure ou détection des menaces). Des milliers d'organisations ont adossé leurs systèmes stratégiques à Elastic, notamment Cisco, Goldman Sachs, Microsoft, The Mayo Clinic, la NASA, The New York Times, Wikipédia ou Verizon. Fondée en 2012, Elastic est cotée à la bourse de New York (NYSE, symbole ESTC). En savoir plus sur elastic.co/fr.

SIÈGE AMÉRICAIN
800 West El Camino Real, Suite 350, Mountain View, California 94040
Général : +1 650 458 2620 ; ventes : +1 650 458 2625

info@elastic.co