Configurer les alertes

Les alertes de Cisco Secure Workload vous aident à surveiller la sécurité de la charge de travail et à réagir aux menaces potentielles. Les différents composants des alertes fonctionnent ensemble pour fournir une visibilité, les sources et configuration des alertes, et la capacité d'envoyer des alertes à partir des serveurs de publication d'alertes. Vous pouvez configurer des alertes, afficher les règles de leur déclencheur et choisir les serveurs de publication d'alertes à qui les envoyer. Les alertes affichées sur la page de configuration varient selon le rôle de l'utilisateur. Les serveurs de publication d'alertes peuvent être des alertes ou des notificateurs.

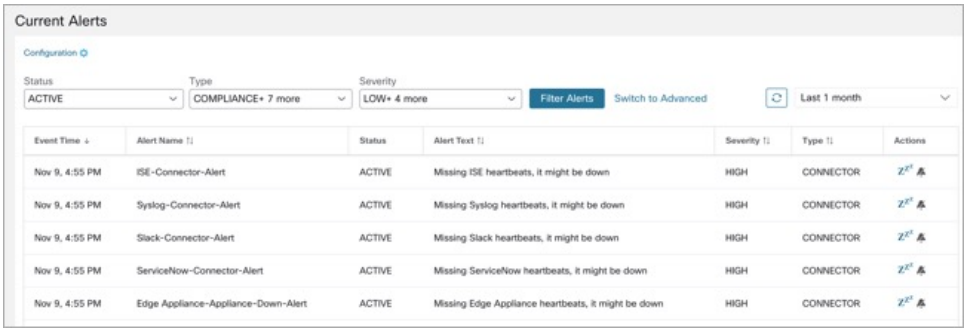
Remarque À partir de la version Secure Workload 3.0, l' Cisco Secure WorkloadApp Store ne prend pas en charge les applications d'alertes et de conformité. Vous pouvez configurer des alertes et des alertes de conformité sur cette page sans créer d'instance d'application d'alerte ou d'application de conformité.

Types d'alertes et serveurs de publication

Les alertes Cisco Secure Workload se composent des éléments suivants :

1. **Visibilité des alertes :**
   - **Alertes actuelles**: dans le volet de navigation, choisissez **Investigate (Investiguer)** > **Alerts (Alertes).** Un aperçu des alertes est envoyé à un surveilleur de données.

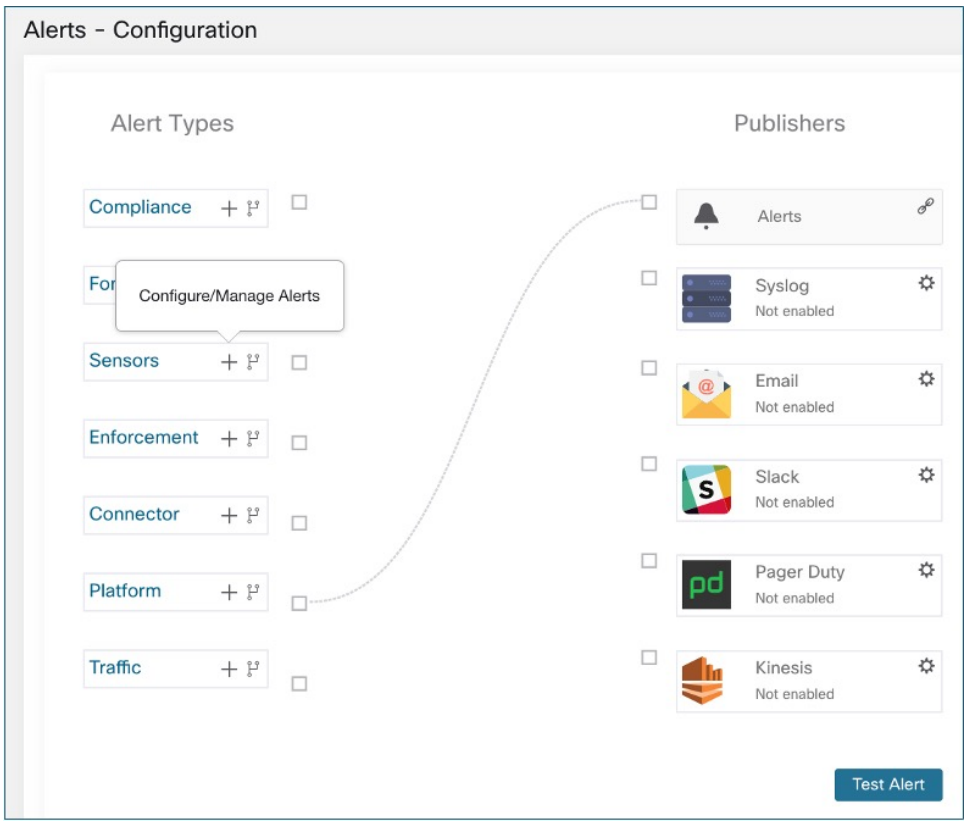
Figure 1: Alertes actuelles



2. **Source et configuration des alertes**

   - **Alertes-Configuration** : Accédez à **Manage (Gestion)** > **Alerts Configs (Configuration des alertes)** . Les configurations d'alertes qui sont configurées à l'aide du serveur de publication modal et d'alertes commun et les paramètres de l'émetteur de notifications sont affichées.

Figure 2: Alertes - Configuration



3. **Envoyer des alertes**

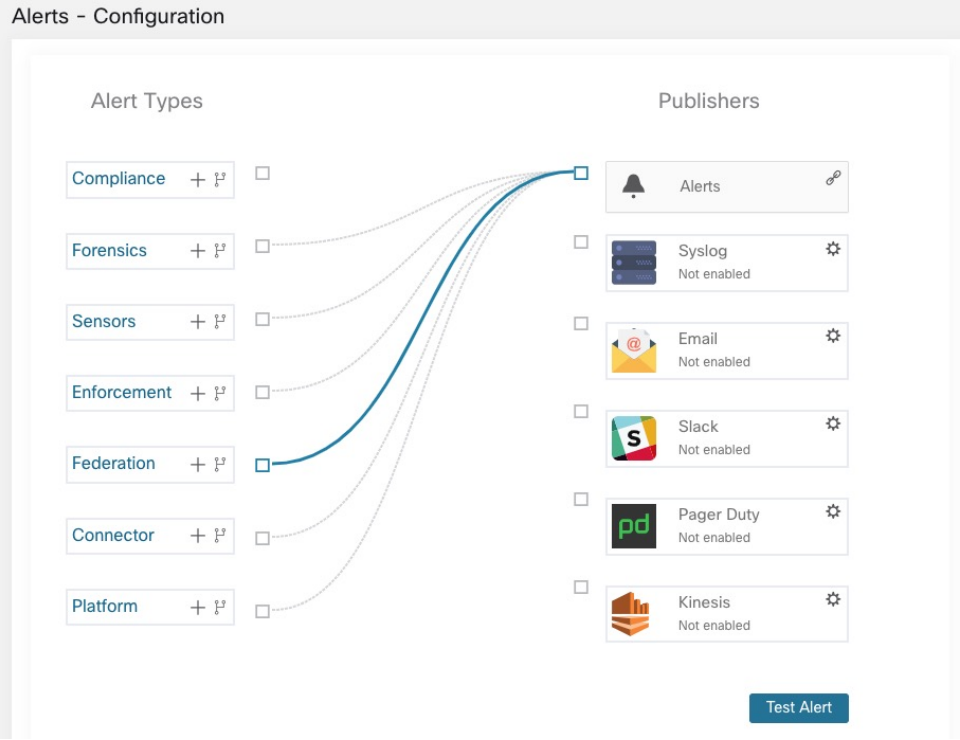
   - **Application Alerts** : une application Cisco Secure Workload implicite qui envoie les alertes générées à un surveilleur de données configuré. L'application Alerts gère des fonctionnalités telles que la **répétition** et la **sourdine**.

- **Serveur de publication d'alertes** : limite le nombre d'alertes affichées et envoie les alertes à Kafka (MDT ou surveilleur de données Data Tap) pour utilisation externe.
- **Appareil de périphérie** : envoie des alertes à d'autres systèmes comme Slack, PagerDuty, Courriel, etc.

Créer des alertes

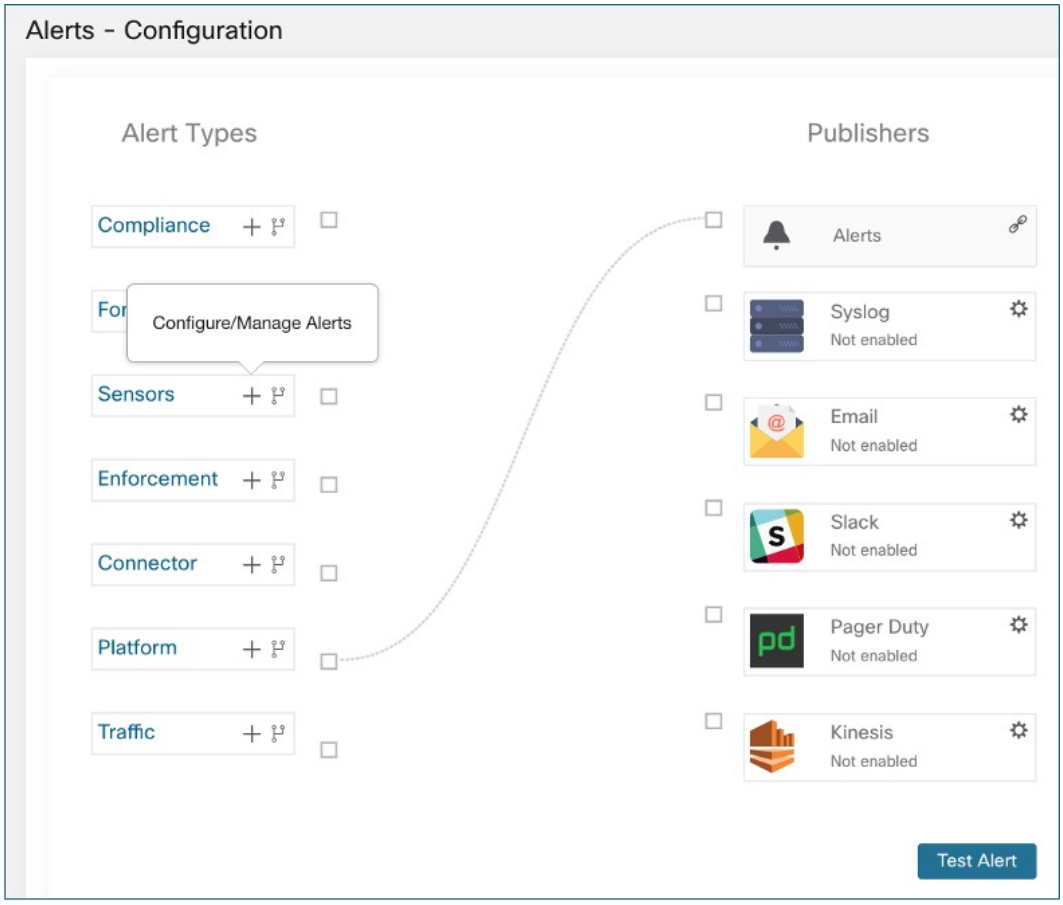
Dans le volet de navigation, choisissez **Alerts** > **Configuration** (configuration des alertes) pour créer des alertes :

Figure 3: Créer une alerte (règle de déclenchement)



Dans le volet de navigation, choisissez **Alerts (Alertes)** > **Configuration(Configuration)** pour configurer les types d'alertes suivants :

Figure 4: Créer une alerte



- **Alertes de mise en application**
  - Accessibilité de l'agent
  - Pare-feu de charge de travail
  - Politique de charge de travail
- **Alertes de capteurs**
  - Mise à niveau de l’agent
  - Exportation du flux de l’agent
  - Connection de l'agent
  - Utilisation de la mémoire de l’agent
  - Quota de CPU (processeur) de l’agent
  - Quantité d’observations de flux
  - Nouvel agent enregistré
  - État Pcap

- Agent désinstallé
- Chiffrement non recommandé
- Version TLS obsolète
- Suppression automatique de l'agent

- **Alertes de conformité**
  - Politique de mise en application
  - Politique d'analyse en direct

Note

- Les règles de déclencheur d'alerte sont appliquées à la portée racine actuellement sélectionnée pour les types d'alertes Enforcement (Application) et Sensors (Capteurs).
- Vous devez avoir une capacité appliquée sur la portée actuellement sélectionnée pour créer une règle de déclencheur d'alerte pour le type d'alerte de conformité.

Les types d'alertes suivants ne possèdent pas de boîte de dialogue modale de configuration :

- Criminalistique
- Connecteurs
- Fédération
- amiral

Boîte de dialogue modale de configuration des alertes

La boîte de dialogue modale de configuration d'alerte se compose des sections suivantes :

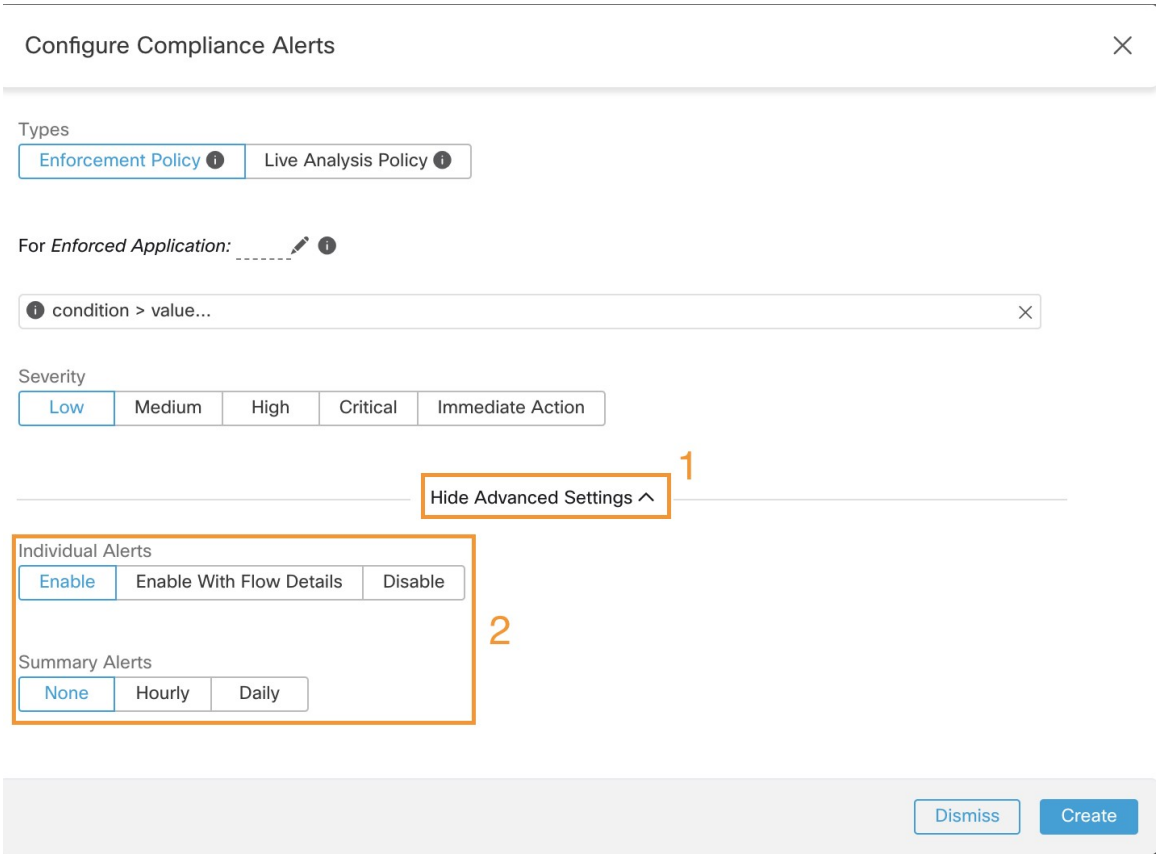
- Les types d'alertes sont affichés lorsque la configuration de l'alerte varie selon le *l'objet*

Note Les types d'alertes pour les alertes de voisinage ne sont pas disponibles pour Cisco Secure Workload 3.7 et les versions antérieures.

- L' *objet* de l'alerte. L'objet dépend de l'application et peut être prérempli lorsque la boîte de dialogue modale de l'alerte est contextuelle.
- Déclenchement d'une alerte : *« quand allons-nous générer une alerte »*. Passez le curseur sur l'icône  pour trouver une liste des conditions disponibles. La liste affiche les conditions disponibles spécifiques au type d'alerte pour la configuration.
- Gravité des alertes : si de nombreuses alertes sont générées, les alertes de gravité plus élevée sont affichées de préférence par rapport aux alertes de gravité inférieure.

- les options de configuration pour les options d'alerte résumées. Cliquez sur **Show Advanced Settings (afficher les paramètres avancés)** pour les développer.
- Fermer la boîte de dialogue : utilisez **Create** (Créer) si vous ajoutez une nouvelle alerte avec toutes les options de configuration spécifiées ou **Dismiss** (Rejeter) si vous n'ajoutez pas de nouvelle alerte.

Figure 5: Options avancées de la boîte de dialogue modale de configuration des alertes

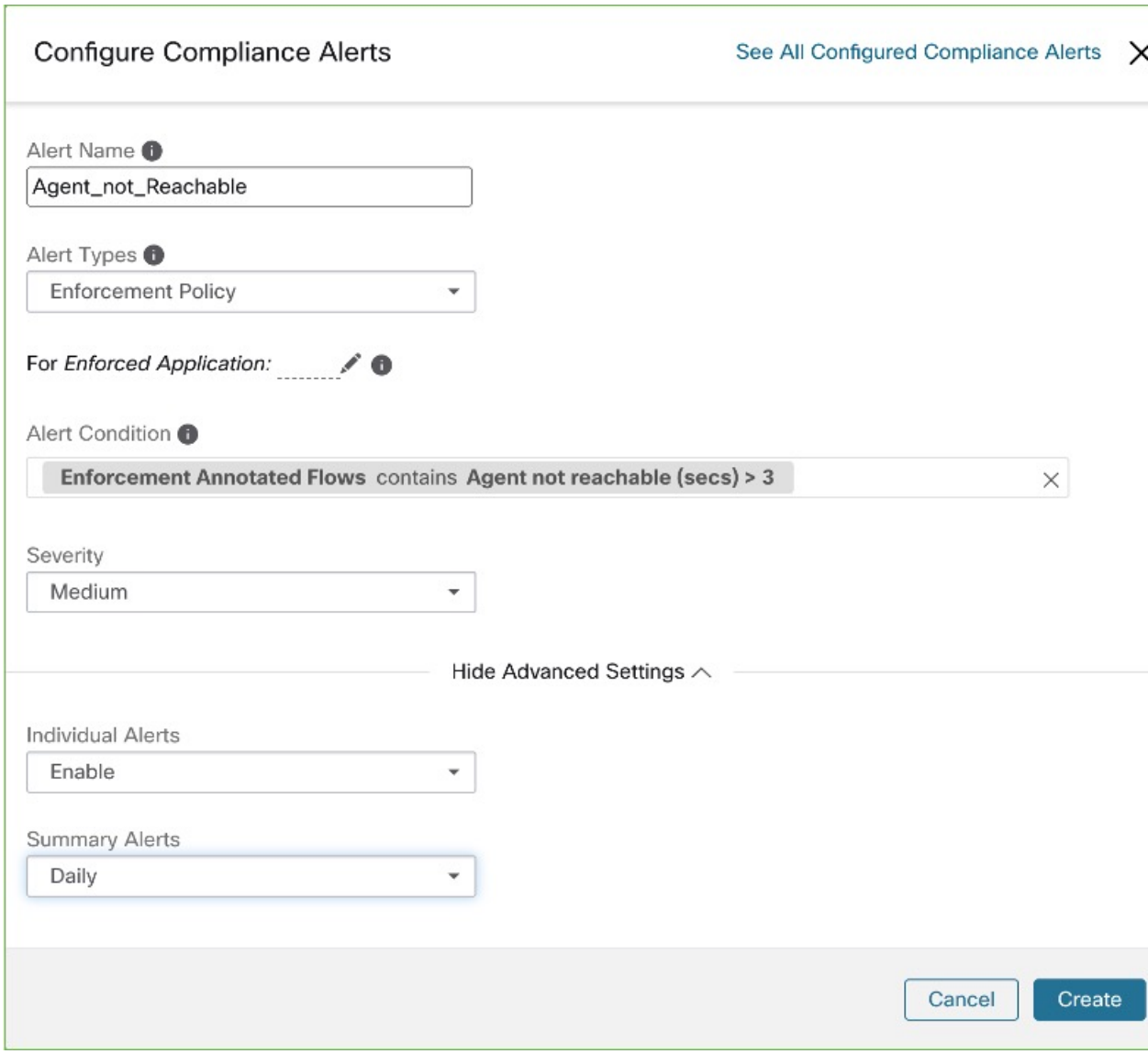


- Le **nom de l'alerte**.
- Les **Types d'alertes**
- Le *sujet* d'une alerte. L'objet dépend de l'application et peut être prérempli lorsque la boîte de dialogue modale de l'alerte est contextuelle.
- La **condition d'alerte** pour laquelle une alerte est déclenchée. Passez le curseur sur l'icône d' **information** pour afficher une liste des conditions disponibles.
- Si plusieurs alertes sont générées, les alertes avec une *gravité* plus élevée sont affichées de préférence par rapport aux alertes avec une gravité plus faible.
- Cliquez sur **Show Advanced Settings** (afficher les paramètres avancés) pour accéder à plus d'options de configuration.

Note

- À la fin de la mise à niveau, toutes les règles de configuration d'alertes existantes des détenteurs actuels reçoivent un **nom d'alerte** selon le format prédéfini. Dans les cas où le nom de l'alerte est absent, le format à utiliser est *Alert_SubType_{DatabaseID}*. Par exemple, Workload_Firewall_64bf9b8493dfc94ca0095718.
- Après le déploiement ou la mise à niveau, toutes les règles de configuration d'alerte par défaut (celles qui sont créées lors de la création d'un nouveau détenteur) se voient attribuer un **nom d'alerte** au format prédéfini : *Alert_SubType*. Par exemple, État_Mise à niveau.

Figure 6: Configurer les alertes



Alertes résumées

Les alertes résumées sont autorisées pour certaines applications et les options de configuration dépendent de l'application.

- Par **alertes individuelles**, on entend les alertes générées à partir d'informations non agrégées (ou faiblement agrégées) et qui sont susceptibles de durer une minute. Notez que cela ne signifie pas nécessairement que les alertes sont réellement générées et envoyées à une minute d'intervalle; les alertes individuelles peuvent toujours être générées à l'intervalle de *fréquence de l'application*.
- **Ls alertes résumées** se réfère aux alertes générées sur des métriques produites pendant une heure ou à la synthèse d'alertes moins fréquentes.

Application	Fréquence de l'application 1	Alertes individuelles	Alertes toutes les heures	Alertes quotidiennes
Conformité	Minute	Oui : à la fréquence de l'application	Résumé individuel	Résumé individuel
Exécution	Minute	Oui : à la fréquence de l'application	Résumé individuel	Résumé individuel
Capteurs	Minute	Oui : à la fréquence de l'application	Résumé individuel	Résumé individuel

Note L'heure de l'événement des alertes résumées représente la première occurrence d'une alerte du même type au cours de la dernière heure ou au cours d'une fenêtre d'intervalle donnée.

Remarque sur la récapitulation par rapport à la répétition d'alarme

La récapitulation s'applique à l'ensemble complet des alertes générées selon la configuration des alertes, tandis que la répétition d'alerte s'applique à une alerte spécifique. Cette distinction est mineure lorsque la configuration d'alerte est très spécifique, mais elle est notable lorsqu'elle est large.

- Par exemple, la configuration de la conformité est assez large : elle porte sur un espace de travail d'application et sur le type de violation pour lequel une alerte doit être générée. Ainsi, la récapitulation s'appliquerait à toutes les alertes déclenchées par une condition « escaped (échappé) », tandis que la répétition s'appliquerait à une portée de consommateur, à une portée de fournisseur, à un port de fournisseur, à un protocole et à la condition échappée très spécifiques.
- À l'opposé, une alerte de plateforme configurée pour envoyer une alerte sur un chemin entre la portée source et la portée de destination avec un nombre de sauts inférieur à une certaine quantité générera une alerte très spécifique.

Autres distinctions

- La répétition d'une alerte n'entraîne son envoi que lorsqu'une nouvelle alerte est générée après l'expiration de l'intervalle de répétition. Rien n'indique le nombre d'alertes supprimées qui auraient pu se produire pendant l'intervalle de répétition.

- Un résumé d'alerte est généré à une fréquence donnée, quel que soit le nombre d'alertes ont générées au cours de cet intervalle. Les résumés d'alertes indiquent le nombre d'alertes déclenchées au cours de la période, ainsi que des mesures agrégées ou par plages.

Outil de notification d'alertes Cisco Secure Workload (TAN)

Note À partir de la version 3.3.1.x de Cisco Secure Workload, le TAN est déplacé vers **l'appareil Cisco Secure Workload de périphérie**.

Les émetteurs de notifications offrent des fonctionnalités pour envoyer des alertes par l'intermédiaire de divers outils tels qu'Amazon Kinesis, Email, Syslog et Slack dans la portée actuellement sélectionnée. En tant que propriétaire de la portée ou administrateur du site, chaque notificateur peut être configuré avec les informations d'authentification requises et d'autres informations spécifiques à l'application du notificateur.

Configurer les outils de notification

Pour configurer des notificateurs, vous devez configurer les connecteurs liés aux alertes. Les connecteurs ne peuvent être configurés qu'après le déploiement d'un appareil de périphérie Cisco Secure Workload. Pour de plus amples renseignements sur le déploiement d'un appareil de périphérie Cisco Secure Workload, consultez Appliances virtuelles pour les connecteurs.

Une fois que l'appareil de périphérie Cisco Secure Workload est configuré, vous pouvez configurer chaque émetteur de notification avec l'entrée requise spécifique. Une fois l'appareil de périphérie Cisco Secure Workload configuré, vous pourrez voir des lignes pointillées connecter les types d'alertes au serveur de publication d'alertes. En effet, l'outil de notification repose sur le serveur de publication d'alertes.

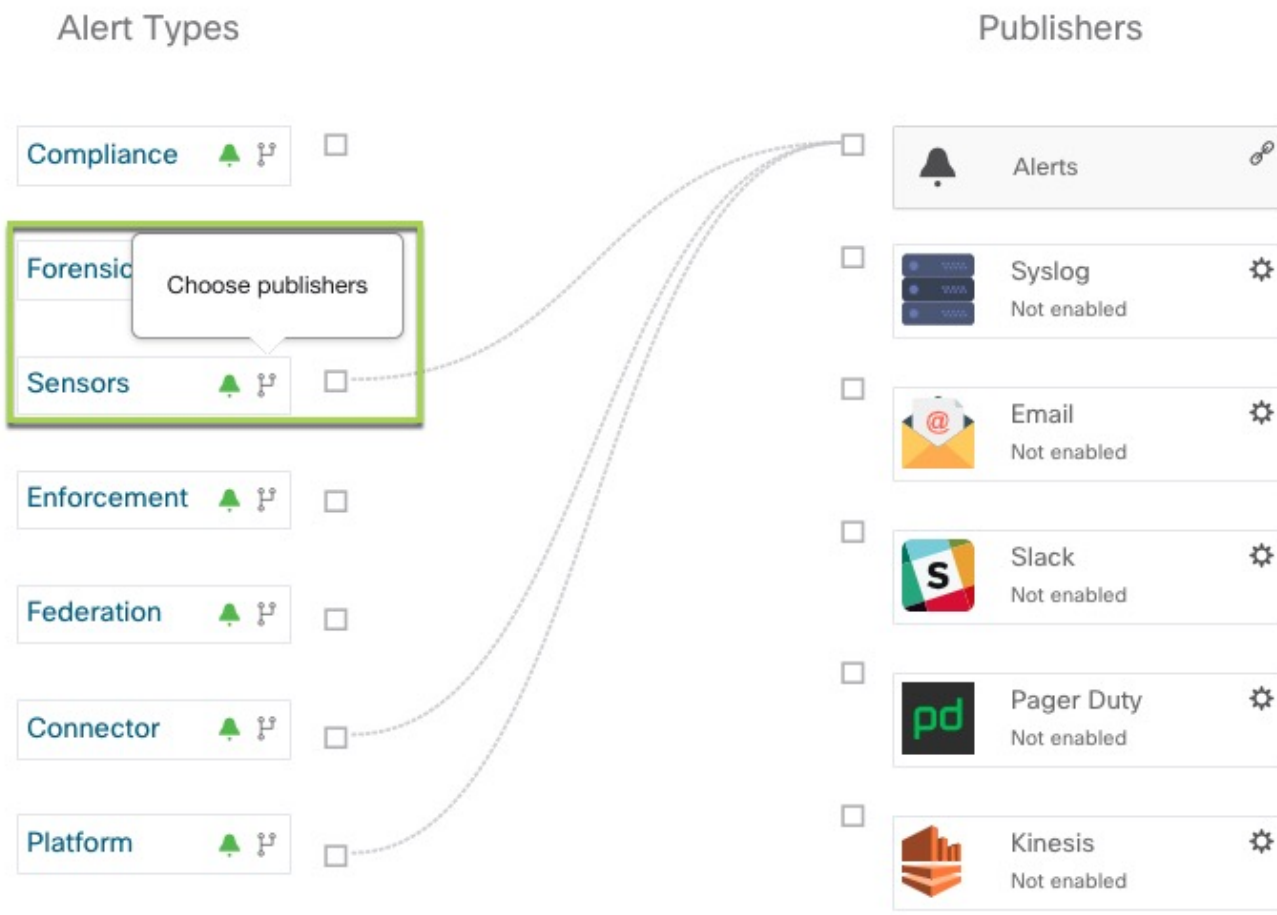
Une fois l'appareil de périphérie Cisco Secure Workload configuré, vous pouvez configurer chaque notificateur avec l'entrée requise. Une fois l'appareil de périphérie Cisco Secure Workload configuré, vous pouvez afficher les lignes en pointillés reliant les types d'alertes au serveur de publication. Cela est dû au fait que l'outil de notification est construit sur le serveur de publication.

La fréquence de l'application est environ la fréquence à laquelle l'application s'exécute et génère des alertes. Par exemple, le service de conformité a une fréquence d'exécution flexible et peut en fait calculer les alertes sur quelques minutes.

Choisir les serveurs de publication d'alertes

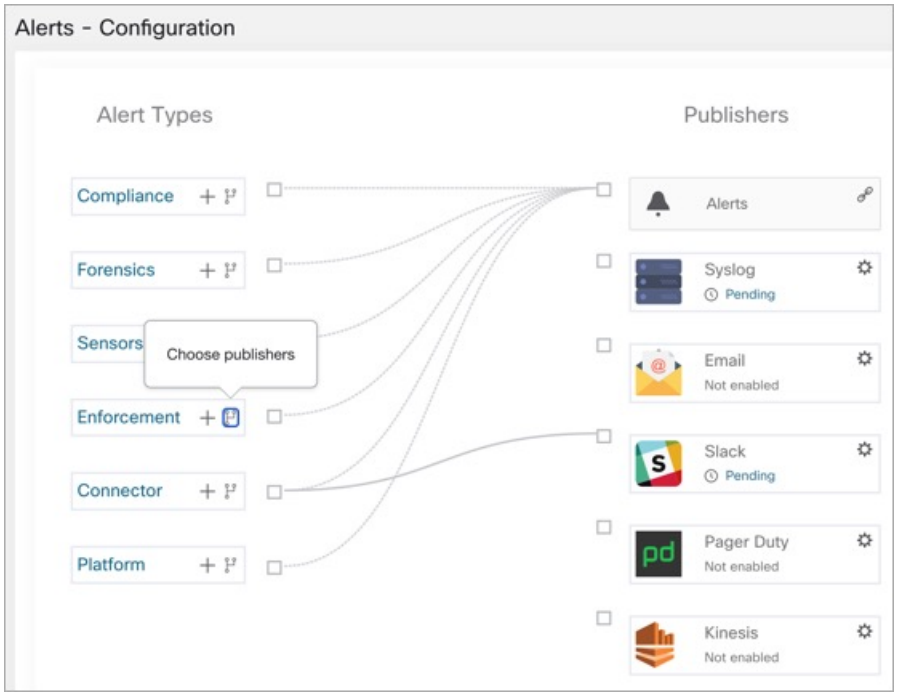
Les propriétaires de la portée et les **administrateurs de site** peuvent choisir les serveurs de publication auxquels **envoyer** des alertes. **Les serveurs de publication** incluent Kafka (Data Tap) et les émetteurs de notifications.

Figure 7: Choisir les serveurs de publication d'alertes



Tous les serveurs de publication disponibles sont affichés dans la fenêtre **Alertes - Configuration**, y compris les **alertes** et **les notificateurs actifs**. Vous pouvez activer ou désactiver l'icône **Envoyer** pour choisir les serveurs de publication du type d'alerte. Le niveau de gravité minimal d'alerte fait référence au niveau de gravité qu'une alerte doit atteindre pour être envoyée par l'intermédiaire des serveurs de publication.

Figure 8: Choisir les serveurs de publication d'alertes



Note Le choix des dérivations de données externes peut avoir une incidence sur le nombre maximal d'alertes qui peuvent être traitées; le nombre maximal d'alertes qui peuvent être traitées pourrait être réduit à 14 000 alertes par lot d'une minute.

La tunnellisation Syslog externe est transférée vers le TAN

Note À partir de la version 3.1.1.x, la fonction de tunnellisation syslog est transférée vers le TAN. Pour configurer le journal système afin d'obtenir les événements de journalisation au niveau de la plateforme, vous devez configurer le TAN Cisco Secure Workload sur l'appareil de périphérie dans la portée racine par défaut. Lorsque l'appareil de périphérie Cisco Secure Workload est configuré sur la portée racine par défaut, vous pouvez configurer le serveur syslog. Pour activer les alertes de plateforme, activez les notifications syslog pour la plateforme. Cela peut être fait en activant la connexion Plateforme Syslog.

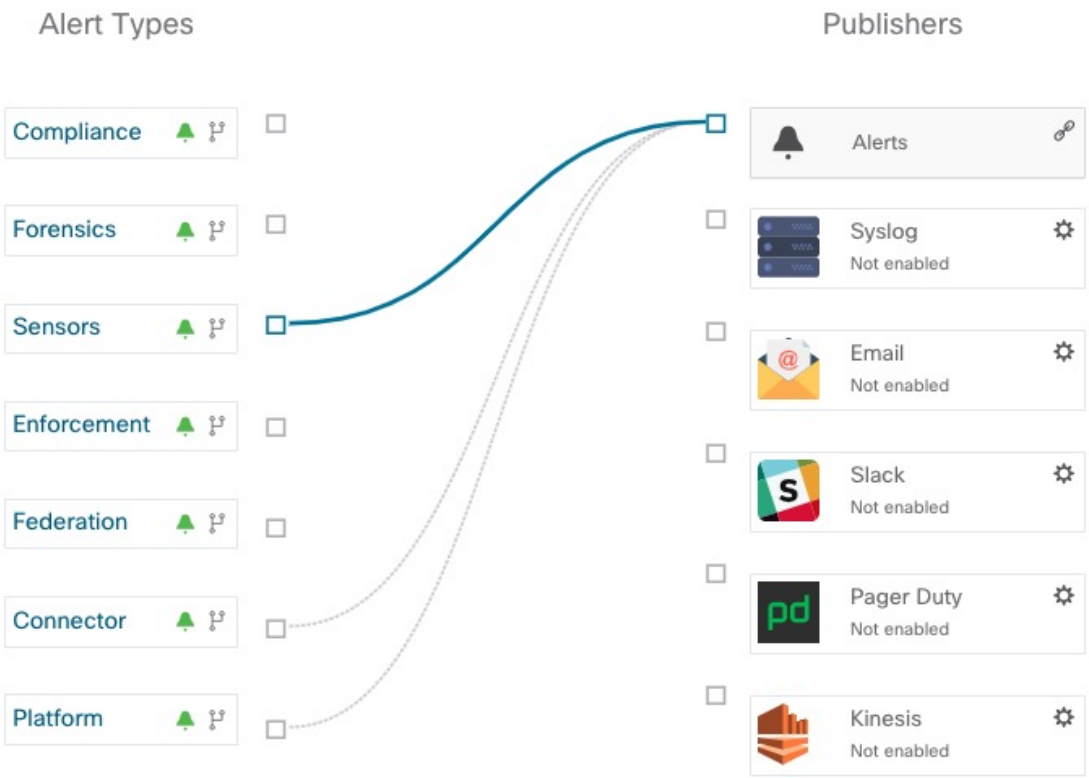
Pour en savoir plus, consultez Connecteur Syslog pour obtenir des détails sur la configuration de syslog.

Tableau des connexions

Le tableau des connexions affiche les liaisons entre **types d'alertes** et **serveurs de publication**. Une fois que vous avez choisi un serveur de publication pour un type d'alerte, une ligne bleue est établie entre le type d'alerte et ce dernier. Notez que la ligne pointant vers le Kafka interne (surveilleur de données) est toujours une ligne pointillée car elle représente un mécanisme interne de mise en œuvre de la notification des alertes.

Figure 9: Tableau des connexions

Figure 10: Tableau des connexions



Note Les alertes générées par l'application utilisateur ne s'affichent pas dans la page de configuration des alertes. Les applications utilisateur peuvent envoyer des messages et des alertes à n'importe quel surveilleur de données (Data Tap) configuré.

Afficher les règles de déclencheur d'alertes

Vous pouvez afficher une liste de toutes les règles de déclenchement d'alertes configurées sur la page **Alertes - Configuration**.

- Vous pouvez filtrer les règles par **type d'alerte** et autres propriétés.
- Dans la colonne **Actions**, cliquez sur l'icône en forme de **crayon** pour modifier les détails comme le nom de l'alerte, les types d'alerte, la condition de l'alerte, la gravité, etc.
- Cliquez sur **See All Configured [alert type] Alerts** (afficher toutes les alertes configurées de type Type d'alerte) pour afficher toutes les alertes du type d'alerte sélectionné dans un nouvel onglet.

Figure 11: Afficher les règles de déclencheur d'alertes

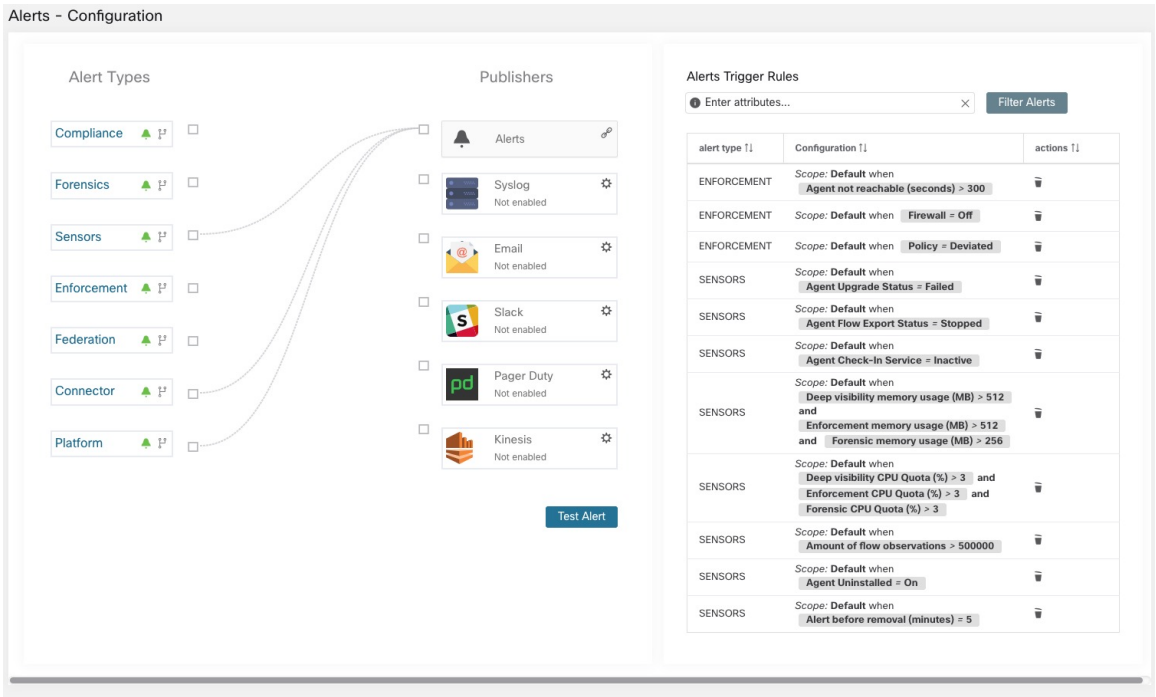
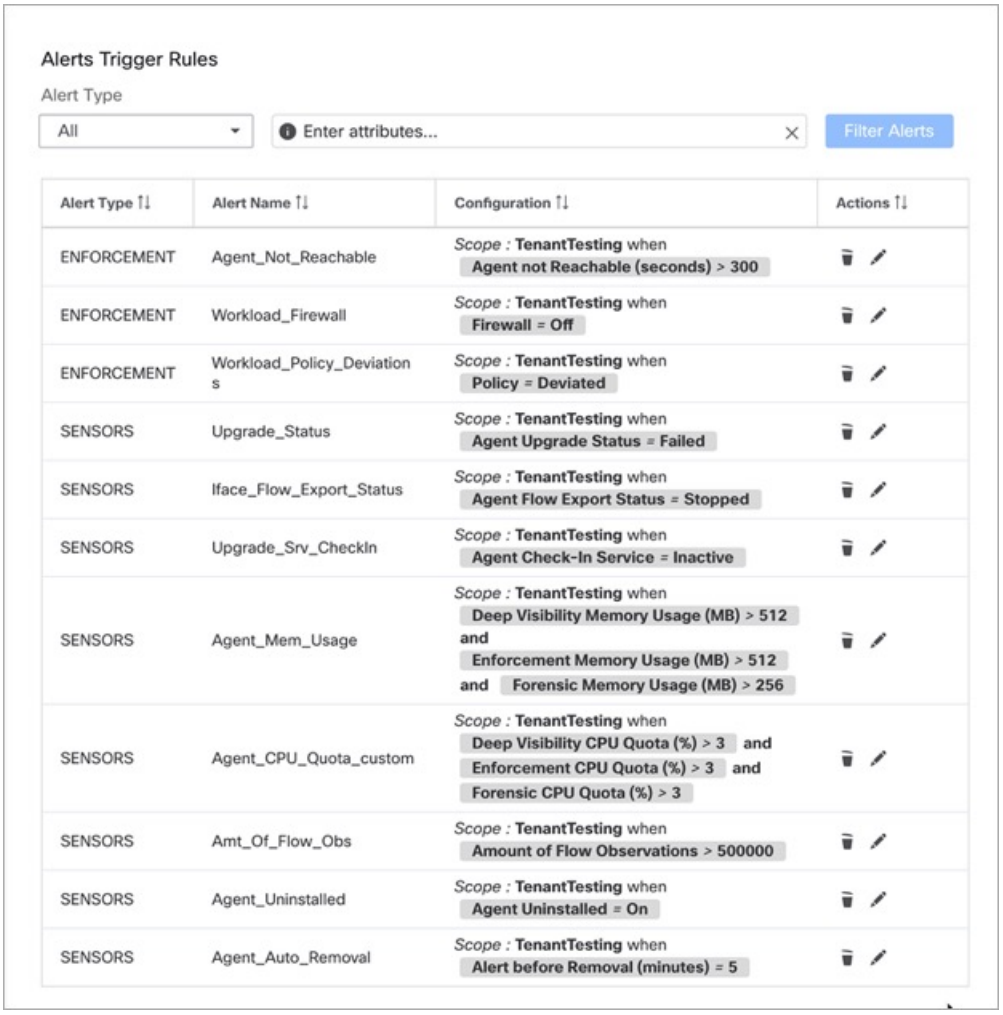


Figure 12: Afficher les règles de déclencheur d'alertes



La fenêtre Règles de déclencheur d'alertes est utilisée pour filtrer les règles de déclencheur d'alertes par type d'alerte et condition de déclencheur.

Note La condition de déclencheur d'alerte est une condition de correspondance exacte.

Détails des règles de déclenchement des alertes

Cliquez sur une ligne de la section **Règles de déclenchement des alertes** pour afficher les détails de la configuration.

1. **Alert Type** : type de l'alerte
2. **Alert Name** : nom de l'alerte.
3. **Configuration** : la condition lorsqu'une alerte est déclenchée dans une portée particulière.

Vous pouvez également afficher d'autres détails comme la **gravité**, les **alertes individuelles** et le **Fréquence des alertes résumées**.

Figure 13: Renseignements détaillés de la configuration des alertes

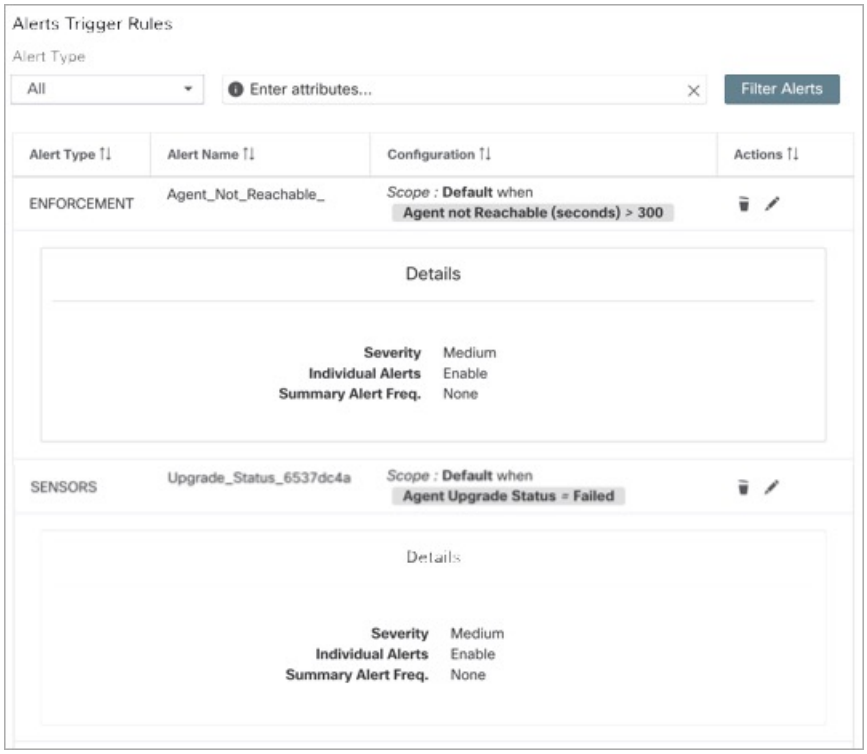
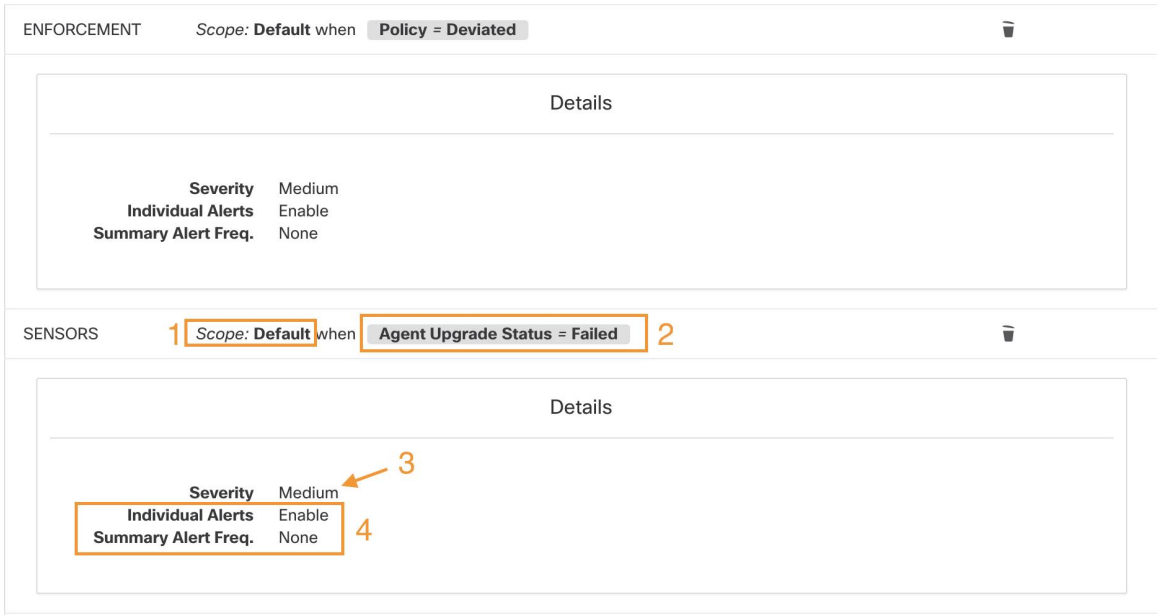


Figure 14: Configuration portée des alertes



Générer des alertes de test

La principale utilisation de la génération d'une alerte de test est de vérifier la connectivité auprès du serveur de publication. Vous pouvez configurer une alerte de test pour envoyer des alertes en fonction du type d'alerte et du serveur de publication lié dans la configuration d'alerte.

Remarque

- La génération d'alertes de test ne se fait pas à partir des sources réelles et est générée à des fins de test uniquement.
- Des alertes de test peuvent être générées pour les types d'alertes liés à au moins un serveur de publication.

Pour générer une alerte de test, procédez comme suit :

Procédure

Étape 1 Dans le volet de navigation, cliquez sur **Manage (Gestion)** > **Workloads (Charges de travail)** > **Alerts Config (Configuration des alertes)**.

Étape 2 Pour configurer une alerte de test, cliquez sur **Test Alert** (Tester l'alerte).

Illustration 15 : Configuration des alertes de test

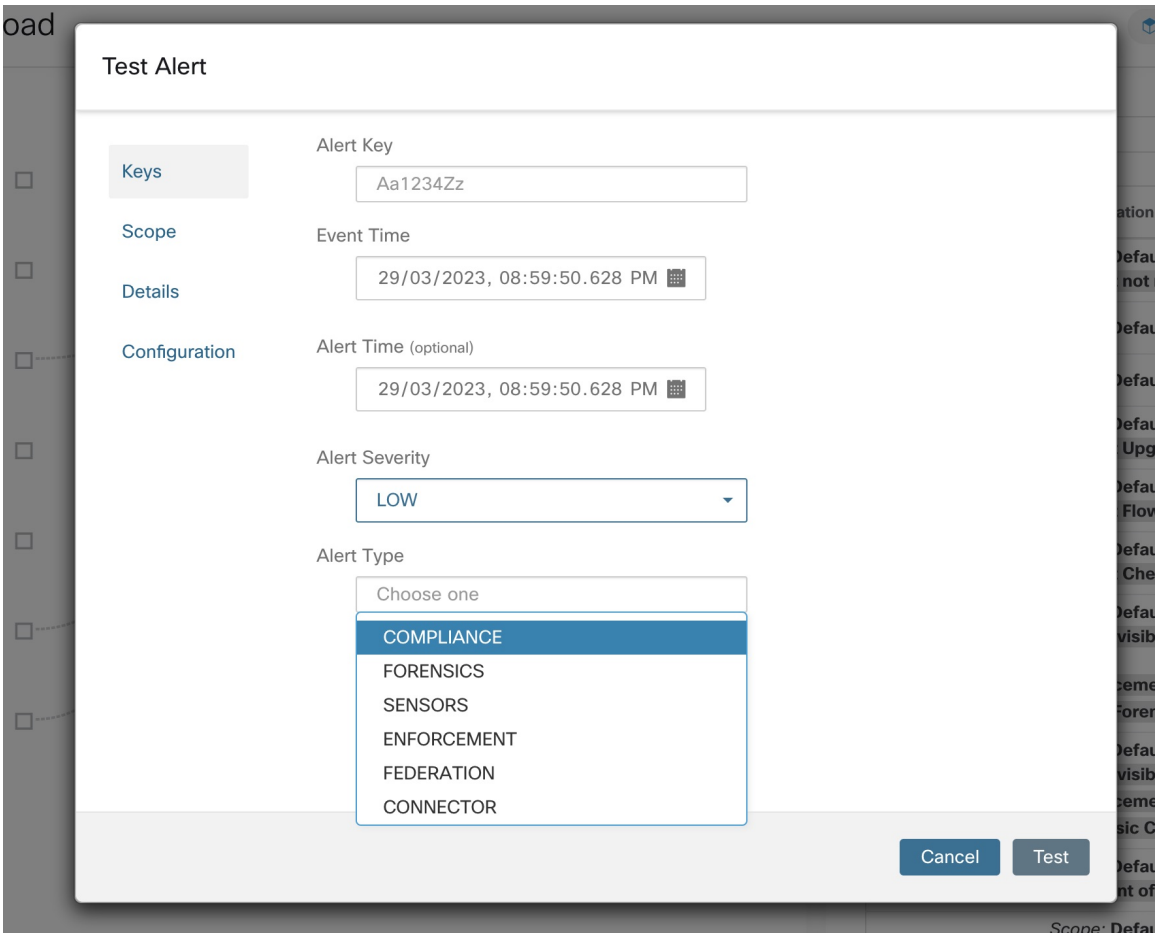
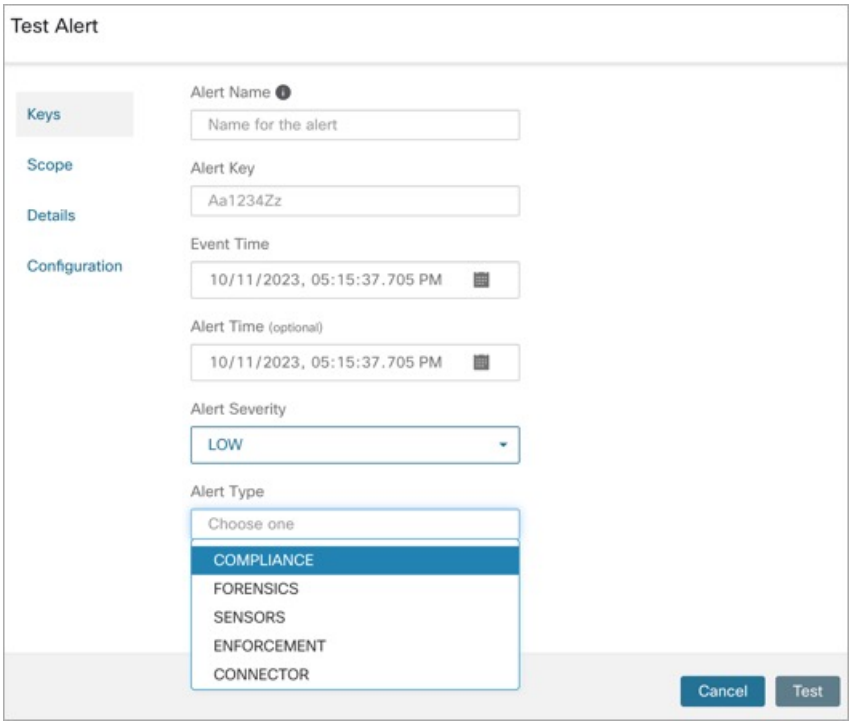


Illustration 16 : Configuration des alertes de test



Étape 3 Sous l'onglet **Keys** (clés), saisissez la valeur pour la clé d'alerte et choisissez les valeurs pour l'heure de l'événement, l'heure de l'alerte, la gravité de l'alerte et le type d'alerte.

Étape 4 Sous l'onglet **Scope** (portée), les valeurs de l'ID de portée et de l'ID du détenteur sont générées automatiquement en fonction de la portée actuelle.

Remarque Si l'ID du détenteur est le même que le VRF de l'ID du détenteur, le système coche automatiquement la case Tenant ID VRF .

Étape 5 Sous l'onglet **Details** (détails), saisissez les valeurs pour le texte de l'alerte, les notes d'événement, les détails de l'alerte et l'ID de configuration de l'alerte.

Remarque Les détails de l'alerte peuvent être une chaîne ou des données au format JSON.

Les options pour le contenu JSON sont les suivantes :

1. Contenant les champs attendus par ce type d'alerte.
2. Tout exemple de données JSON, si ce type d'alerte n'attend pas de champs json par défaut.

   Exemple de JSON :

   ```
   {"alert_name ":"sample","alert_category":{"severity": "dummy"}}
   ```

Étape 6 Sous l'onglet **Configuration** (configuration), choisissez la valeur pour l'alerte individuelle, la fréquence des alertes et le résumé de la fréquence des alertes.

Pour des alertes individuelles, choisissez *ENABLE* (activer) ou *DISABLE* (Désactiver) dans la liste déroulante.

La fréquence des alertes est sélectionnée automatiquement et la fréquence est *INDIVIDUAL* (INDIVIDUELLE).

Remarque Elle prend uniquement en charge les alertes individuelles et ne prend pas en compte la récapitulation.

L'alerte récapitulative est automatiquement sélectionnée à *NONE* (AUCUNE).

Étape 7 Pour générer l'alerte de test, cliquez sur **TEST**.

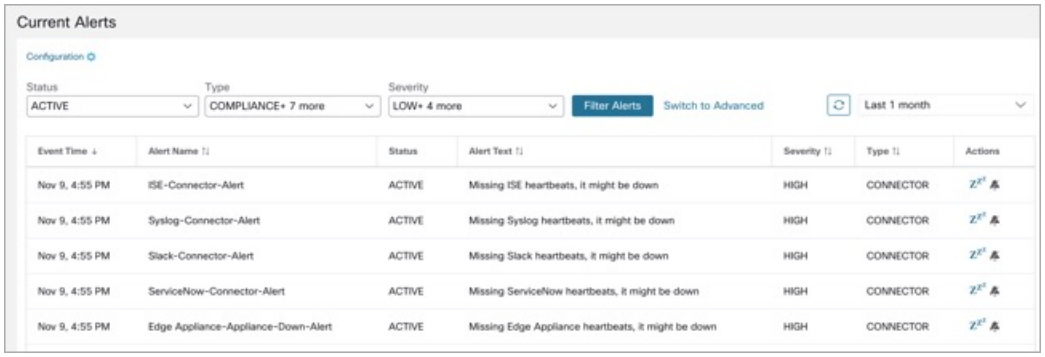
Remarque Une alerte de test est générée et envoyée au serveur de publication configuré.

Alertes actuelles

Accédez à la page **Investigate** (Enquêter) > **Alerts (Alertes)** pour afficher la liste de toutes les alertes actives. Vous pouvez filtrer les alertes par **état**, **type**, **gravité** et plage temporelle.

Seules les alertes dont la gravité est définie sur IMMEDIATE_ACTION, CRITICAL, HIGH, MEDIUM, ou LOW (IMMÉDIAT_ACTION, CRITIQUE, ÉLEVÉE, MOYENNE ou FAIBLE) sont affichées dans la page **Current Alerts** Alertes actuelles). Toutes les alertes, quelles que soient les valeurs de gravité, sont envoyées au broker Kafka configuré.

Figure 17: Alertes actuelles



Filtrer les alertes par plage temporelle

1. Choisissez une valeur dans la liste déroulante. La valeur par défaut est 1 mois.
2. Cliquez sur **Personnalisé** et remplissez les dates **Du** et **Au** pour configurer une plage personnalisée. Cliquez sur **Apply**. Notez que lorsqu'une plage temporelle personnalisée est sélectionnée, le bouton **Refresh** (Actualiser) est désactivé.

Filtrage avancé

1. Cliquez sur **Basculer vers les fonctions avancées**.
2. Saisissez les attributs à filtrer. Passez le curseur sur l'icône d'**information** pour afficher les propriétés à filtrer.

   Les filtres d'alerte ne sont pas conservés lorsque vous revenez aux options de base.

Afficher des détails supplémentaires sur l'alerte

Vous pouvez afficher plus de détails en cliquant sur une alerte.

Figure 18: Détails de l'alerte

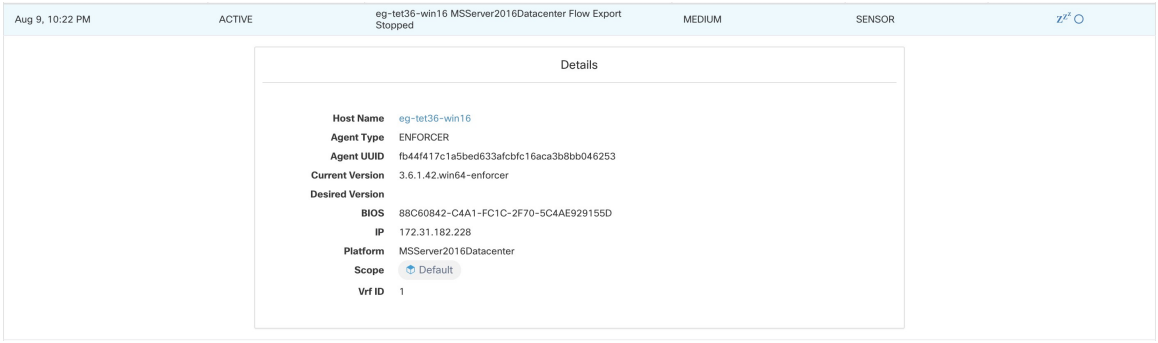
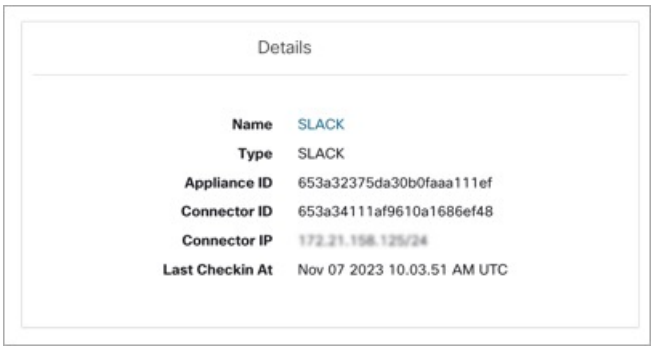


Figure 19: Détails de l'alerte



- Seules 60 alertes par minute et par portée racine sont affichées. Un volume d'alertes plus élevé entraîne un type d'alerte appelé alertes récapitulatives, avec un nombre d'alertes qui ne sont pas affichées .
- Il y a un nombre maximal d'alertes qui s'affichent à tout moment; les alertes plus anciennes sont abandonnées au fur et à mesure que de nouvelles alertes arrivent.

  Pour en savoir plus, consultez la section Limites.

Répéter les alertes

L'application Alerts (Alertes) permet de répéter des alertes du même type pour une durée donnée. Le type d'alerte est défini différemment selon l'espace de travail pour lequel l'alerte est actuellement configurée. Par exemple, le type d'alerte de conformité est défini selon quatre dimensions : portée du consommateur, portée du fournisseur, protocole et port du fournisseur.

Note Actuellement, vous ne pouvez pas répéter ou désactiver le son des alertes créées par l'application de l'utilisateur.

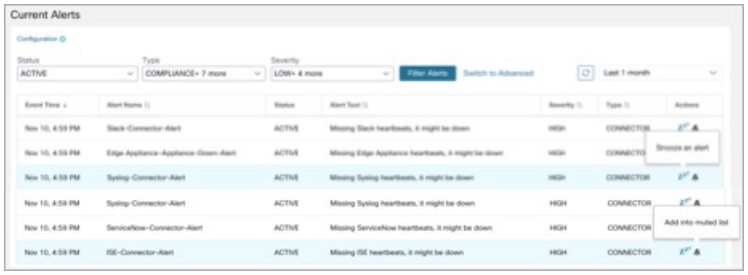
Répéter ou désactiver une alerte

Répéter les alertes :

1. Sous **Actions**, cliquez sur l'icône **Snooze** (Répéter).
2. Choisissez un intervalle dans la liste déroulante.

3. Cliquez sur **Snooze** (Répéter).

Figure 20: Répéter une alerte



Mute Alert (Désactiver l'alerte) :

Utilisez l'option de mise en sourdine pour ne plus recevoir d'alertes.

1. Sous **Actions**, cliquez sur l'icône **Mute** (Désactiver l'alerte, la mettre en sourdine).
2. Pour confirmer, cliquez sur **Yes** (Oui).

   Pour réactiver le son, supprimez l'alerte de la liste des mises en sourdines. Utilisez le menu déroulant de filtre **Status** (État du filtre) pour afficher toutes les alertes **MUTED** (Mises en sourdines) et réactivez le son de l'alerte requise.

Note Vous pouvez afficher jusqu'à 5 000 alertes mises en sourdine ou répétées en attente dans une portée.

Alertes Admiral

Admiral est un système d'alerte intégré, qui remplace le système Bosun des versions précédentes. Pour obtenir plus de renseignements, reportez-vous à la section sur les alertes Admiral.

Détails de l'alerte

Structure commune des alertes

Toutes les alertes respectent une structure globale commune. La structure correspond à la structure de message json disponible par l'intermédiaire de dérivations de données Kafka.

Champ	Format	À propos de
root_scope_id	chaîne	ID de la portée correspondant à la portée supérieure dans la hiérarchie des portées.
key_id	chaîne	id utilisé pour déterminer les alertes « similaires ». Les key_id identiques peuvent être répétés.

Champ	Format	À propos de
type	chaîne	Type de l’alerte. Ensemble fixe de valeurs de chaîne : COMPLIANCE, USERAPP, FORENSICS, ENFORCEMENT, SENSOR, PLATFORM, FEDERATION, CONNECTOR
event_time	long	Horodatage du déclenchement de l’événement (ou si l’événement s’étend sur une plage, le début de la plage). Cet horodatage est en heure d'origine en millisecondes (UTC).
alert_time	long	Horodatage de la première tentative d’envoi de l’alerte. Ce sera après la plage temporelle de l’événement. Cet horodatage est en heure d'origine en millisecondes (UTC).
alert_text	chaîne	Titre de l’alerte.
alert_text_with_names	chaîne	Même contenu que alert_text, mais tous les champs ID sont remplacés par le nom correspondant. Ce champ peut ne pas exister pour toutes les alertes.
gravité	chaîne	Ensemble de valeurs de chaînes fixe : LOW, MEDIUM, HIGH, CRITICAL, IMMEDIATE_ACTION. Il s’agit de la gravité de l’alerte. Pour certains types d’alertes, ces valeurs sont configurables.
alert_notes	chaîne	Généralement non défini. Peut exister dans certains cas particuliers pour la transmission d’informations supplémentaires par Kafka DataTap.
alert_conf_id	chaîne	ID de la configuration d’alerte qui a déclenché cette alerte. Peut ne pas exister pour toutes les alertes.

Champ	Format	À propos de
alert_details	chaîne	Données structurées json sous forme de chaîne de caractères. Consultez les détails de la fonctionnalité pour un type d'alerte spécifique, car la structure exacte de ce champ varie en fonction du type d'alerte.
alert_details_json	json	Même contenu qu'alerte_détails, mais sans chaîne de caractères. Présent uniquement pour les alertes de conformité et uniquement par l'intermédiaire de Kafka.
tenant_id	chaîne	Peut contenir un VRF correspondant à root_scope_id. Ou peut contenir 0 comme valeur par défaut. Il peut aussi ne pas être présent du tout.
alert_id	chaîne	ID temporaire généré en interne. Il est préférable de l'ignorer.
alert_name	chaîne	Nom de l'alerte.

- Conformité : lab- compliance-alert-details
- Criminalistique : Champs d'intégration externe et d'événements criminalistiques
- Capteur : détails de l'alerte de capteur
- Mise en application : détails de l'alerte d'application
- Connecteur : détails de l'alerte

Types d'alertes supplémentaires pour les grappes sur site

- Fabric (Structure) : fabric-alerte-details
- Fédération : federation-alert-details
- Plateforme : Détails de l'alerte
- Fédération : federation-alert-details
- Plateforme : Détails de l'alerte

Format général de l'alerte par outil de notification

Voici des exemples de l'affichage des alertes pour différents types de notifications.

Note À partir de la version 3.9 de Cisco Secure Workload, les détails de l'émetteur de la notification comprennent **Alert Name**.

Kafka (Surveillance de données)

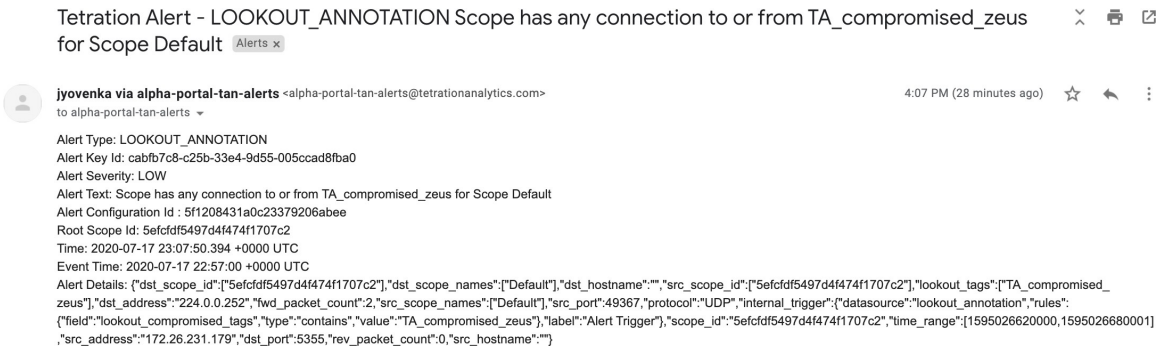
Les messages Kafka (DataTap) sont au format JSON. l'exemple ci-dessous; consultez la section alert_details ci-dessus pour obtenir des exemples supplémentaires.


```
  {
  "severity": "LOW",
  "tenant_id": 0,
  "alert_time": 1595207103337,
  "alert_text": "Lookout Annotated Flows contains TA_zeus for
<scope_id:5efcfdf5497d4f474f1707c2>",
  "key_id": "0a4a4208-f721-398c-b61c-c07af3be9413",
  "alert_id": "/Alerts/5efcfdf5497d4f474f1707c2/DataSource{location_type='TETRATION_PARQUET',
 location_name='lookout_annotation', location_grain='HOURLY',
root_scope_id='5efcfdf5497d4f474f1707c2'}/bd33f37af32a5ce71e888f95ccfe845305e61a12a7829ca5f2d72bf96237d403",

  "alert_text_with_names": "Lookout Annotated Flows contains TA_zeus for Scope Default",
  "root_scope_id": "5efcfdf5497d4f474f1707c2",
  "alert_conf_id": "5f10c7141a0c236b78148da1",
  "type": "LOOKOUT_ANNOTATION",
  "event_time": 1595204760000,
  "alert_details":
"{\"dst_scope_id\":[\"5efcfdf5497d4f474f1707c2\"],\"dst_scope_names\":[\"Default\"],\"dst_hostname\":\"\",\"src_scope_id\":[\"5efcfdf5497d4f474f1707c2\"],\"lookout_tags\":[\"TA_compromised_zeus\"],\"dst_address\":\"224.0.0.252\",\"fwd_packet_count\":2,\"src_scope_names\":[\"Default\"],\"src_port\":49367,\"protocol\":\"UDP\",\"internal_trigger\":{\"datasource\":\"lookout_annotation\",\"rules\":[{\"field\":\"lookout_compromised_tags\",\"type\":\"contains\",\"value\":\"TA_compromised_zeus\"}],\"label\":\"Alert Trigger\"},\"scope_id\":\"5efcfdf5497d4f474f1707c2\",\"time_range\":[1595026620000,1595026680001],\"src_address\":\"172.26.231.179\",\"dst_port\":5355,\"rev_packet_count\":0,\"src_hostname\":\"\"}"

  }
```


Courriel

Renseignements sur la configuration des alertes par courriel : connecteur de courriel

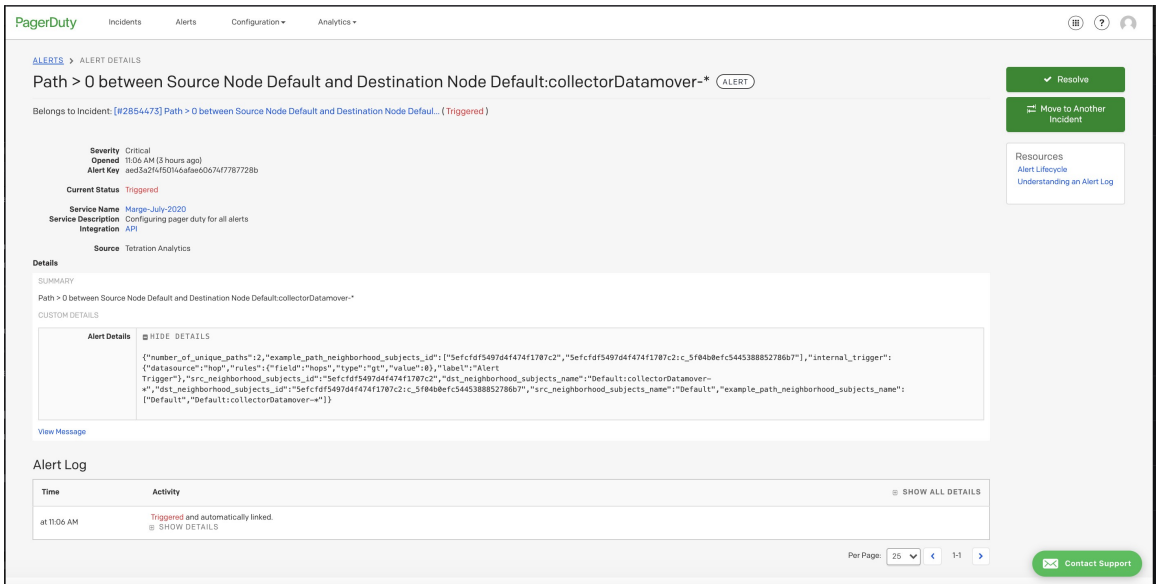
Figure 21: Exemple d'alerte Cisco Cisco Secure Workload



PagerDuty

Renseignements sur la configuration des alertes de PagerDuty : PagerDuty Connector

Figure 22: Exemple d'alerte Cisco Secure Workload dans PagerDuty



Les alertes envoyées à PagerDuty sont un nouveau déclenchement de la même alerte en fonction de key_id.

La gravité est mappée à la gravité PagerDuty comme suit :

Gravité Cisco Secure Workload	Gravité PagerDuty
IMMEDIATE_ACTION (ACTION_IMMÉDIATE)	critique
CRITIQUE	critique
ÉLEVÉE	erreur
MOYENNE	avertissement
FAIBLE	Information

Syslog

Informations sur la configuration des alertes Syslog et le réglage du mappage de gravité : connecteur Syslog

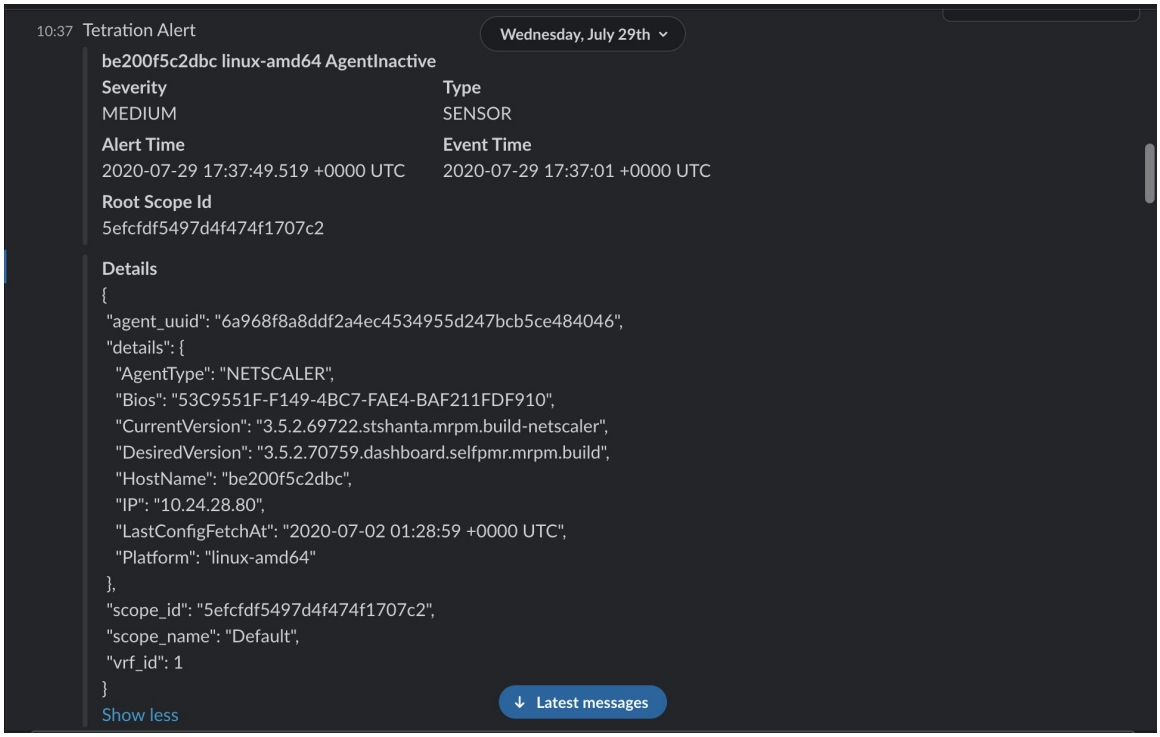
Figure 23: Exemple de plusieurs alertes Cisco Secure Workload envoyées à syslog

Aug 2 18:45:21 tan-5f035bae1a0c231d5880d7f8-tac-demo-data-ingest Tetration Alert[26841]: [DEBUG] {"keyId":"3ee0d8b7-bc81-3427-9e84-6b9f8fedb98c","eventTime":"1596393720000","alertTime":"1596393968822","alertText":"Enforcement Annotated Flows contains escaped for \u003capplication_id:5f04b0b9755f024d4e36a279\u003e","severity":"LOW","tenantId":"0","type":"COMPLIANCE","alertDetails":"{\"consumer_scope_ids\":[\"5efcfdf5497d4f474f1707c2\"],\"consumer_scope_names\":[\"Default\"],\"provider_scope_names\":[\"Default\"],\"provider_port\":53,\"application_id\":\"5f04b0b9755f024d4e36a279\",\"constituent_flows\":[{\"consumer_port\":37367,\"protocol\":\"UDP\",\"consumer_address\":\"172.31.163.139\",\"provider_address\":\"171.70.168.183\",\"provider_port\":53},{\"consumer_port\":39652,\"protocol\":\"UDP\",\"consumer_address\":\"172.31.163.137\",\"provider_address\":\"171.70.168.183\",\"provider_port\":53},{\"consumer_port\":63811,\"protocol\":\"UDP\",\"consumer_address\":\"172.31.163.136\",\"provider_address\":\"171.70.168.183\",\"provider_port\":53},{\"consumer_port\":57418,\"protocol\":\"UDP\",\"consumer_address\":\"172.31.163.138\",\"provider_address\":\"173.36.131.10\",\"provider_port\":53},{\"consumer_port\":12599,\"protocol\":\"UDP\",\"consumer_address\":\"172.31.163.141\",\"provider_address\":\"173.36.131.10\",\"provider_port\":53},{\"consumer_port\":7385,\"protocol\":\"UDP\",\"consumer_address\":\"172.31.163.140\",\"provider_address\":\"173.36.131.10\",\"provider_port\":53}],\"escaped_count\":6,\"provider_scope_ids\":[\"5efcfdf5497d4f474f1707c2\"],\"policy_type\":\"ENFORCED_POLICY\",\"protocol\":\"UDP\",\"internal_trigger\":{\"datasource\":\"compliance\",\"rules\":{\"field\":\"policy_violations\",\"type\":\"contains\",\"value\":\"escaped\"},\"label\":\"Alert Trigger\"},\"time_range\":[1596393720000,1596393779999],\"policy_category\":[\"ESCAPED\"]}","rootScopeId":"5efcfdf5497d4f474f1707c2","alertConfId":"5f15cca71a0c231ebd66ca3b","alertTextWithNames":"Enforcement Annotated Flows contains escaped for Enforced Application j1"}
Aug 2 18:45:21 tan-5f035bae1a0c231d5880d7f8-tac-demo-data-ingest Tetration Alert[26841]: [DEBUG] {"keyId":"8f0cfcb5-f8c1-3130-a069-3721b7d50159","eventTime":"1596393720000","alertTime":"1596393968822","alertText":"Enforcement Annotated Flows contains escaped for \u003capplication_id:5f04b0b9755f024d4e36a279\u003e","severity":"LOW","tenantId":"0","type":"COMPLIANCE","alertDetails":"{\"consumer_scope_ids\":[\"5efcfdf5497d4f474f1707c2\"],\"consumer_scope_names\":[\"Default\"],\"provider_scope_names\":[\"Default\"],\"provider_port\":5660,\"application_id\":\"5f04b0b9755f024d4e36a279\",\"constituent_flows\":[{\"consumer_port\":17131,\"protocol\":\"TCP\",\"consumer_address\":\"172.26.231.193\",\"provider_address\":\"172.31.163.140\",\"provider_port\":5660}],\"escaped_count\":1,\"provider_scope_ids\":[\"5efcfdf5497d4f474f1707c2\"],\"policy_type\":\"ENFORCED_POLICY\",\"protocol\":\"TCP\",\"internal_trigger\":{\"datasource\":\"compliance\",\"rules\":{\"field\":\"policy_violations\",\"type\":\"contains\",\"value\":\"escaped\"},\"label\":\"Alert Trigger\"},\"time_range\":[1596393720000,1596393779999],\"policy_category\":[\"ESCAPED\"]}","rootScopeId":"5efcfdf5497d4f474f1707c2","alertConfId":"5f15cca71a0c231ebd66ca3b","alertTextWithNames":"Enforcement Annotated Flows contains escaped for Enforced Application j1"}
Aug 2 18:45:21 tan-5f035bae1a0c231d5880d7f8-tac-demo-data-ingest Tetration Alert[26841]: [DEBUG] {"keyId":"1ef4a974-be89-31de-abe9-dc71cb0170ad","eventTime":"1596393720000","alertTime":"1596393968822","alertText":"Enforcement Annotated Flows contains escaped for \u003capplication_id:5f04b0b9755f024d4e36a279\u003e","severity":"LOW","tenantId":"0","type":"COMPLIANCE","alertDetails":"{\"consumer_scope_ids\":[\"5efcfdf5497d4f474f1707c2\"],\"consumer_scope_names\":[\"Default\"],\"provider_scope_names\":[\"Default\"],\"provider_port\":443,\"application_id\":\"5f04b0b9755f024d4e36a279\",\"constituent_flows\":[{\"consumer_port\":17792,\"protocol\":\"TCP\",\"consumer_address\":\"172.26.231.193\",\"provider_address\":\"172.31.163.133\",\"provider_port\":443}],\"escaped_count\":1,\"provider_scope_ids\":[\"5efcfdf5497d4f474f1707c2\"],\"policy_type\":\"ENFORCED_POLICY\",\"protocol\":\"TCP\",\"internal_trigger\":{\"datasource\":\"compliance\",\"rules\":{\"field\":\"policy_violations\",\"type\":\"contains\",\"value\":\"escaped\"},\"label\":\"Alert Trigger\"},\"time_range\":[1596393720000,1596393779999],\"policy_category\":[\"ESCAPED\"]}","rootScopeId":"5efcfdf5497d4f474f1707c2","alertConfId":"5f15cca71a0c231ebd66ca3b","alertTextWithNames":"Enforcement Annotated Flows contains escaped for Enforced Application j1"}

Slack

Informations sur la configuration des alertes Slack : connecteur Slack

Figure 24: Exemple d'alerte Cisco Secure Workload envoyée au canal Slack



Kinesis

Renseignements sur la configuration des alertes Kinesis : Connecteur Kinesis

Les alertes Kinesis sont similaires aux alertes Kafka, car ce sont deux files d'attente de messages.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.