Moniteurs et alertes

Data Infrastructure Insights

NetApp
February 11, 2026

Sommaire

Moniteurs et alertes

Alertes avec moniteurs

Configurez des moniteurs pour suivre les seuils de performances, consigner les événements et les anomalies sur l'ensemble de vos ressources d'infrastructure. Créez des alertes personnalisées pour des mesures telles que la latence d'écriture des nœuds, la capacité de stockage ou les performances des applications, et recevez des notifications lorsque ces conditions sont remplies.

Les moniteurs vous permettent de définir des seuils sur les métriques générées par les objets « d'infrastructure » tels que le stockage, la VM, EC2 et les ports, ainsi que pour les données « d'intégration » telles que celles collectées pour Kubernetes, les métriques avancées ONTAP et les plugins Telegraf. Ces moniteurs *métriques* vous alertent lorsque les seuils de niveau d'avertissement ou de niveau critique sont dépassés.

Vous pouvez également créer des moniteurs pour déclencher des alertes de niveau avertissement, critique ou informatif lorsque des *événements de journal* spécifiés sont détectés.

Data Infrastructure Insights fournit un certain nombre de"Moniteurs définis par le système" également, en fonction de votre environnement.

Meilleures pratiques de sécurité

Les alertes Data Infrastructure Insights sont conçues pour mettre en évidence les points de données et les tendances de votre locataire, et Data Infrastructure Insights vous permet de saisir n'importe quelle adresse e-mail valide comme destinataire d'alerte. Si vous travaillez dans un environnement sécurisé, soyez particulièrement attentif à qui reçoit la notification ou a accès à l'alerte.

Moniteur métrique ou journal ?

1. Dans le menu Data Infrastructure Insights , cliquez sur **Alertes > Gérer les moniteurs**

   La page de liste des moniteurs s'affiche, affichant les moniteurs actuellement configurés.

2. Pour modifier un moniteur existant, cliquez sur le nom du moniteur dans la liste.
3. Pour ajouter un moniteur, cliquez sur **+ Moniteur**.

Lorsque vous ajoutez un nouveau moniteur, vous êtes invité à créer un moniteur de métriques ou un moniteur de journaux.

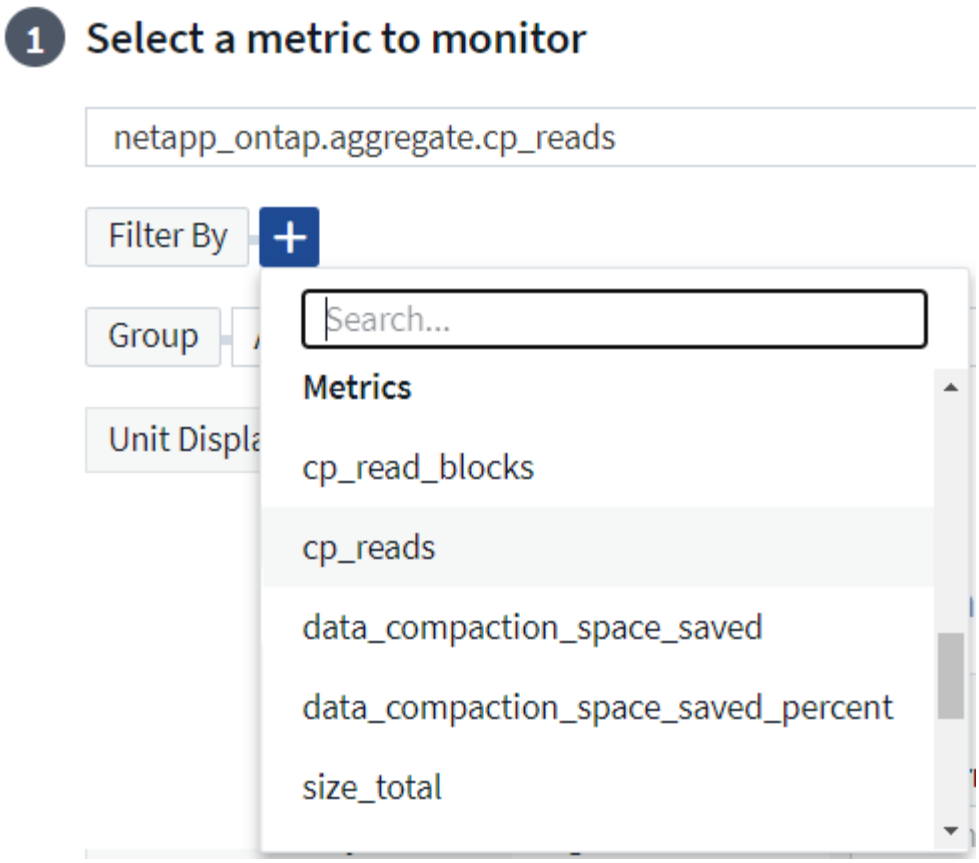
- *Metric* surveille les alertes sur les déclencheurs liés à l'infrastructure ou aux performances
- *Log* surveille les alertes sur l'activité liée au journal

Après avoir choisi votre type de moniteur, la boîte de dialogue Configuration du moniteur s'affiche. La configuration varie en fonction du type de moniteur que vous créez.

Moniteur métrique

1. Dans la liste déroulante, recherchez et choisissez un type d'objet et une métrique à surveiller.

Vous pouvez définir des filtres pour affiner les attributs d'objet ou les mesures à surveiller.

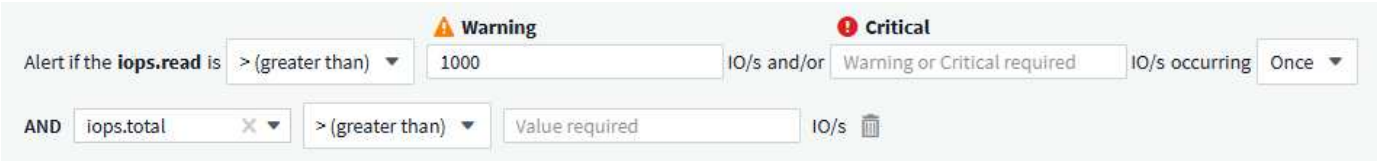


Lorsque vous travaillez avec des données d'intégration (Kubernetes, ONTAP Advanced Data, etc.), le filtrage des métriques supprime les points de données individuels/non appariés de la série de données tracées, contrairement aux données d'infrastructure (stockage, VM, ports, etc.) où les filtres fonctionnent sur la valeur agrégée de la série de données et suppriment potentiellement l'objet entier du graphique.

Les moniteurs de métriques s'appliquent aux objets d'inventaire tels que le stockage, le commutateur, l'hôte, la machine virtuelle, etc., ainsi qu'aux métriques d'intégration telles que les données ONTAP Advanced ou Kubernetes. Lors de la surveillance des objets d'inventaire, notez que vous ne pouvez pas sélectionner une méthode « Grouper par ». Cependant, le regroupement est autorisé lors de la surveillance des données d'intégration.

Moniteurs multi-conditions

Vous pouvez choisir d'affiner davantage votre surveillance métrique en ajoutant une deuxième condition. Développez simplement l'invite « + Ajouter une condition de métrique secondaire » et configurez la condition supplémentaire.



Le moniteur émettra une alerte si les deux conditions sont remplies.

Notez que vous ne pouvez utiliser qu'un « ET » pour une deuxième condition ; vous ne pouvez pas choisir d'alerter sur une condition OU sur l'autre.

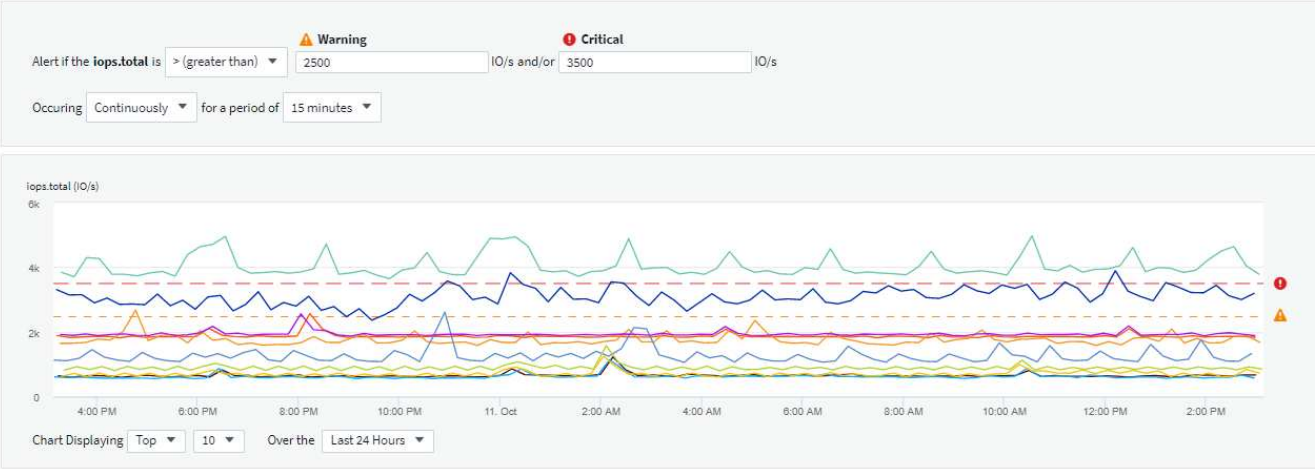
Définir les conditions du moniteur.

1. Après avoir choisi l'objet et la métrique à surveiller, définissez les seuils de niveau d'avertissement et/ou de niveau critique.
2. Pour le niveau *Avertissement*, entrez 200 pour notre exemple. La ligne pointillée indiquant ce niveau d'avertissement s'affiche dans l'exemple de graphique.
3. Pour le niveau *Critique*, entrez 400. La ligne pointillée indiquant ce niveau critique s'affiche dans l'exemple de graphique.

   Le graphique affiche les données historiques. Les lignes de niveau d'avertissement et critique sur le graphique sont une représentation visuelle du moniteur, vous pouvez donc facilement voir quand le moniteur peut déclencher une alerte dans chaque cas.

4. Pour l'intervalle d'occurrence, choisissez *En continu* pour une période de *15 minutes*.

   Vous pouvez choisir de déclencher une alerte dès qu'un seuil est dépassé ou d'attendre que le seuil soit dépassé en continu pendant un certain temps. Dans notre exemple, nous ne souhaitons pas être alertés à chaque fois que le nombre total d'IOPS dépasse le niveau d'avertissement ou critique, mais uniquement lorsqu'un objet surveillé dépasse en continu l'un de ces niveaux pendant au moins 15 minutes.



Définir le comportement de résolution des alertes

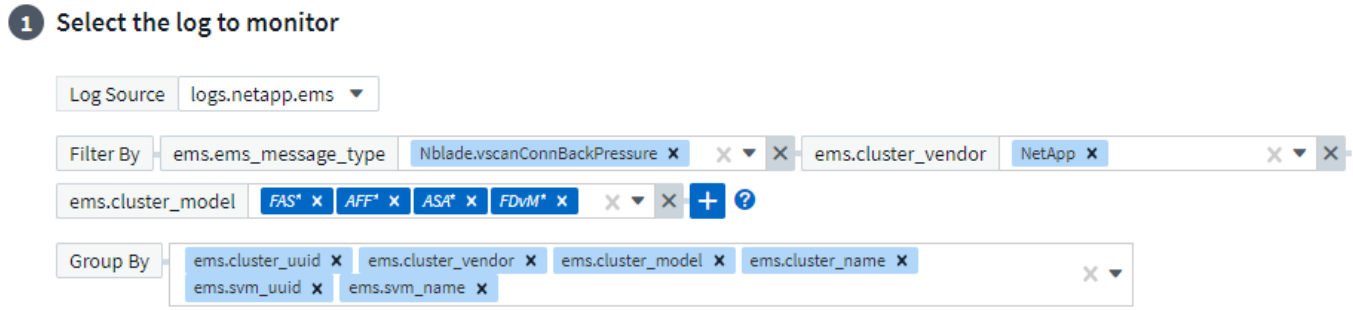
Vous pouvez choisir comment une alerte de surveillance métrique est résolue. Deux choix s'offrent à vous :

- Résoudre le problème lorsque la métrique revient dans la plage acceptable.
- Résoudre lorsque la métrique se situe dans la plage acceptable pendant une durée spécifiée, de 1 minute à 7 jours.

Moniteur de journal

Lors de la création d'un **Moniteur de journaux**, choisissez d'abord le journal à surveiller dans la liste des journaux disponibles. Vous pouvez ensuite filtrer en fonction des attributs disponibles comme ci-dessus. Vous pouvez également choisir un ou plusieurs attributs « Grouper par ».

Le filtre Log Monitor ne peut pas être vide.



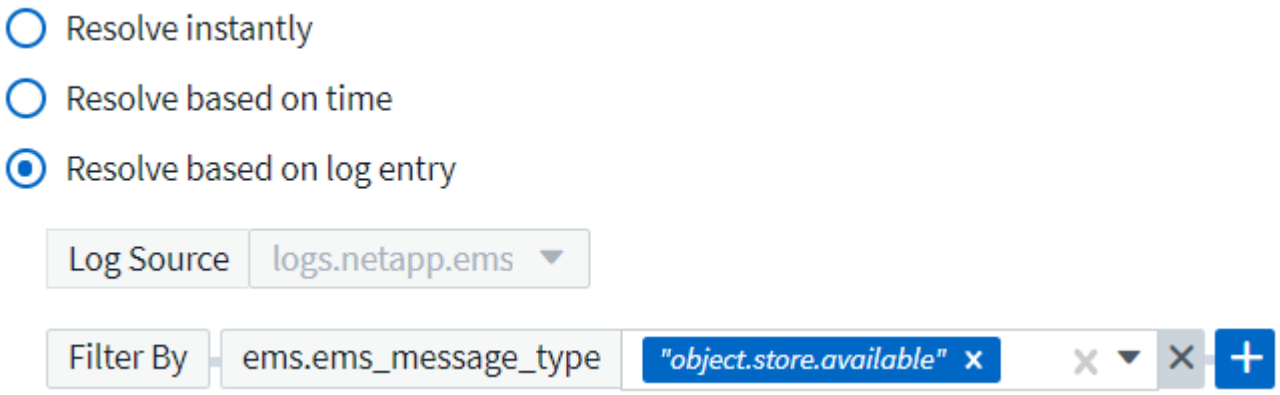
Définir le comportement de l'alerte

Vous pouvez créer le moniteur pour alerter avec un niveau de gravité *Critique*, *Avertissement* ou *Informationnel*, lorsque les conditions que vous avez définies ci-dessus se produisent une fois (c'est-à-dire immédiatement), ou attendre d'alerter jusqu'à ce que les conditions se produisent 2 fois ou plus.

Définir le comportement de résolution des alertes

Vous pouvez choisir comment une alerte de surveillance de journal est résolue. Trois choix s'offrent à vous :

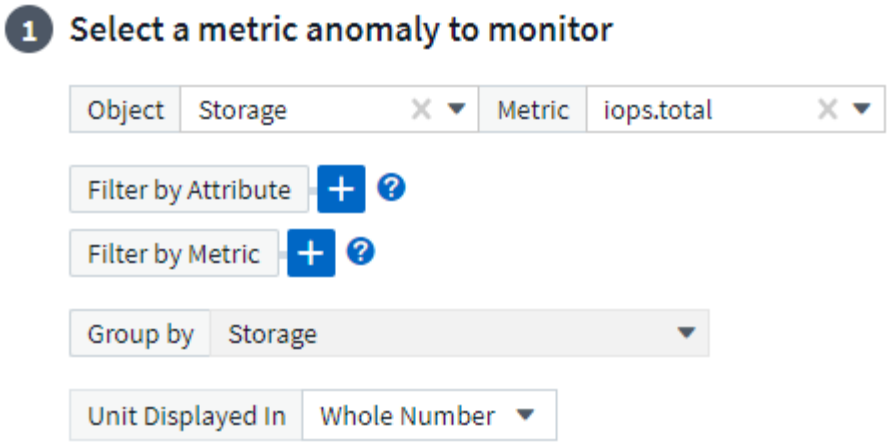
- **Résoudre instantanément** : L'alerte est immédiatement résolue sans aucune autre action nécessaire
- **Résolution en fonction du temps** : L'alerte est résolue une fois le temps spécifié écoulé
- **Résolution basée sur l'entrée de journal** : L'alerte est résolue lorsqu'une activité de journal ultérieure s'est produite. Par exemple, lorsqu'un objet est enregistré comme « disponible ».



Moniteur de détection d'anomalies

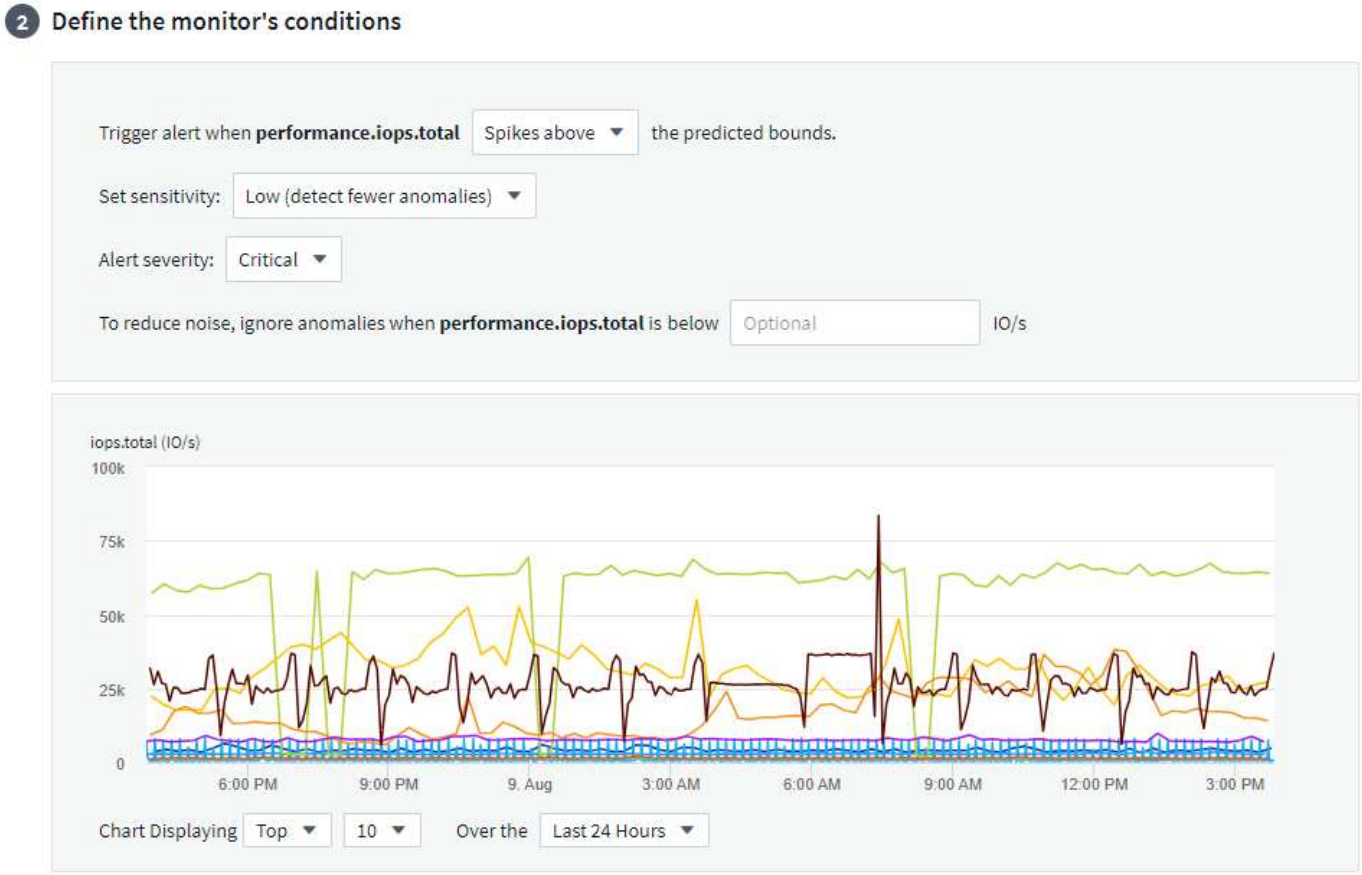
1. Dans la liste déroulante, recherchez et choisissez un type d'objet et une métrique à surveiller.

Vous pouvez définir des filtres pour affiner les attributs d'objet ou les mesures à surveiller.



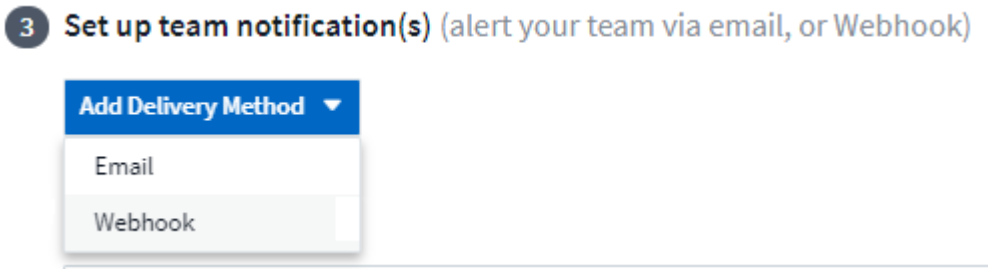
Définir les conditions du moniteur.

1. Après avoir choisi l'objet et la métrique à surveiller, vous définissez les conditions dans lesquelles une anomalie est détectée.
   - Choisissez de détecter une anomalie lorsque la métrique choisie **monte au-dessus** des limites prédites, **descend en dessous** de ces limites, ou **monte au-dessus ou descend en dessous** des limites.
   - Définissez la **sensibilité** de détection. **Faible** (moins d'anomalies sont détectées), **Moyen** ou **Élevé** (plus d'anomalies sont détectées).
   - Définissez les alertes sur **Avertissement** ou **Critique**.
   - Si vous le souhaitez, vous pouvez choisir de réduire le bruit, en ignorant les anomalies lorsque la métrique choisie est inférieure à un seuil que vous avez défini.



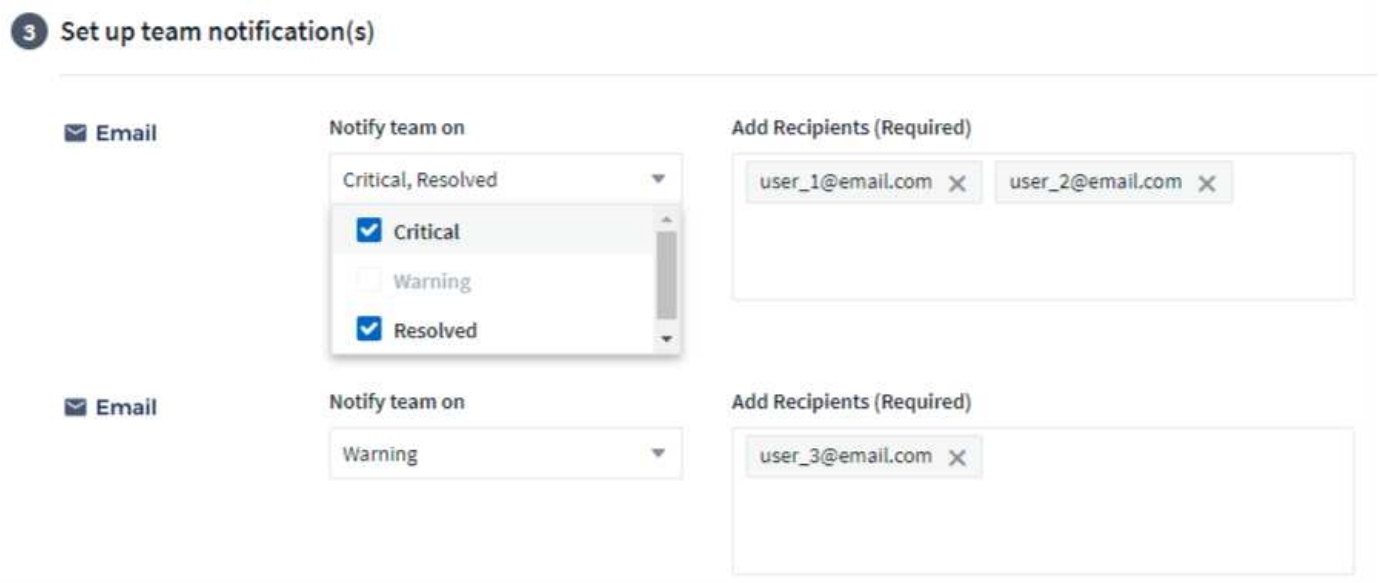
Sélectionnez le type de notification et les destinataires

Dans la section *Configurer les notifications d'équipe*, vous pouvez choisir d'alerter votre équipe par e-mail ou par Webhook.



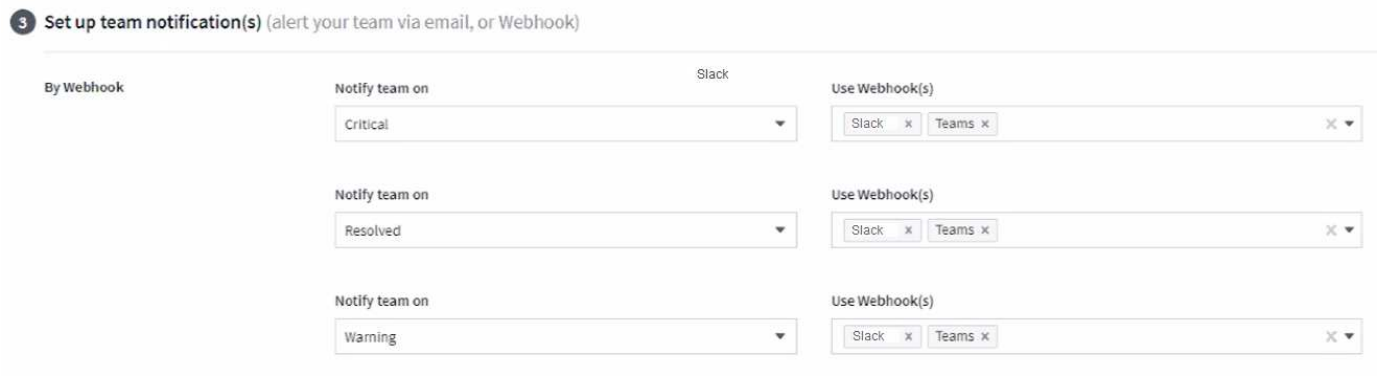
Alerte par e-mail :

Spécifiez les destinataires de courrier électronique pour les notifications d'alerte. Si vous le souhaitez, vous pouvez choisir différents destinataires pour les avertissements ou les alertes critiques.



Alerte via Webhook :

Spécifiez le(s) webhook(s) pour les notifications d'alerte. Si vous le souhaitez, vous pouvez choisir différents webhooks pour les alertes d'avertissement ou critiques.



Les notifications du collecteur de données ONTAP ont priorité sur toutes les notifications de surveillance spécifiques pertinentes pour le cluster/collecteur de données. La liste de destinataires que vous avez définie pour le collecteur de données lui-même recevra les alertes du collecteur de données. S'il n'y a pas d'alertes de collecteur de données actives, les alertes générées par le moniteur seront envoyées à des destinataires de moniteur spécifiques.

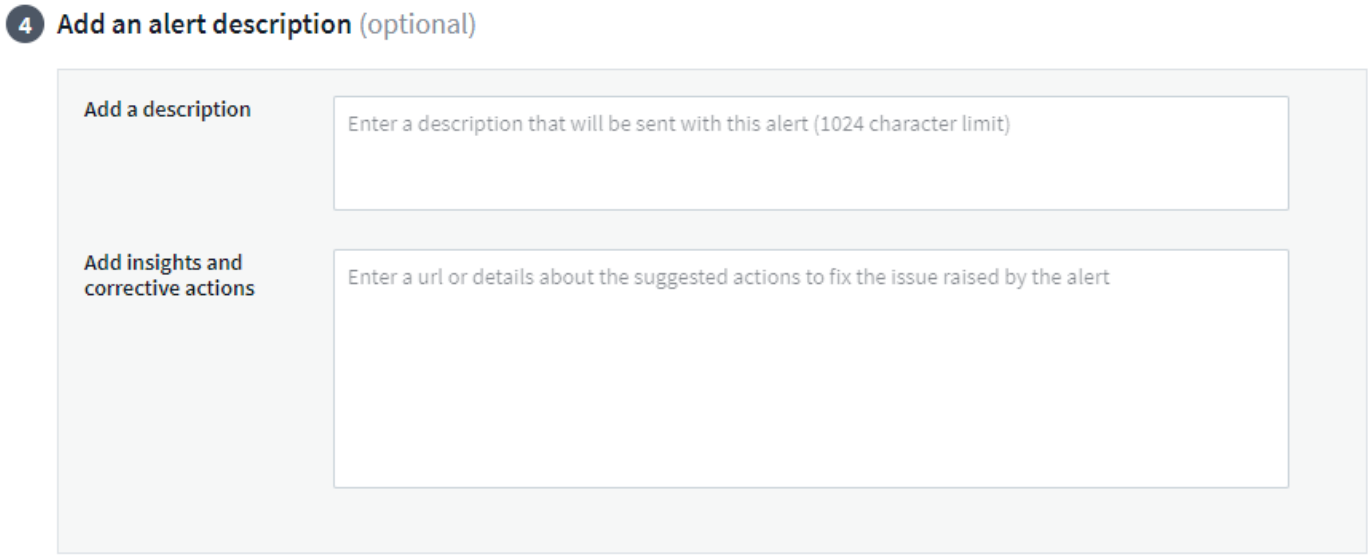
Définition d'actions correctives ou d'informations supplémentaires

Vous pouvez ajouter une description facultative ainsi que des informations supplémentaires et/ou des actions correctives en remplissant la section **Ajouter une description d'alerte**. La description peut contenir jusqu'à 1024 caractères et sera envoyée avec l'alerte. Le champ Informations/Actions correctives peut contenir jusqu'à 67 000 caractères et sera affiché dans la section récapitulative de la page de destination de l'alerte.

Dans ces champs, vous pouvez fournir des notes, des liens ou des étapes à suivre pour corriger ou traiter l'alerte.

Vous pouvez ajouter n'importe quel attribut d'objet (par exemple, le nom de stockage) comme paramètre à une description d'alerte. Par exemple, vous pouvez définir des paramètres pour le nom du volume et le nom du stockage dans une description telle que : « Latence élevée pour le volume :

%%relatedObject.volume.name%%, Stockage : *%%relatedObject.storage.name%%* ».



Sauvegardez votre moniteur

1. Si vous le souhaitez, vous pouvez ajouter une description du moniteur.
2. Donnez au moniteur un nom significatif et cliquez sur **Enregistrer**.

   Votre nouveau moniteur est ajouté à la liste des moniteurs actifs.

Liste des moniteurs

La page Moniteur répertorie les moniteurs actuellement configurés, affichant les éléments suivants :

- Nom du moniteur
- Statut
- Objet/métrique surveillé
- Conditions du moniteur

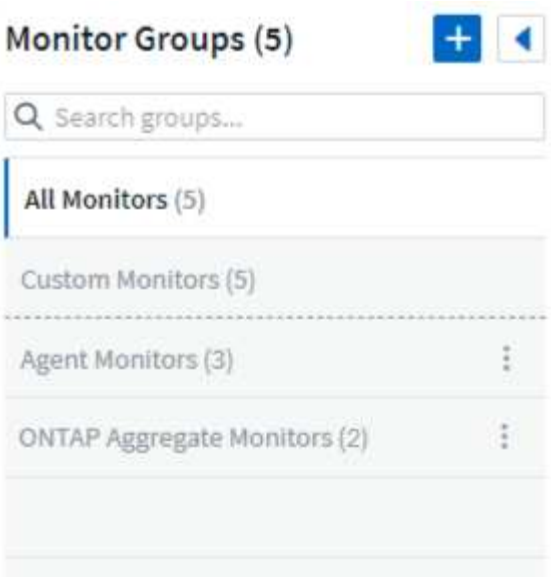
Vous pouvez choisir de suspendre temporairement la surveillance d'un type d'objet en cliquant sur le menu à droite du moniteur et en sélectionnant **Pause**. Lorsque vous êtes prêt à reprendre la surveillance, cliquez sur **Reprendre**.

Vous pouvez copier un moniteur en sélectionnant **Dupliquer** dans le menu. Vous pouvez ensuite modifier le nouveau moniteur et changer l'objet/la métrique, le filtre, les conditions, les destinataires des e-mails, etc.

Si un moniteur n'est plus nécessaire, vous pouvez le supprimer en sélectionnant **Supprimer** dans le menu.

Groupes de surveillance

Le regroupement vous permet d'afficher et de gérer les moniteurs associés. Par exemple, vous pouvez disposer d'un groupe de surveillance dédié au stockage sur votre locataire ou de surveillances pertinentes pour une certaine liste de destinataires.



Les groupes de moniteurs suivants sont affichés. Le nombre de moniteurs contenus dans un groupe est indiqué à côté du nom du groupe.

- **Tous les moniteurs** répertorie tous les moniteurs.
- **Moniteurs personnalisés** répertorie tous les moniteurs créés par l'utilisateur.
- **Moniteurs suspendus** répertorie tous les moniteurs système qui ont été suspendus par Data Infrastructure Insights.
- Data Infrastructure Insights affichera également un certain nombre de **Groupes de surveillance système**, qui répertorieront un ou plusieurs groupes de"moniteurs définis par le système" , y compris les moniteurs d'infrastructure et de charge de travail ONTAP .

Les moniteurs personnalisés peuvent être suspendus, repris, supprimés ou déplacés vers un autre groupe. Les moniteurs définis par le système peuvent être suspendus et repris, mais ne peuvent pas être supprimés ou déplacés.

Moniteurs suspendus

Ce groupe ne sera affiché que si Data Infrastructure Insights a suspendu un ou plusieurs moniteurs. Un moniteur peut être suspendu s'il génère des alertes excessives ou continues. Si le moniteur est un moniteur personnalisé, modifiez les conditions pour empêcher l'alerte continue, puis reprenez le moniteur. Le moniteur sera supprimé du groupe Moniteurs suspendus lorsque le problème à l'origine de la suspension sera résolu.

Moniteurs définis par le système

Ces groupes afficheront les moniteurs fournis par Data Infrastructure Insights, à condition que votre environnement contienne les périphériques et/ou la disponibilité des journaux requis par les moniteurs.

Les moniteurs définis par le système ne peuvent pas être modifiés, déplacés vers un autre groupe ou supprimés. Cependant, vous pouvez dupliquer un moniteur système et modifier ou déplacer le doublon.

Les moniteurs système peuvent inclure des moniteurs pour l'infrastructure ONTAP (stockage, volume, etc.) ou les charges de travail (c'est-à-dire les moniteurs de journaux) ou d'autres groupes. NetApp évalue en permanence les besoins des clients et les fonctionnalités des produits, et mettra à jour ou ajoutera des moniteurs et des groupes système selon les besoins.

Groupes de moniteurs personnalisés

Vous pouvez créer vos propres groupes pour contenir des moniteurs en fonction de vos besoins. Par exemple, vous souhaiterez peut-être un groupe pour tous vos moniteurs liés au stockage.

Pour créer un nouveau groupe de moniteurs personnalisé, cliquez sur le bouton **"+" Créer un nouveau groupe de moniteurs**. Saisissez un nom pour le groupe et cliquez sur **Créer un groupe**. Un groupe vide est créé avec ce nom.

Pour ajouter des moniteurs au groupe, accédez au groupe *Tous les moniteurs* (recommandé) et effectuez l'une des opérations suivantes :

- Pour ajouter un seul moniteur, cliquez sur le menu à droite du moniteur et sélectionnez *Ajouter au groupe*. Choisissez le groupe auquel ajouter le moniteur.
- Cliquez sur le nom du moniteur pour ouvrir la vue d'édition du moniteur et sélectionnez un groupe dans la section *Associer à un groupe de moniteurs*.

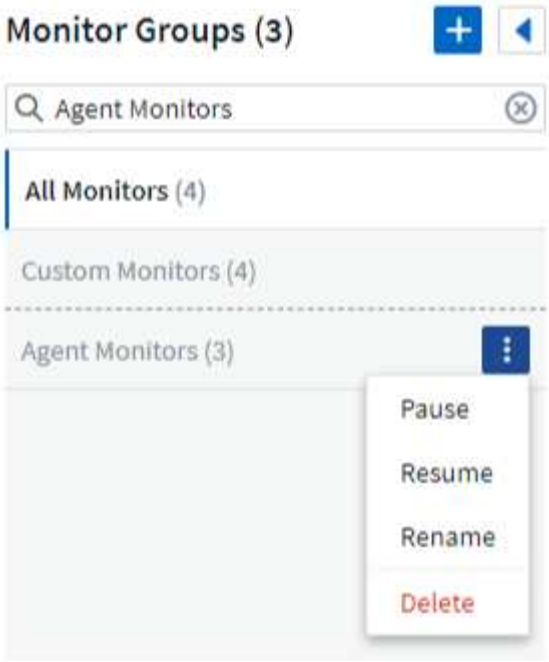
Supprimez les moniteurs en cliquant sur un groupe et en sélectionnant *Supprimer du groupe* dans le menu. Vous ne pouvez pas supprimer des moniteurs du groupe *Tous les moniteurs* ou *Moniteurs personnalisés*. Pour supprimer un moniteur de ces groupes, vous devez supprimer le moniteur lui-même.

> La suppression d'un moniteur d'un groupe ne supprime pas le moniteur de Data Infrastructure Insights. Pour supprimer complètement un moniteur, sélectionnez le moniteur et cliquez sur *Supprimer*. Cela le supprime également du groupe auquel il appartenait et il n'est plus disponible pour aucun utilisateur.

Vous pouvez également déplacer un moniteur vers un groupe différent de la même manière, en sélectionnant *Déplacer vers le groupe*.

Pour mettre en pause ou reprendre tous les moniteurs d'un groupe à la fois, sélectionnez le menu du groupe et cliquez sur *Pause* ou *Reprendre*.

Utilisez le même menu pour renommer ou supprimer un groupe. La suppression d'un groupe ne supprime pas les moniteurs de Data Infrastructure Insights; ils sont toujours disponibles dans *Tous les moniteurs*.



Moniteurs définis par le système

Data Infrastructure Insights comprend un certain nombre de moniteurs définis par le système pour les métriques et les journaux. Les moniteurs système disponibles dépendent des collecteurs de données présents sur votre locataire. De ce fait, les moniteurs disponibles dans Data Infrastructure Insights peuvent changer à mesure que des collecteurs de données sont ajoutés ou que leurs configurations sont modifiées.

Voir le"Moniteurs définis par le système" page pour les descriptions des moniteurs inclus avec Data Infrastructure Insights.

Plus d'informations

- "Affichage et suppression des alertes"

Affichage et gestion des alertes des moniteurs

Data Infrastructure Insights affiche des alertes lorsque"seuils surveillés" sont dépassés.

Les moniteurs et les alertes sont disponibles dans Data Infrastructure Insights Standard Edition et versions ultérieures.

Affichage et gestion des alertes

Pour afficher et gérer les alertes, procédez comme suit.

1. Accédez à la page **Alertes > Toutes les alertes**.
2. Une liste contenant jusqu'aux 1 000 alertes les plus récentes s'affiche. Vous pouvez trier cette liste sur n'importe quel champ en cliquant sur l'en-tête de colonne du champ. La liste affiche les informations suivantes. Notez que toutes ces colonnes ne sont pas affichées par défaut. Vous pouvez sélectionner les colonnes à afficher en cliquant sur l'icône « engrenage » :
   - **ID d'alerte** : ID d'alerte unique généré par le système

- **Heure de déclenchement** : L'heure à laquelle le moniteur concerné a déclenché l'alerte
- **Gravité actuelle** (onglet Alertes actives) : la gravité actuelle de l'alerte active
- **Gravité maximale** (onglet Alertes résolues) ; la gravité maximale de l'alerte avant sa résolution
- **Moniteur** : Le moniteur configuré pour déclencher l'alerte
- **Déclenché le** : L'objet sur lequel le seuil surveillé a été dépassé
- **Statut** : État d'alerte actuel, *Nouveau* ou *En cours*
- **Statut actif** : *Actif* ou *Résolu*
- **Condition** : La condition de seuil qui a déclenché l'alerte
- **Métrique** : La métrique de l'objet sur laquelle le seuil surveillé a été dépassé
- **État du moniteur** : État actuel du moniteur qui a déclenché l'alerte
- **A une action corrective** : L'alerte a suggéré des actions correctives. Ouvrez la page d'alerte pour les afficher.

Vous pouvez gérer une alerte en cliquant sur le menu à droite de l'alerte et en choisissant l'une des options suivantes :

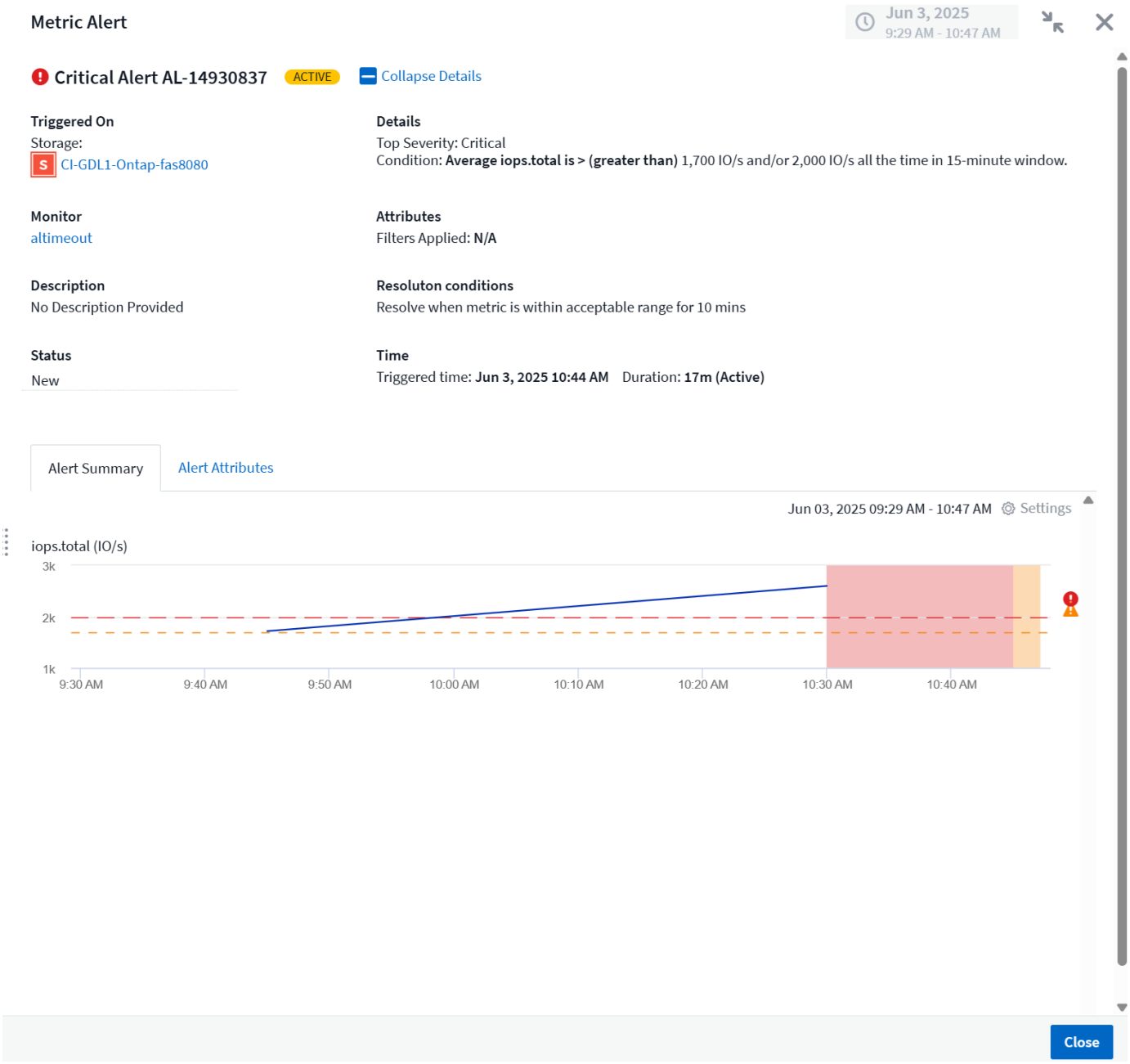
- **En cours** pour indiquer que l'alerte fait l'objet d'une enquête ou doit rester ouverte
- **Ignorer** pour supprimer l'alerte de la liste des alertes actives.

Vous pouvez gérer plusieurs alertes en sélectionnant la case à cocher à gauche de chaque alerte et en cliquant sur *Modifier le statut des alertes sélectionnées*.

Cliquer sur un ID d'alerte ouvre la page de détails de l'alerte.

Panneau de détails des alertes

Sélectionnez n'importe quelle ligne d'alerte pour ouvrir le panneau de détails de l'alerte. Le panneau de détails de l'alerte fournit des détails supplémentaires sur l'alerte, notamment un *Résumé*, une section *Performances* affichant des graphiques liés aux données de l'objet, tous les *Actifs associés* et les *Commentaires* saisis par les enquêteurs de l'alerte.



Alertes lorsque des données sont manquantes

Dans un système en temps réel tel que Data Infrastructure Insights, pour déclencher l'analyse d'un moniteur afin de décider si une alerte doit être générée, nous nous appuyons sur l'une des deux choses suivantes :

- le prochain point de données à arriver
- un minuteur à déclencher lorsqu'il n'y a pas de point de données et que vous avez attendu suffisamment longtemps

Comme c'est le cas avec une arrivée lente des données (ou aucune arrivée de données), le mécanisme de minuterie doit prendre le relais car le taux d'arrivée des données est insuffisant pour déclencher des alertes en « temps réel ». La question devient donc généralement : « Combien de temps dois-je attendre avant de fermer la fenêtre d'analyse et de regarder ce que j'ai ? » Si vous attendez trop longtemps, vous ne générez pas les alertes assez rapidement pour être utiles.

Si vous disposez d'un moniteur avec une fenêtre de 30 minutes qui détecte qu'une condition est violée par le dernier point de données avant une perte de données à long terme, une alerte sera générée car le moniteur n'a reçu aucune autre information à utiliser pour confirmer une récupération de la métrique ou pour signaler que la condition a persisté.

Alertes « actives en permanence »

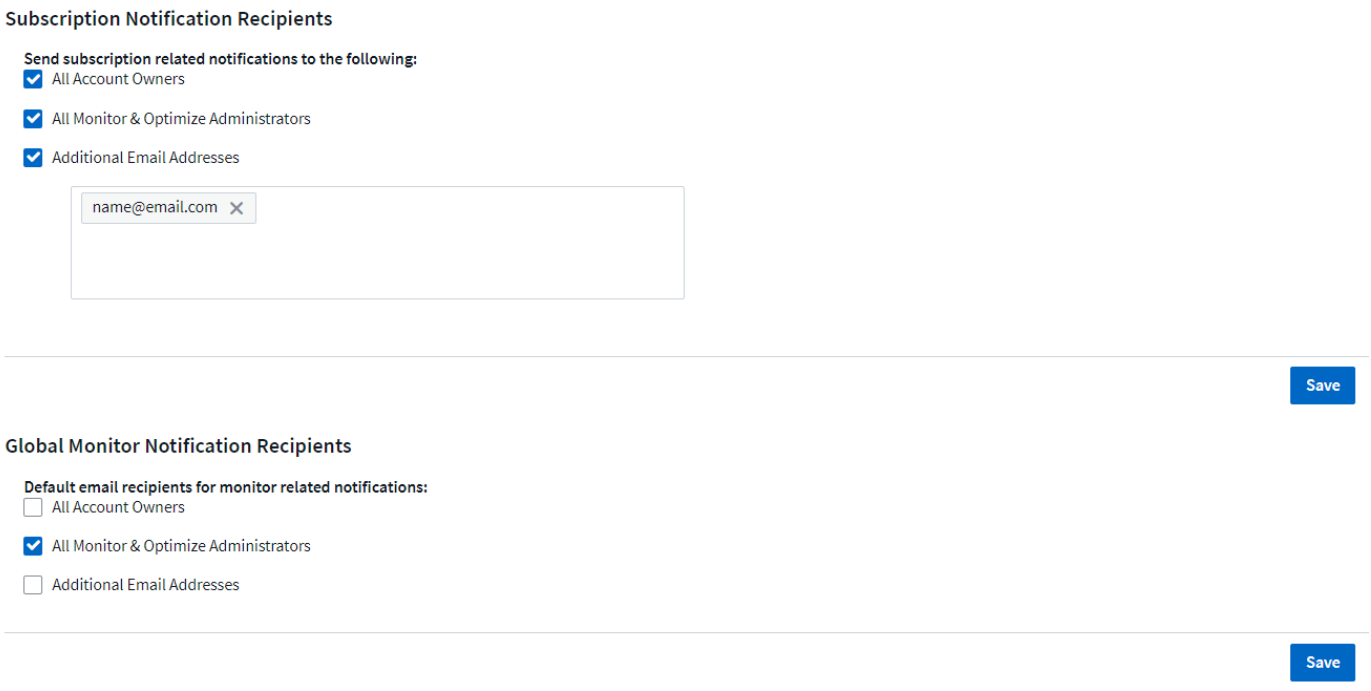
Il est possible de configurer un moniteur de telle manière que la condition existe **toujours** sur l'objet surveillé, par exemple, IOPS > 1 ou latence > 0. Ceux-ci sont souvent créés comme moniteurs « de test » puis oubliés. Ces moniteurs créent des alertes qui restent ouvertes en permanence sur les objets constitutifs, ce qui peut entraîner des problèmes de stress et de stabilité du système au fil du temps.

Pour éviter cela, Data Infrastructure Insights fermera automatiquement toute alerte « active en permanence » après 7 jours. Notez que les conditions de surveillance sous-jacentes peuvent (probablement) continuer à exister, provoquant l'émission d'une nouvelle alerte presque immédiatement, mais cette fermeture des alertes « toujours actives » atténue une partie du stress du système qui peut autrement se produire.

Configuration des notifications par e-mail

Vous pouvez configurer une liste de courrier électronique pour les notifications liées à l'abonnement, ainsi qu'une liste de courrier électronique globale de destinataires pour la notification des violations de seuil de politique de performances.

Pour configurer les paramètres des destinataires des e-mails de notification, accédez à la page **Admin > Notifications** et sélectionnez l'onglet *E-mail*.



Destinataires des notifications d'abonnement

Pour configurer les destinataires des notifications d'événements liés à l'abonnement, accédez à la section « Destinataires des notifications d'abonnement ». Vous pouvez choisir de recevoir des notifications par e-mail pour les événements liés à l'abonnement à tout ou partie des destinataires suivants :

- Tous les propriétaires de compte
- Tous les administrateurs *Monitor & Optimize*
- Adresses e-mail supplémentaires que vous spécifiez

Voici des exemples des types de notifications qui peuvent être envoyées et des actions utilisateur que vous pouvez effectuer.

Notification:	**Action de l'utilisateur :**
L'essai ou l'abonnement a été mis à jour	Consultez les détails de l'abonnement sur le"Abonnement" page
L'abonnement expirera dans 90 jours L'abonnement expirera dans 30 jours	Aucune action n'est nécessaire si le « Renouvellement automatique » est activé. Contactez le service commercial NetApp pour renouveler l'abonnement.
Le procès se termine dans 2 jours	Renouveler l'essai à partir du"Abonnement" page. Vous pouvez renouveler un essai une fois. Contactez le service commercial de NetApp pour acheter un abonnement
L'essai ou l'abonnement a expiré Le compte cessera de collecter des données dans 48 heures Le compte sera supprimé après 48 heures	Contactez le service commercial de NetApp pour acheter un abonnement

Pour garantir que vos destinataires reçoivent les notifications de Data Infrastructure Insights, ajoutez les adresses e-mail suivantes à toutes les listes « autorisées » :

- accounts@service.cloudinsights.netapp.com
- DoNotReply@cloudinsights.netapp.com

Liste globale des destinataires des alertes

Les notifications par courrier électronique des alertes sont envoyées à la liste des destinataires des alertes pour chaque action sur l'alerte. Vous pouvez choisir d'envoyer des notifications d'alerte à une liste de destinataires globale.

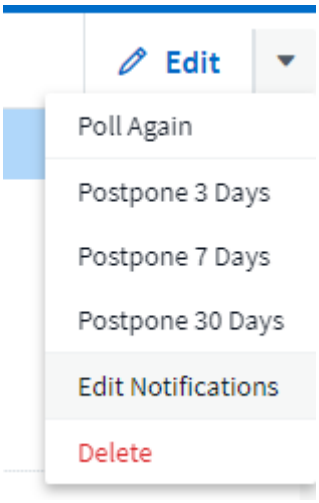
Pour configurer les destinataires d'alerte globale, choisissez les destinataires souhaités dans la section **Destinataires des notifications du moniteur global**.

Vous pouvez toujours remplacer la liste des destinataires globaux pour un moniteur individuel lors de la création ou de la modification du moniteur.

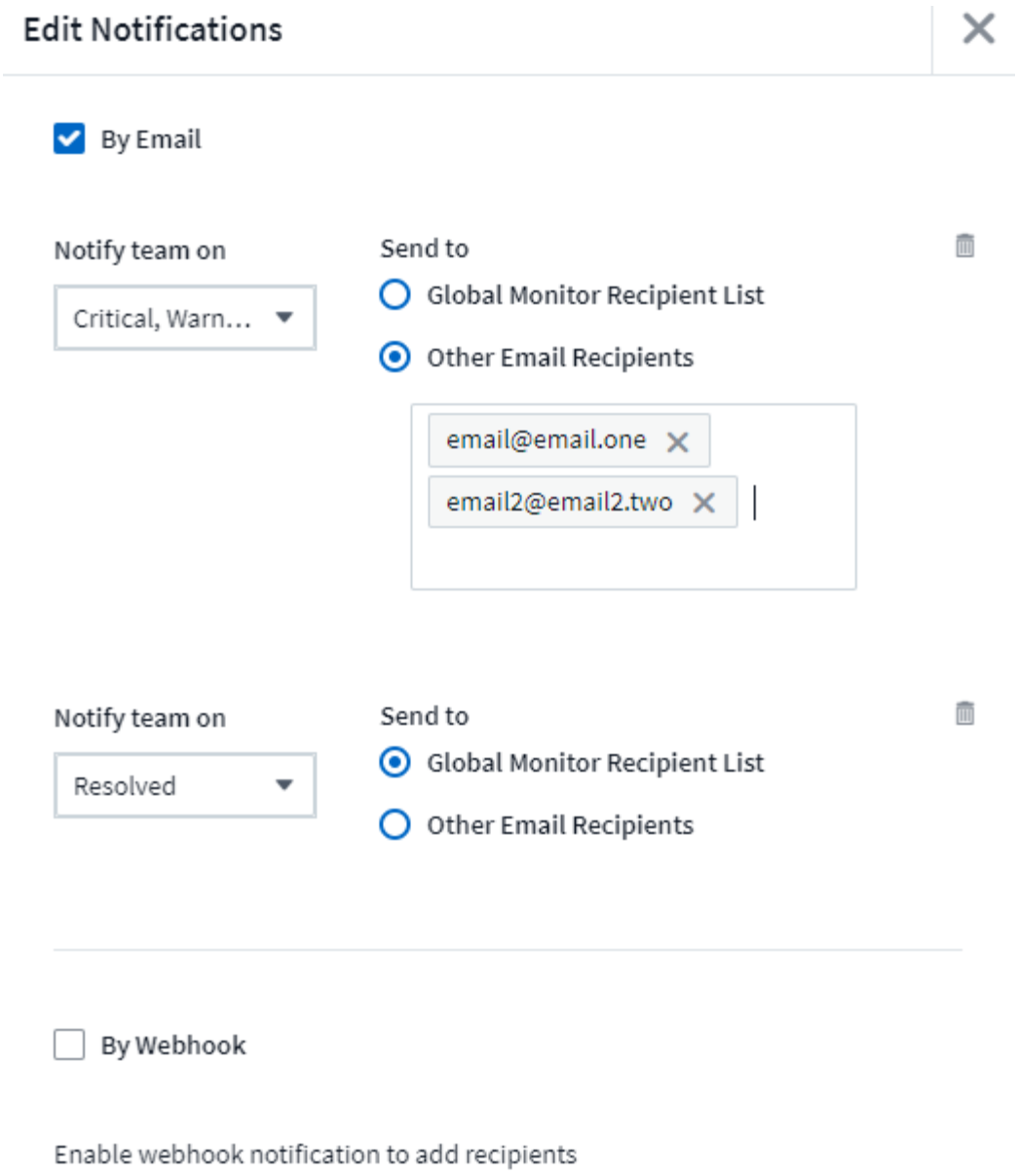
Les notifications du collecteur de données ONTAP ont priorité sur toutes les notifications de surveillance spécifiques pertinentes pour le cluster/collecteur de données. La liste de destinataires que vous avez définie pour le collecteur de données lui-même recevra les alertes du collecteur de données. S'il n'y a pas d'alertes de collecteur de données actives, les alertes générées par le moniteur seront envoyées à des destinataires de moniteur spécifiques.

Modification des notifications pour ONTAP

Vous pouvez modifier les notifications pour les clusters ONTAP en sélectionnant *Modifier les notifications* dans la liste déroulante supérieure droite d'une page de destination de stockage.



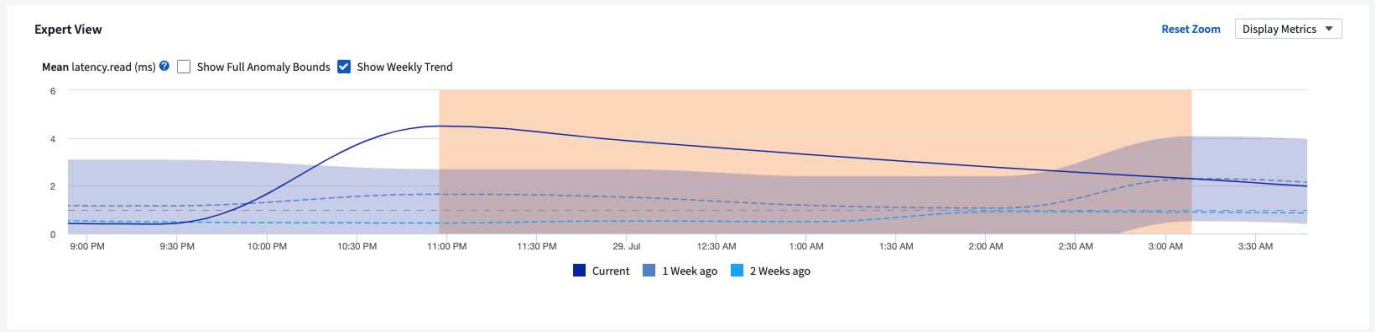
À partir de là, vous pouvez définir des notifications pour les alertes critiques, d'avertissement, d'information et/ou résolues. Chaque scénario peut notifier la liste des destinataires globaux ou d'autres destinataires de votre choix.



Moniteurs de détection d'anomalies

La détection des anomalies fournit un aperçu des changements inattendus dans les modèles de données de votre locataire. Une anomalie se produit lorsque le modèle de comportement d'un objet change, par exemple, si un objet subit un certain niveau de latence à un certain moment le mercredi, mais que la latence dépasse ce niveau à ce moment-là le mercredi suivant, ce pic serait considéré comme une anomalie. Data Infrastructure Insights permet la création de moniteurs pour alerter lorsque des anomalies telles que celle-ci se produisent.

La détection d'anomalies convient aux mesures d'objets qui présentent un modèle récurrent et prévisible. Lorsque ces mesures d'objet dépassent ou chutent en dessous de leurs niveaux attendus, Data Infrastructure Insights peut générer une alerte pour inciter à une enquête.



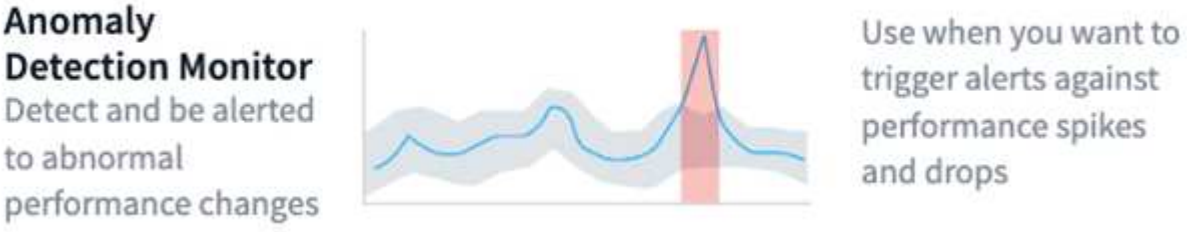
Qu’est-ce que la détection d’anomalies ?

Une anomalie se produit lorsque la valeur moyenne d’une mesure est éloignée d’un certain nombre d’écarts types de la moyenne pondérée de cette mesure pour les semaines précédentes, les semaines récentes ayant plus de poids que les semaines précédentes. Data Infrastructure Insights offre la possibilité de surveiller les données et d’alerter lorsque des anomalies sont détectées. Vous avez le choix de définir les niveaux de « sensibilité » de détection. Par exemple, une sensibilité plus élevée serait obtenue lorsque la valeur moyenne présente moins d’écarts types par rapport à la moyenne, ce qui entraînerait la génération d’un plus grand nombre d’alertes. À l’inverse, une sensibilité plus faible = plus d’écarts types par rapport à la moyenne = moins d’alertes.

La surveillance de la détection des anomalies diffère de la surveillance des seuils.

- **La surveillance basée sur des seuils** fonctionne lorsque vous avez des seuils prédéfinis pour des mesures spécifiques. En d’autres termes, lorsque vous avez une compréhension claire de ce qui est attendu (c’est-à-dire dans une fourchette normale).

- **La surveillance de détection d’anomalies** utilise des algorithmes d’apprentissage automatique pour identifier les valeurs aberrantes qui s’écartent de la norme, lorsque la définition de « normal » n’est pas claire.



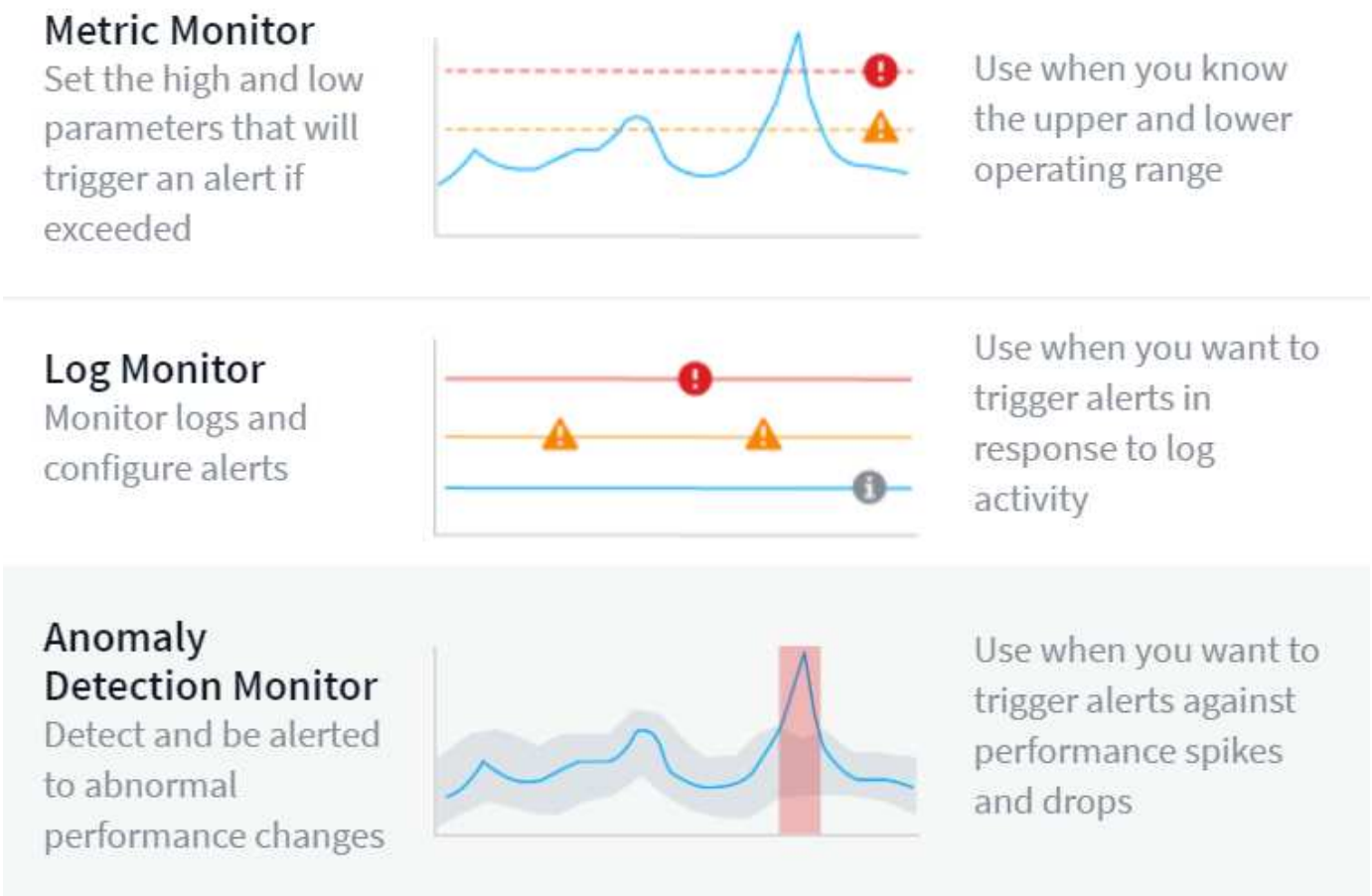
Quand aurais-je besoin de la détection d'anomalies ?

La surveillance de la détection des anomalies peut fournir des alertes utiles dans de nombreuses situations, notamment les suivantes :

- Lorsque la définition de *normal* n'est pas claire. Par exemple, les taux d'erreur SAN peuvent être attendus à des niveaux variables selon le port. Alerter sur une erreur est bruyant et inutile, mais une augmentation soudaine ou significative pourrait indiquer un problème généralisé.
- Là où il y a des changements au fil du temps. Charges de travail qui présentent une saisonnalité (c'est-à-dire qu'elles sont occupées ou calmes à certains moments). Cela peut inclure des périodes de silence inattendues qui peuvent indiquer un blocage du lot.
- Travailler avec de grandes quantités de données où la définition et le réglage manuels des seuils ne sont pas pratiques. Par exemple, un locataire avec un grand nombre d'hôtes et/ou de volumes avec des charges de travail variables. Chacun peut avoir des SLA différents, il est donc important de comprendre ceux qui dépassent la norme.

Création d'un moniteur de détection d'anomalies

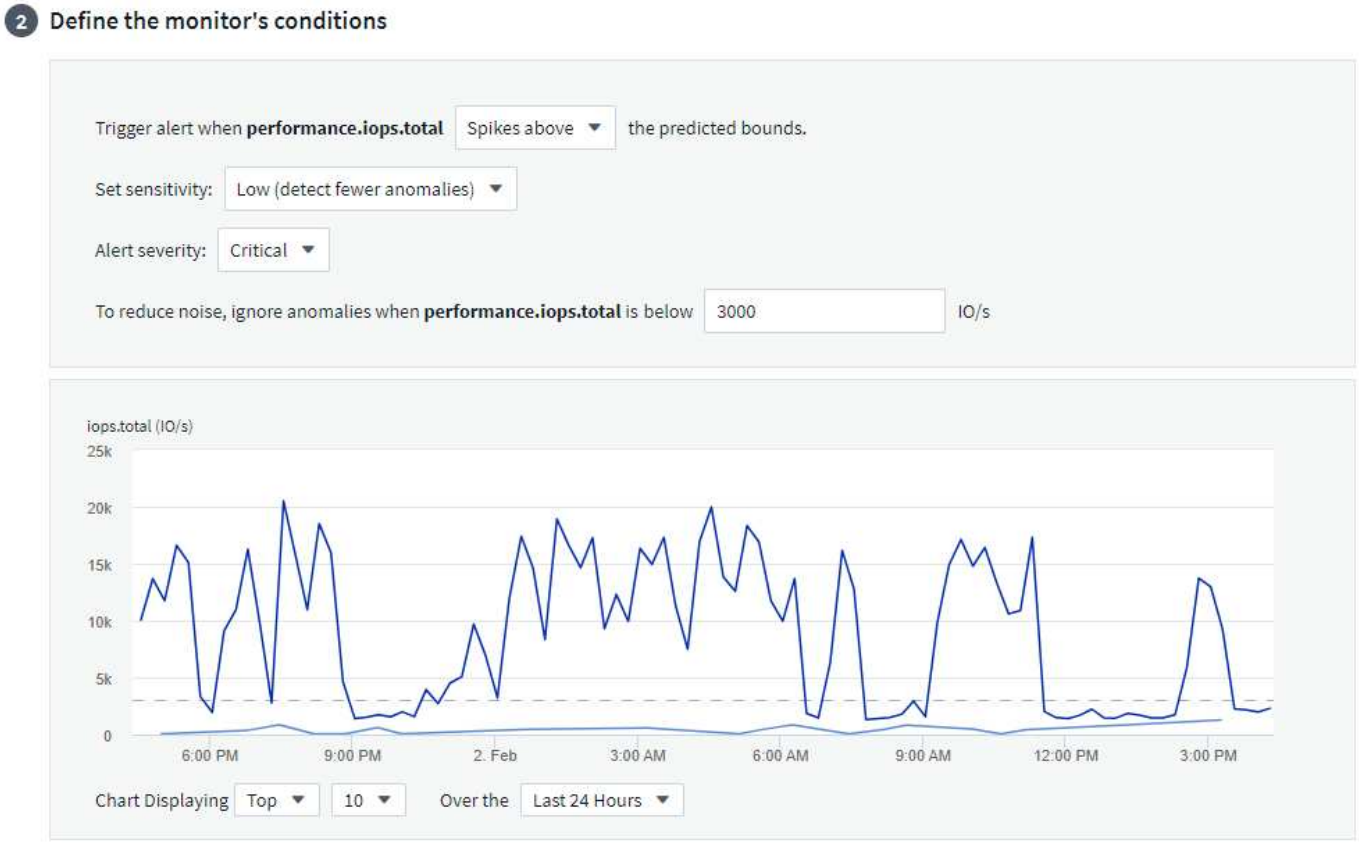
Pour alerter sur les anomalies, créez un moniteur en accédant à **Observabilité > Alertes > +Moniteur**. Sélectionnez *Anomaly Detection Monitor* comme type de moniteur.



Choisissez l'objet et la métrique que vous souhaitez surveiller. Vous pouvez définir des filtres et des regroupements comme avec d'autres types de moniteurs.

Ensuite, définissez les conditions du moniteur.

- Déclenchez une alerte lorsque la métrique sélectionnée dépasse les limites prévues, chute en dessous de ces limites ou les deux.
- Définissez la sensibilité sur *Moyenne*, *Faible* (moins d'anomalies sont détectées) ou *Élevée* (plus d'anomalies sont détectées).
- Déterminez si le niveau d'alerte est *Critique* ou *Avertissement*.
- Vous pouvez également définir une valeur en dessous de laquelle les anomalies sont *ignorées*. Cela peut aider à réduire le bruit. Cette valeur est affichée sous forme de ligne pointillée sur l'exemple de graphique.



Enfin, vous pouvez configurer une méthode de livraison pour les alertes (e-mail, webhook ou les deux), donner au moniteur une description facultative ou des actions correctives et ajouter le moniteur à un groupe personnalisé, si vous le souhaitez.

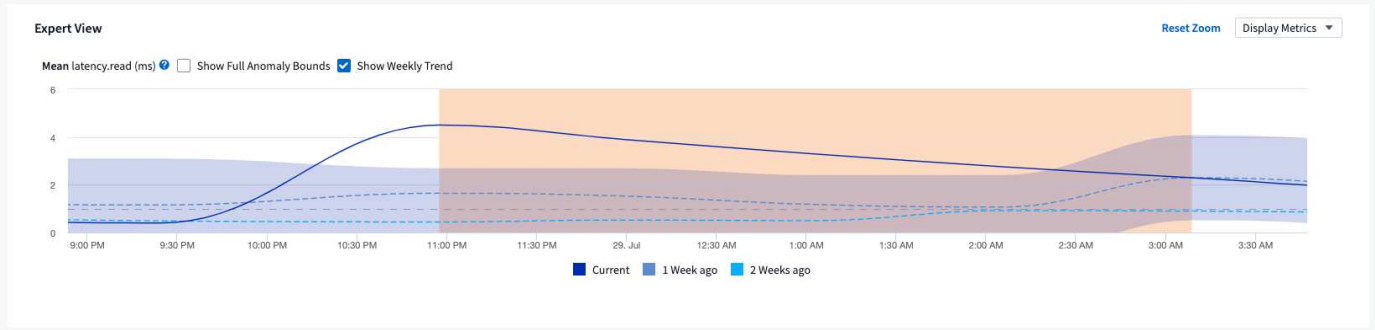
Enregistrez le moniteur avec un nom significatif et vous avez terminé.

Lors de sa création, le moniteur analyse les données de la semaine précédente pour établir une base de référence initiale. La détection des anomalies devient plus précise à mesure que le temps passe et que l'historique se déroule.

> Lorsqu'un moniteur est créé, DII examine toutes les données existantes de la semaine précédente pour détecter des pics ou des baisses de données significatifs ; ceux-ci sont considérés comme des anomalies. Au cours de la première semaine suivant la création du moniteur (la phase « d'apprentissage »), il existe un risque d'augmentation du « bruit » dans les alertes. Pour atténuer ce bruit, seuls les pics ou les chutes durant plus de 30 minutes sont considérés comme des anomalies et génèrent des alertes. Au cours de la semaine suivante, à mesure que davantage de données sont analysées, le bruit diminue généralement et un pic ou une baisse significative durant une certaine période sera considéré comme une anomalie.

Visualisation des anomalies

Sur une page de destination d'alerte, les alertes déclenchées lorsque des anomalies sont détectées afficheront une bande en surbrillance dans le graphique, à partir du moment où la métrique a dépassé les limites prévues jusqu'au moment où elle est revenue à l'intérieur de ces limites.



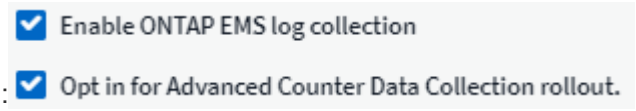
Lorsque vous consultez un graphique d'anomalie sur une page de destination d'alerte, vous pouvez choisir les options suivantes :

- Tendance hebdomadaire : comparez les valeurs à la même heure, au même jour des semaines précédentes, jusqu'à 5 semaines précédentes.
- Limites d'anomalie complètes : par défaut, le graphique se concentre sur la valeur de la métrique afin que vous puissiez mieux analyser le comportement de la métrique. Sélectionnez pour afficher les limites complètes de l'anomalie (valeur maximale, etc.)

Vous pouvez également afficher les objets qui ont contribué à l'anomalie en les sélectionnant dans la section des performances de la page de destination. Le graphique montrera le comportement des objets sélectionnés.

Moniteurs système

Data Infrastructure Insights comprend un certain nombre de moniteurs définis par le système pour les métriques et les journaux. Les moniteurs système disponibles dépendent des collecteurs de données présents sur votre locataire. De ce fait, les moniteurs disponibles dans Data Infrastructure Insights peuvent changer à mesure que des collecteurs de données sont ajoutés ou que leurs configurations sont modifiées.

De nombreux moniteurs système sont dans l'état *Paused* par défaut. Vous pouvez activer un moniteur système en sélectionnant l'option *Reprendre* pour le moniteur. Assurez-vous que *Collecte de données de compteur avancée* et *Activer la collecte de journaux ONTAP EMS* sont activés dans le collecteur de données ONTAP sous *Configuration avancée* : 

toc:[]

Descriptions des moniteurs

Les moniteurs définis par le système sont composés de mesures et de conditions prédéfinies, ainsi que de descriptions par défaut et d'actions correctives, qui ne peuvent pas être modifiées. Vous *pouvez* modifier la liste des destinataires des notifications pour les moniteurs définis par le système. Pour afficher les métriques, les conditions, la description et les actions correctives, ou pour modifier la liste des destinataires, ouvrez un groupe de moniteurs défini par le système et cliquez sur le nom du moniteur dans la liste.

Les groupes de moniteurs définis par le système ne peuvent pas être modifiés ou supprimés.

Les moniteurs définis par le système suivants sont disponibles, dans les groupes indiqués.

- * ONTAP Infrastructure* inclut des moniteurs pour les problèmes liés à l'infrastructure dans les clusters ONTAP .
- * Exemples de charge de travail ONTAP * inclut des moniteurs pour les problèmes liés à la charge de travail.
- Les moniteurs des deux groupes sont par défaut à l'état *Paused*.

Vous trouverez ci-dessous les moniteurs système actuellement inclus avec Data Infrastructure Insights:

Moniteurs métriques

Nom du moniteur	Gravité	Description du moniteur	Action corrective

Utilisation élevée des ports Fibre Channel	CRITIQUE	Les ports du protocole Fibre Channel sont utilisés pour recevoir et transférer le trafic SAN entre le système hôte client et les LUN ONTAP . Si l'utilisation du port est élevée, elle deviendra un goulot d'étranglement et affectera à terme les performances des charges de travail sensibles du protocole Fibre Channel. Une alerte d'avertissement indique qu'une action planifiée doit être prise pour équilibrer le trafic réseau. Une alerte critique indique qu'une interruption de service est imminente et que des mesures d'urgence doivent être prises pour équilibrer le trafic réseau afin de garantir la continuité du service.	Si le seuil critique est dépassé, envisagez des actions immédiates pour minimiser les interruptions de service : 1. Déplacez les charges de travail vers un autre port FCP moins utilisé. 2. Limitez le trafic de certains LUN uniquement aux travaux essentiels, soit via des politiques QoS dans ONTAP , soit via une configuration côté hôte pour alléger l'utilisation des ports FCP.… Si le seuil d'avertissement est dépassé, prévoyez de prendre les mesures suivantes : 1. Configurez davantage de ports FCP pour gérer le trafic de données afin que l'utilisation du port soit répartie entre davantage de ports. 2. Déplacez les charges de travail vers un autre port FCP moins utilisé. 3. Limitez le trafic de certains LUN uniquement aux travaux essentiels, soit via des politiques QoS dans ONTAP , soit via une configuration côté hôte pour alléger l'utilisation des ports FCP.

Latence Lun élevée	CRITIQUE	Les LUN sont des objets qui servent au trafic d'E/S souvent généré par des applications sensibles aux performances telles que les bases de données. Des latences LUN élevées signifient que les applications elles-mêmes peuvent souffrir et être incapables d'accomplir leurs tâches.…Une alerte d'avertissement indique qu'une action planifiée doit être entreprise pour déplacer le LUN vers le nœud ou l'agrégat approprié.…Une alerte critique indique qu'une interruption de service est imminente et que des mesures d'urgence doivent être prises pour assurer la continuité du service. Voici les latences attendues en fonction du type de support : SSD jusqu'à 1 à 2 millisecondes ; SAS jusqu'à 8 à 10 millisecondes et disque dur SATA 17 à 20 millisecondes	Si le seuil critique est dépassé, envisagez les actions suivantes pour minimiser les interruptions de service : si le LUN ou son volume est associé à une politique de qualité de service (QoS), évaluez ses limites de seuil et vérifiez si elles entraînent une limitation de la charge de travail du LUN. Si le seuil d'avertissement est dépassé, prévoyez de prendre les mesures suivantes : 1. Si l'agrégat connaît également une utilisation élevée, déplacez le LUN vers un autre agrégat. 2. Si le nœud subit également une utilisation élevée, déplacez le volume vers un autre nœud ou réduisez la charge de travail totale du nœud. 3. Si le LUN ou son volume est associé à une stratégie QoS, évaluez ses limites de seuil et vérifiez si elles entraînent une limitation de la charge de travail du LUN.

Utilisation élevée des ports réseau	CRITIQUE	Les ports réseau sont utilisés pour recevoir et transférer le trafic des protocoles NFS, CIFS et iSCSI entre les systèmes hôtes clients et les volumes ONTAP . Si l'utilisation du port est élevée, cela devient un goulot d'étranglement et cela affectera à terme les performances des charges de travail NFS, CIFS et iSCSI.…Une alerte d'avertissement indique qu'une action planifiée doit être prise pour équilibrer le trafic réseau.…Une alerte critique indique qu'une interruption de service est imminente et que des mesures d'urgence doivent être prises pour équilibrer le trafic réseau afin de garantir la continuité du service.	Si le seuil critique est dépassé, envisagez les actions immédiates suivantes pour minimiser les interruptions de service : 1. Limitez le trafic de certains volumes uniquement aux travaux essentiels, soit via des politiques QoS dans ONTAP , soit via une analyse côté hôte pour réduire l'utilisation des ports réseau. 2. Configurez un ou plusieurs volumes pour utiliser un autre port réseau moins utilisé.… Si le seuil d'avertissement est dépassé, envisagez les actions immédiates suivantes : 1. Configurez davantage de ports réseau pour gérer le trafic de données afin que l'utilisation du port soit répartie entre davantage de ports. 2. Configurez un ou plusieurs volumes pour utiliser un autre port réseau moins utilisé.

Latence de l’espace de noms NVMe élevée	CRITIQUE	Les espaces de noms NVMe sont des objets qui servent au trafic d’E/S généré par des applications sensibles aux performances telles que les bases de données. Une latence élevée des espaces de noms NVMe signifie que les applications elles-mêmes peuvent souffrir et être incapables d’accomplir leurs tâches.…Une alerte d’avertissement indique qu’une action planifiée doit être entreprise pour déplacer le LUN vers le nœud ou l’agrégat approprié.…Une alerte critique indique qu’une interruption de service est imminente et que des mesures d’urgence doivent être prises pour assurer la continuité du service.	Si le seuil critique est dépassé, envisagez des actions immédiates pour minimiser les interruptions de service : si l’espace de noms NVMe ou son volume dispose d’une politique de qualité de service qui lui est attribuée, évaluez ses seuils de limite au cas où ils entraîneraient une limitation de la charge de travail de l’espace de noms NVMe. Si le seuil d’avertissement est dépassé, envisagez de prendre les mesures suivantes : 1. Si l’agrégat connaît également une utilisation élevée, déplacez le LUN vers un autre agrégat. 2. Si le nœud subit également une utilisation élevée, déplacez le volume vers un autre nœud ou réduisez la charge de travail totale du nœud. 3. Si l’espace de noms NVMe ou son volume dispose d’une politique QoS qui lui est attribuée, évaluez ses seuils de limite au cas où ils entraîneraient une limitation de la charge de travail de l’espace de noms NVMe.

Capacité QTree complète	CRITIQUE	Un qtree est un système de fichiers défini logiquement qui peut exister en tant que sous-répertoire spécial du répertoire racine dans un volume. Chaque qtree dispose d'un quota d'espace par défaut ou d'un quota défini par une politique de quota pour limiter la quantité de données stockées dans l'arbre dans la capacité du volume.…Une alerte d'avertissement indique qu'une action planifiée doit être entreprise pour augmenter l'espace.…Une alerte critique indique qu'une interruption de service est imminente et que des mesures d'urgence doivent être prises pour libérer de l'espace afin d'assurer la continuité du service.	Si le seuil critique est dépassé, envisagez des actions immédiates pour minimiser les interruptions de service : 1. Augmentez l'espace du qtree afin de s'adapter à la croissance. 2. Supprimez les données indésirables pour libérer de l'espace.… Si le seuil d'avertissement est dépassé, prévoyez de prendre les mesures immédiates suivantes : 1. Augmentez l'espace du qtree afin de s'adapter à la croissance. 2. Supprimez les données indésirables pour libérer de l'espace.

Limite stricte de capacité de QTree	CRITIQUE	Un qtree est un système de fichiers défini logiquement qui peut exister en tant que sous-répertoire spécial du répertoire racine dans un volume. Chaque qtree dispose d'un quota d'espace mesuré en Ko qui est utilisé pour stocker des données afin de contrôler la croissance du volume de données utilisateur et de ne pas dépasser sa capacité totale.…Un qtree maintient un quota de capacité de stockage souple qui fournit une alerte à l'utilisateur de manière proactive avant d'atteindre la limite de quota de capacité totale dans le qtree et de ne plus pouvoir stocker de données. La surveillance de la quantité de données stockées dans un qtree garantit que l'utilisateur reçoit un service de données ininterrompu.	Si le seuil critique est dépassé, envisagez les actions immédiates suivantes pour minimiser les interruptions de service : 1. Augmenter le quota d'espace des arbres afin de s'adapter à la croissance 2. Demandez à l'utilisateur de supprimer les données indésirables dans l'arborescence pour libérer de l'espace

Limite souple de capacité QTree	AVERTISSEMENT	Un qtree est un système de fichiers défini logiquement qui peut exister en tant que sous-répertoire spécial du répertoire racine dans un volume. Chaque qtree dispose d'un quota d'espace mesuré en Ko qu'il peut utiliser pour stocker des données afin de contrôler la croissance du volume de données utilisateur et de ne pas dépasser sa capacité totale.…Un qtree maintient un quota de capacité de stockage souple qui fournit une alerte à l'utilisateur de manière proactive avant d'atteindre la limite de quota de capacité totale dans le qtree et de ne plus pouvoir stocker de données. La surveillance de la quantité de données stockées dans un qtree garantit que l'utilisateur reçoit un service de données ininterrompu.	Si le seuil d'avertissement est dépassé, envisagez les actions immédiates suivantes : 1. Augmenter le quota d'espace des arbres pour s'adapter à la croissance. 2. Demandez à l'utilisateur de supprimer les données indésirables dans l'arborescence pour libérer de l'espace.

Limite stricte des fichiers QTree	CRITIQUE	Un qtree est un système de fichiers défini logiquement qui peut exister en tant que sous-répertoire spécial du répertoire racine dans un volume. Chaque qtree dispose d'un quota du nombre de fichiers qu'il peut contenir pour maintenir une taille de système de fichiers gérable au sein du volume.…Un qtree maintient un quota de nombre de fichiers fixe au-delà duquel les nouveaux fichiers de l'arbre sont refusés. La surveillance du nombre de fichiers dans un qtree garantit que l'utilisateur reçoit un service de données ininterrompu.	Si le seuil critique est dépassé, envisagez des actions immédiates pour minimiser les interruptions de service : 1. Augmentez le quota de nombre de fichiers pour le qtree. 2. Supprimez les fichiers indésirables du système de fichiers qtree.
Limite souple des fichiers QTree	AVERTISSEMENT	Un qtree est un système de fichiers défini logiquement qui peut exister en tant que sous-répertoire spécial du répertoire racine dans un volume. Chaque qtree dispose d'un quota du nombre de fichiers qu'il peut contenir afin de maintenir une taille de système de fichiers gérable au sein du volume. Un qtree maintient un quota de nombre de fichiers souple pour fournir une alerte à l'utilisateur de manière proactive avant d'atteindre la limite de fichiers dans le qtree et de ne pas pouvoir stocker de fichiers supplémentaires. La surveillance du nombre de fichiers dans un qtree garantit que l'utilisateur reçoit un service de données ininterrompu.	Si le seuil d'avertissement est dépassé, prévoyez de prendre les mesures immédiates suivantes : 1. Augmentez le quota de nombre de fichiers pour le qtree. 2. Supprimez les fichiers indésirables du système de fichiers qtree.

Instantané Réserve Espace Plein	CRITIQUE	La capacité de stockage d'un volume est nécessaire pour stocker les données d'application et de client. Une partie de cet espace, appelée espace réservé aux instantanés, est utilisée pour stocker des instantanés qui permettent de protéger les données localement. Plus les données nouvelles et mises à jour sont stockées dans le volume ONTAP , plus la capacité de snapshot est utilisée et moins la capacité de stockage de snapshot est disponible pour les données nouvelles ou mises à jour futures. Si la capacité des données de snapshot dans un volume atteint l'espace de réserve total de snapshot, le client peut être incapable de stocker de nouvelles données de snapshot et le niveau de protection des données dans le volume peut être réduit. La surveillance de la capacité de snapshot du volume utilisé garantit la continuité des services de données.	Si le seuil critique est dépassé, envisagez des actions immédiates pour minimiser les interruptions de service : 1. Configurez les instantanés pour utiliser l'espace de données dans le volume lorsque la réserve d'instantanés est pleine. 2. Supprimez quelques anciens instantanés indésirables pour libérer de l'espace.… Si le seuil d'avertissement est dépassé, prévoyez de prendre les mesures immédiates suivantes : 1. Augmentez l'espace de réserve d'instantanés dans le volume pour s'adapter à la croissance. 2. Configurez les instantanés pour utiliser l'espace de données dans le volume lorsque la réserve d'instantanés est pleine.

Limite de capacité de stockage	CRITIQUE	Lorsqu'un pool de stockage (agrégat) se remplit, les opérations d'E/S ralentissent et finissent par s'arrêter, ce qui entraîne un incident de panne de stockage. Une alerte d'avertissement indique qu'une action planifiée doit être entreprise prochainement pour restaurer l'espace libre minimum. Une alerte critique indique qu'une interruption de service est imminente et que des mesures d'urgence doivent être prises pour libérer de l'espace afin d'assurer la continuité du service.	Si le seuil critique est dépassé, envisagez immédiatement les actions suivantes pour minimiser les interruptions de service : 1. Supprimer les instantanés sur les volumes non critiques. 2. Supprimez les volumes ou les LUN qui sont des charges de travail non essentielles et qui peuvent être restaurés à partir de copies hors stockage. Si le seuil d'avertissement est dépassé, planifiez les actions immédiates suivantes : 1. Déplacez un ou plusieurs volumes vers un autre emplacement de stockage. 2. Ajoutez plus de capacité de stockage. 3. Modifiez les paramètres d'efficacité du stockage ou hiérarchisez les données inactives vers le stockage cloud.

Limite de performance de stockage	CRITIQUE	Lorsqu'un système de stockage atteint sa limite de performances, les opérations ralentissent, la latence augmente et les charges de travail et les applications peuvent commencer à échouer. ONTAP évalue l'utilisation du pool de stockage pour les charges de travail et estime le pourcentage de performances consommé.…Une alerte d'avertissement indique qu'une action planifiée doit être prise pour réduire la charge du pool de stockage afin de garantir qu'il restera suffisamment de performances du pool de stockage pour répondre aux pics de charge de travail.…Une alerte critique indique qu'une baisse de performances est imminente et que des mesures d'urgence doivent être prises pour réduire la charge du pool de stockage afin de garantir la continuité du service.	Si le seuil critique est dépassé, envisagez les actions immédiates suivantes pour minimiser les interruptions de service : 1. Suspendez les tâches planifiées telles que les instantanés ou la réplication SnapMirror . 2. Charges de travail non essentielles inactives.… Si le seuil d'avertissement est dépassé, prenez immédiatement les mesures suivantes : 1. Déplacez une ou plusieurs charges de travail vers un autre emplacement de stockage. 2. Ajoutez davantage de nœuds de stockage (AFF) ou d'étagères de disques (FAS) et redistribuez les charges de travail 3. Modifier les caractéristiques de la charge de travail (taille des blocs, mise en cache des applications).

Limite stricte de capacité de quota utilisateur	CRITIQUE	ONTAP reconnaît les utilisateurs de systèmes Unix ou Windows qui ont le droit d'accéder aux volumes, fichiers ou répertoires d'un volume. Par conséquent, ONTAP permet aux clients de configurer la capacité de stockage pour leurs utilisateurs ou groupes d'utilisateurs de leurs systèmes Linux ou Windows. Le quota de stratégie d'utilisateur ou de groupe limite la quantité d'espace que l'utilisateur peut utiliser pour ses propres données. Une limite stricte de ce quota permet de notifier l'utilisateur lorsque la quantité de capacité utilisée dans le volume est juste avant d'atteindre le quota de capacité totale. La surveillance de la quantité de données stockées dans un quota d'utilisateur ou de groupe garantit que l'utilisateur reçoit un service de données ininterrompu.	Si le seuil critique est dépassé, envisagez les actions immédiates suivantes pour minimiser les interruptions de service : 1. Augmentez l'espace du quota utilisateur ou groupe afin de s'adapter à la croissance. 2. Demandez à l'utilisateur ou au groupe de supprimer les données indésirables pour libérer de l'espace.

Limite souple de capacité de quota utilisateur	AVERTISSEMENT	ONTAP reconnaît les utilisateurs de systèmes Unix ou Windows qui ont le droit d'accéder aux volumes, fichiers ou répertoires d'un volume. Par conséquent, ONTAP permet aux clients de configurer la capacité de stockage pour leurs utilisateurs ou groupes d'utilisateurs de leurs systèmes Linux ou Windows. Le quota de stratégie d'utilisateur ou de groupe limite la quantité d'espace que l'utilisateur peut utiliser pour ses propres données. Une limite souple de ce quota permet une notification proactive à l'utilisateur lorsque la quantité de capacité utilisée dans le volume atteint le quota de capacité totale. La surveillance de la quantité de données stockées dans un quota d'utilisateur ou de groupe garantit que l'utilisateur reçoit un service de données ininterrompu.	Si le seuil d'avertissement est dépassé, prévoyez de prendre les mesures immédiates suivantes : 1. Augmentez l'espace du quota utilisateur ou groupe afin de s'adapter à la croissance. 2. Supprimez les données indésirables pour libérer de l'espace.

Volume Capacité Plein	CRITIQUE	La capacité de stockage d'un volume est nécessaire pour stocker les données d'application et de client. Plus les données stockées dans le volume ONTAP sont nombreuses, moins il y a de disponibilité de stockage pour les données futures. Si la capacité de stockage des données dans un volume atteint la capacité de stockage totale, le client peut être incapable de stocker des données en raison d'un manque de capacité de stockage. La surveillance du volume de capacité de stockage utilisé garantit la continuité des services de données.	Si le seuil critique est dépassé, envisagez les actions immédiates suivantes pour minimiser les interruptions de service : 1. Augmentez l'espace du volume pour accueillir la croissance. 2. Supprimez les données indésirables pour libérer de l'espace. 3. Si les copies d'instantanés occupent plus d'espace que la réserve d'instantanés, supprimez les anciens instantanés ou activez la suppression automatique des instantanés de volume.…Si le seuil d'avertissement est dépassé, prévoyez de prendre les mesures immédiates suivantes : 1. Augmenter l'espace du volume afin d'accueillir la croissance 2. Si les copies d'instantanés occupent plus d'espace que la réserve d'instantanés, supprimez les anciens instantanés ou activez la suppression automatique des instantanés de volume.……

Limite de volume d’inodes	CRITIQUE	Les volumes qui stockent des fichiers utilisent des nœuds d’index (inode) pour stocker les métadonnées des fichiers. Lorsqu’un volume épuise son allocation d’inodes, aucun fichier supplémentaire ne peut y être ajouté. Une alerte d’avertissement indique qu’une action planifiée doit être entreprise pour augmenter le nombre d’inodes disponibles. Une alerte critique indique que l’épuisement de la limite de fichiers est imminent et que des mesures d’urgence doivent être prises pour libérer des inodes afin de garantir la continuité du service.	Si le seuil critique est dépassé, envisagez les actions immédiates suivantes pour minimiser les interruptions de service : 1. Augmentez la valeur des inodes pour le volume. Si la valeur des inodes est déjà à la valeur maximale, divisez le volume en deux volumes ou plus, car le système de fichiers a dépassé la taille maximale. 2. Utilisez FlexGroup car il permet de prendre en charge des systèmes de fichiers volumineux.… Si le seuil d’avertissement est dépassé, prévoyez de prendre les mesures immédiates suivantes : 1. Augmentez la valeur des inodes pour le volume. Si la valeur des inodes est déjà au maximum, divisez le volume en deux volumes ou plus, car le système de fichiers a dépassé la taille maximale. 2. Utilisez FlexGroup car il permet de prendre en charge des systèmes de fichiers volumineux

Volume Latence élevée	CRITIQUE	Les volumes sont des objets qui servent le trafic d'E/S souvent généré par des applications sensibles aux performances, notamment les applications DevOps, les répertoires personnels et les bases de données. Des latences de volume élevées signifient que les applications elles-mêmes peuvent en souffrir et être incapables d'accomplir leurs tâches. La surveillance des latences de volume est essentielle pour maintenir des performances cohérentes des applications. Les latences suivantes sont attendues en fonction du type de support : SSD jusqu'à 1 à 2 millisecondes ; SAS jusqu'à 8 à 10 millisecondes et disque dur SATA 17 à 20 millisecondes.	Si le seuil critique est dépassé, envisagez de suivre les actions immédiates pour minimiser les interruptions de service : si une politique de qualité de service (QoS) est attribuée au volume, évaluez ses seuils de limite au cas où ils entraîneraient une limitation de la charge de travail du volume. Si le seuil d'avertissement est dépassé, envisagez les actions immédiates suivantes : 1. Si l'agrégat connaît également une utilisation élevée, déplacez le volume vers un autre agrégat. 2. Si une politique QoS est attribuée au volume, évaluez ses seuils de limite au cas où ils entraîneraient une limitation de la charge de travail du volume. 3. Si le nœud subit également une utilisation élevée, déplacez le volume vers un autre nœud ou réduisez la charge de travail totale du nœud.
Nom du moniteur	Gravité	Description du moniteur	Action corrective

Nœud à latence élevée	AVERTISSEMENT / CRITIQUE	La latence du nœud a atteint des niveaux où elle pourrait affecter les performances des applications sur le nœud. Une latence de nœud plus faible garantit des performances constantes des applications. Les latences attendues en fonction du type de support sont : SSD jusqu'à 1 à 2 millisecondes ; SAS jusqu'à 8 à 10 millisecondes et HDD SATA 17 à 20 millisecondes.	Si le seuil critique est dépassé, des mesures immédiates doivent être prises pour minimiser les interruptions de service : 1. Suspendre les tâches planifiées, les instantanés ou la réplication SnapMirror 2. Réduisez la demande de charges de travail de moindre priorité via des limites de QoS 3. Désactiver les charges de travail non essentielles Envisagez des actions immédiates lorsque le seuil d'avertissement est dépassé : 1. Déplacer une ou plusieurs charges de travail vers un autre emplacement de stockage 2. Réduisez la demande de charges de travail de moindre priorité via des limites de QoS 3. Ajoutez davantage de nœuds de stockage (AFF) ou d'étagères de disques (FAS) et redistribuez les charges de travail 4. Modifier les caractéristiques de la charge de travail (taille des blocs, mise en cache des applications, etc.)

Limite de performance du nœud	AVERTISSEMENT / CRITIQUE	L'utilisation des performances du nœud a atteint des niveaux où elle pourrait affecter les performances des E/S et des applications prises en charge par le nœud. Une faible utilisation des performances des nœuds garantit des performances constantes des applications.	Des mesures immédiates doivent être prises pour minimiser les interruptions de service si le seuil critique est dépassé : 1. Suspendre les tâches planifiées, les instantanés ou la réplication SnapMirror 2. Réduisez la demande de charges de travail de moindre priorité via des limites de QoS 3. Désactiver les charges de travail non essentielles Envisagez les actions suivantes si le seuil d'avertissement est dépassé : 1. Déplacer une ou plusieurs charges de travail vers un autre emplacement de stockage 2. Réduisez la demande de charges de travail de moindre priorité via des limites de QoS 3. Ajoutez davantage de nœuds de stockage (AFF) ou d'étagères de disques (FAS) et redistribuez les charges de travail 4. Modifier les caractéristiques de la charge de travail (taille des blocs, mise en cache des applications, etc.)

Machine virtuelle de stockage à latence élevée	AVERTISSEMENT / CRITIQUE	La latence de la machine virtuelle de stockage (SVM) a atteint des niveaux où elle pourrait affecter les performances des applications sur la machine virtuelle de stockage. La faible latence des machines virtuelles de stockage garantit des performances constantes des applications. Les latences attendues en fonction du type de support sont : SSD jusqu'à 1 à 2 millisecondes ; SAS jusqu'à 8 à 10 millisecondes et HDD SATA 17 à 20 millisecondes.	Si le seuil critique est dépassé, évaluez immédiatement les limites de seuil pour les volumes de la machine virtuelle de stockage avec une politique QoS attribuée, afin de vérifier si elles entraînent une limitation des charges de travail du volume. Envisagez les actions immédiates suivantes lorsque le seuil d'avertissement est dépassé : 1. Si l'agrégat connaît également une utilisation élevée, déplacez certains volumes de la machine virtuelle de stockage vers un autre agrégat. 2. Pour les volumes de la machine virtuelle de stockage avec une politique QoS attribuée, évaluez les limites de seuil si elles entraînent une limitation des charges de travail du volume 3. Si le nœud connaît une utilisation élevée, déplacez certains volumes de la machine virtuelle de stockage vers un autre nœud ou réduisez la charge de travail totale du nœud.
Limite stricte des fichiers de quotas utilisateur	CRITIQUE	Le nombre de fichiers créés dans le volume a atteint la limite critique et des fichiers supplémentaires ne peuvent pas être créés. La surveillance du nombre de fichiers stockés garantit que l'utilisateur reçoit un service de données ininterrompu.	Des mesures immédiates sont nécessaires pour minimiser les interruptions de service si le seuil critique est dépassé.…Envisagez de prendre les mesures suivantes : 1. Augmenter le quota de nombre de fichiers pour l'utilisateur spécifique 2. Supprimez les fichiers indésirables pour réduire la pression sur le quota de fichiers pour l'utilisateur spécifique

Limite souple des fichiers de quotas utilisateur	AVERTISSEMENT	Le nombre de fichiers créés dans le volume a atteint la limite du quota et est proche de la limite critique. Vous ne pouvez pas créer de fichiers supplémentaires si le quota atteint la limite critique. La surveillance du nombre de fichiers stockés par un utilisateur garantit que l'utilisateur reçoit un service de données ininterrompu.	Envisagez des actions immédiates si le seuil d'alerte est dépassé : 1. Augmenter le quota de nombre de fichiers pour le quota utilisateur spécifique 2. Supprimez les fichiers indésirables pour réduire la pression sur le quota de fichiers pour l'utilisateur spécifique

Taux d’échec du cache de volume	AVERTISSEMENT / CRITIQUE	Le ratio de manque de cache de volume est le pourcentage de demandes de lecture provenant des applications clientes qui sont renvoyées depuis le disque au lieu d’être renvoyées depuis le cache. Cela signifie que le volume a atteint le seuil défini.	Si le seuil critique est dépassé, des mesures immédiates doivent être prises pour minimiser les interruptions de service : 1. Déplacez certaines charges de travail hors du nœud du volume pour réduire la charge d’E/S 2. S’il n’est pas déjà présent sur le nœud du volume, augmentez le cache WAFL en achetant et en ajoutant un Flash Cache 3. Réduisez la demande de charges de travail de priorité inférieure sur le même nœud via des limites de QoS. Envisagez des actions immédiates lorsque le seuil d’avertissement est dépassé : 1. Déplacez certaines charges de travail hors du nœud du volume pour réduire la charge d’E/S 2. S’il n’est pas déjà présent sur le nœud du volume, augmentez le cache WAFL en achetant et en ajoutant un Flash Cache 3. Réduisez la demande de charges de travail de priorité inférieure sur le même nœud via des limites QoS 4. Modifier les caractéristiques de la charge de travail (taille des blocs, mise en cache des applications, etc.)

Surengagement de quota de volume Qtree	AVERTISSEMENT / CRITIQUE	Volume Qtree Quota Overcommit spécifie le pourcentage auquel un volume est considéré comme surengagé par les quotas qtree. Le seuil défini pour le quota qtree est atteint pour le volume. La surveillance du dépassement de quota du volume qtree garantit que l'utilisateur reçoit un service de données ininterrompu.	Si le seuil critique est dépassé, des mesures immédiates doivent être prises pour minimiser les interruptions de service : 1. Augmenter l'espace du volume 2. Supprimer les données indésirables Lorsque le seuil d'avertissement est dépassé, envisagez d'augmenter l'espace du volume.

Retour en haut

Moniteurs de journaux

Nom du moniteur	Gravité	Description	Action corrective
Informations d'identification AWS non initialisées	INFO	Cet événement se produit lorsqu'un module tente d'accéder aux informations d'identification basées sur les rôles Amazon Web Services (AWS) Identity and Access Management (IAM) à partir du thread d'informations d'identification cloud avant leur initialisation.	Attendez que le thread d'informations d'identification cloud, ainsi que le système, terminent l'initialisation.

Niveau Cloud inaccessible	CRITIQUE	Un nœud de stockage ne peut pas se connecter à l'API du magasin d'objets Cloud Tier. Certaines données seront inaccessibles.	Si vous utilisez des produits sur site, effectuez les actions correctives suivantes : …Vérifiez que votre LIF intercluster est en ligne et fonctionnel à l'aide de la commande « network interface show ». …Vérifiez la connectivité réseau au serveur de magasin d'objets à l'aide de la commande « ping » sur le LIF intercluster du nœud de destination. …Assurez-vous des points suivants : …La configuration de votre magasin d'objets n'a pas changé. …Les informations de connexion et de connectivité sont toujours valides. …Contactez le support technique NetApp si le problème persiste. Si vous utilisez Cloud Volumes ONTAP, effectuez les actions correctives suivantes : …Assurez-vous que la configuration de votre magasin d'objets n'a pas changé.… Assurez-vous que les informations de connexion et de connectivité sont toujours valides. Contactez le support technique NetApp si le problème persiste.
Disque hors service	INFO	Cet événement se produit lorsqu'un disque est retiré du service parce qu'il a été marqué comme défectueux, est en cours de nettoyage ou est entré dans le centre de maintenance.	Aucun.

FlexGroup Constituent Full	CRITIQUE	Un constituant d'un volume FlexGroup est plein, ce qui peut entraîner une interruption potentielle du service. Vous pouvez toujours créer ou développer des fichiers sur le volume FlexGroup . Cependant, aucun des fichiers stockés sur le constituant ne peut être modifié. Par conséquent, vous risquez de voir des erreurs aléatoires de manque d'espace lorsque vous essayez d'effectuer des opérations d'écriture sur le volume FlexGroup .	Il est recommandé d'ajouter de la capacité au volume FlexGroup en utilisant la commande « volume modify -files +X ». Vous pouvez également supprimer les fichiers du volume FlexGroup . Il est toutefois difficile de déterminer quels dossiers ont atterri chez le mandant.
Le constituant de Flexgroup est presque plein	AVERTISSEMENT	Un constituant d'un volume FlexGroup est presque à court d'espace, ce qui peut entraîner une interruption potentielle du service. Les fichiers peuvent être créés et développés. Cependant, si le constituant manque d'espace, vous ne pourrez peut-être pas ajouter ou modifier les fichiers sur le constituant.	Il est recommandé d'ajouter de la capacité au volume FlexGroup en utilisant la commande « volume modify -files +X ». Vous pouvez également supprimer les fichiers du volume FlexGroup . Il est toutefois difficile de déterminer quels dossiers ont atterri chez le mandant.
Le constituant de FlexGroup est presque à court d'inodes	AVERTISSEMENT	Un constituant d'un volume FlexGroup est presque à court d'inodes, ce qui peut entraîner une interruption potentielle du service. Le constituant reçoit moins de demandes de création que la moyenne. Cela peut avoir un impact sur les performances globales du volume FlexGroup , car les demandes sont acheminées vers les composants avec plus d'inodes.	Il est recommandé d'ajouter de la capacité au volume FlexGroup en utilisant la commande « volume modify -files +X ». Vous pouvez également supprimer les fichiers du volume FlexGroup . Il est toutefois difficile de déterminer quels dossiers ont atterri chez le mandant.

Constituant FlexGroup hors des inodes	CRITIQUE	Un constituant d'un volume FlexGroup est à court d'inodes, ce qui peut entraîner une interruption potentielle du service. Vous ne pouvez pas créer de nouveaux fichiers sur ce constituant. Cela pourrait conduire à une distribution globalement déséquilibrée du contenu sur le volume FlexGroup .	Il est recommandé d'ajouter de la capacité au volume FlexGroup en utilisant la commande « volume modify -files +X ». Vous pouvez également supprimer les fichiers du volume FlexGroup . Il est toutefois difficile de déterminer quels dossiers ont atterri chez le mandant.
LUN hors ligne	INFO	Cet événement se produit lorsqu'un LUN est mis hors ligne manuellement.	Remettez le LUN en ligne.
Panne du ventilateur de l'unité principale	AVERTISSEMENT	Un ou plusieurs ventilateurs de l'unité principale sont en panne. Le système reste opérationnel.…Cependant , si la condition persiste trop longtemps, la surchauffe peut déclencher un arrêt automatique.	Réinstallez les ventilateurs défectueux. Si l'erreur persiste, remplacez-les.
Ventilateur de l'unité principale en état d'avertissement	INFO	Cet événement se produit lorsqu'un ou plusieurs ventilateurs de l'unité principale sont dans un état d'avertissement.	Remplacez les ventilateurs indiqués pour éviter la surchauffe.

Batterie NVRAM faible	AVERTISSEMENT	La capacité de la batterie NVRAM est extrêmement faible. Il peut y avoir une perte de données potentielle si la batterie est déchargée. Votre système génère et transmet un message AutoSupport ou « appel à domicile » au support technique NetApp et aux destinations configurées s'il est configuré pour le faire. La livraison réussie d'un message AutoSupport améliore considérablement la détermination et la résolution des problèmes.	Effectuez les actions correctives suivantes :…Affichez l'état actuel de la batterie, sa capacité et son état de charge à l'aide de la commande « system node environment sensors show »….Si la batterie a été remplacée récemment ou si le système n'a pas été opérationnel pendant une période prolongée, surveillez la batterie pour vérifier qu'elle se charge correctement.…Contactez le support technique NetApp si l'autonomie de la batterie continue de diminuer en dessous des niveaux critiques et que le système de stockage s'arrête automatiquement.
Processeur de service non configuré	AVERTISSEMENT	Cet événement se produit chaque semaine pour vous rappeler de configurer le processeur de service (SP). Le SP est un périphérique physique intégré à votre système pour fournir des capacités d'accès à distance et de gestion à distance. Vous devez configurer le SP pour utiliser toutes ses fonctionnalités.	Effectuez les actions correctives suivantes :…Configurez le SP à l'aide de la commande « system service-processor network modify ».…Vous pouvez également obtenir l'adresse MAC du SP à l'aide de la commande « system service-processor network show ».…Vérifiez la configuration réseau du SP à l'aide de la commande « system service-processor network show ».…Vérifiez que le SP peut envoyer un e-mail AutoSupport à l'aide de la commande « system service-processor autosupport invoke ». REMARQUE : les hôtes et les destinataires de messagerie AutoSupport doivent être configurés dans ONTAP avant d'émettre cette commande.

Processeur de service hors ligne	CRITIQUE	ONTAP ne reçoit plus de pulsations du processeur de service (SP), même si toutes les actions de récupération du SP ont été effectuées. ONTAP ne peut pas surveiller l'état du matériel sans le SP… Le système s'arrêtera pour éviter tout dommage matériel et toute perte de données. Configurez une alerte panique pour être averti immédiatement si le SP se déconnecte.	Redémarrez le système en effectuant les actions suivantes :…Retirez le contrôleur du châssis.…Remettez le contrôleur en place.…Rallumez le contrôleur.…Si le problème persiste, remplacez le module du contrôleur.
Les ventilateurs d'étagère sont en panne	CRITIQUE	Le ventilateur de refroidissement ou le module de ventilateur indiqué de l'étagère est en panne. Il est possible que les disques de l'étagère ne reçoivent pas suffisamment de flux d'air de refroidissement, ce qui peut entraîner une panne du disque.	Effectuez les actions correctives suivantes :…Vérifiez que le module du ventilateur est bien en place et fixé. REMARQUE : le ventilateur est intégré au module d'alimentation de certaines étagères de disques. Si le problème persiste, remplacez le module de ventilateur. Si le problème persiste, contactez le support technique NetApp pour obtenir de l'aide.
Le système ne peut pas fonctionner en raison d'une panne du ventilateur de l'unité principale	CRITIQUE	Un ou plusieurs ventilateurs de l'unité principale sont tombés en panne, perturbant le fonctionnement du système. Cela pourrait entraîner une perte potentielle de données.	Remplacez les ventilateurs défectueux.
Disques non attribués	INFO	Le système possède des disques non attribués : la capacité est gaspillée et votre système peut être soumis à une mauvaise configuration ou à une modification partielle de la configuration.	Effectuez les actions correctives suivantes :…Déterminez quels disques ne sont pas attribués à l'aide de la commande « disk show -n ».…Attribuez les disques à un système à l'aide de la commande « disk assign ».

Serveur antivirus occupé	AVERTISSEMENT	Le serveur antivirus est trop occupé pour accepter de nouvelles demandes d'analyse.	Si ce message apparaît fréquemment, assurez-vous qu'il existe suffisamment de serveurs antivirus pour gérer la charge d'analyse antivirus générée par le SVM.
Les informations d'identification AWS pour le rôle IAM ont expiré	CRITIQUE	Cloud Volume ONTAP est devenu inaccessible. Les informations d'identification basées sur les rôles de gestion des identités et des accès (IAM) ont expiré. Les informations d'identification sont acquises auprès du serveur de métadonnées Amazon Web Services (AWS) à l'aide du rôle IAM et sont utilisées pour signer les demandes d'API à Amazon Simple Storage Service (Amazon S3).	Procédez comme suit :…Connectez-vous à la console de gestion AWS EC2.…Accédez à la page Instances.…Recherchez l'instance pour le déploiement Cloud Volumes ONTAP et vérifiez son état.…Vérifiez que le rôle AWS IAM associé à l'instance est valide et que les privilèges appropriés lui ont été accordés.
Informations d'identification AWS pour le rôle IAM introuvables	CRITIQUE	Le thread d'informations d'identification cloud ne peut pas acquérir les informations d'identification basées sur les rôles Amazon Web Services (AWS) Identity and Access Management (IAM) à partir du serveur de métadonnées AWS. Les informations d'identification sont utilisées pour signer les demandes d'API à Amazon Simple Storage Service (Amazon S3). Cloud Volume ONTAP est devenu inaccessible.…	Procédez comme suit :…Connectez-vous à la console de gestion AWS EC2.…Accédez à la page Instances.…Recherchez l'instance pour le déploiement Cloud Volumes ONTAP et vérifiez son état.…Vérifiez que le rôle AWS IAM associé à l'instance est valide et que les privilèges appropriés lui ont été accordés.

Les informations d'identification AWS pour le rôle IAM ne sont pas valides	CRITIQUE	Les informations d'identification basées sur les rôles de gestion des identités et des accès (IAM) ne sont pas valides. Les informations d'identification sont acquises auprès du serveur de métadonnées Amazon Web Services (AWS) à l'aide du rôle IAM et sont utilisées pour signer les demandes d'API à Amazon Simple Storage Service (Amazon S3). Cloud Volume ONTAP est devenu inaccessible.	Procédez comme suit :…Connectez-vous à la console de gestion AWS EC2.…Accédez à la page Instances.…Recherchez l'instance pour le déploiement Cloud Volumes ONTAP et vérifiez son état.…Vérifiez que le rôle AWS IAM associé à l'instance est valide et que les privilèges appropriés lui ont été accordés.
Rôle AWS IAM introuvable	CRITIQUE	Le thread des rôles de gestion des identités et des accès (IAM) ne trouve pas de rôle IAM Amazon Web Services (AWS) sur le serveur de métadonnées AWS. Le rôle IAM est requis pour acquérir les informations d'identification basées sur les rôles utilisées pour signer les demandes d'API à Amazon Simple Storage Service (Amazon S3). Cloud Volume ONTAP est devenu inaccessible.…	Procédez comme suit :…Connectez-vous à la console de gestion AWS EC2.…Accédez à la page Instances.…Recherchez l'instance pour le déploiement Cloud Volumes ONTAP et vérifiez son état.…Vérifiez que le rôle AWS IAM associé à l'instance est valide.
Rôle AWS IAM non valide	CRITIQUE	Le rôle Amazon Web Services (AWS) Identity and Access Management (IAM) sur le serveur de métadonnées AWS n'est pas valide. Le Cloud Volume ONTAP est devenu inaccessible.…	Procédez comme suit :…Connectez-vous à la console de gestion AWS EC2.…Accédez à la page Instances.…Recherchez l'instance pour le déploiement Cloud Volumes ONTAP et vérifiez son état.…Vérifiez que le rôle AWS IAM associé à l'instance est valide et que les privilèges appropriés lui ont été accordés.

Échec de la connexion au serveur de métadonnées AWS	CRITIQUE	Le thread des rôles de gestion des identités et des accès (IAM) ne peut pas établir de lien de communication avec le serveur de métadonnées Amazon Web Services (AWS). Une communication doit être établie pour acquérir les informations d'identification basées sur les rôles AWS IAM nécessaires utilisées pour signer les demandes d'API à Amazon Simple Storage Service (Amazon S3). Cloud Volume ONTAP est devenu inaccessible.…	Procédez comme suit :…Connectez-vous à la console de gestion AWS EC2.…Accédez à la page Instances.…Recherchez l'instance pour le déploiement Cloud Volumes ONTAP et vérifiez son état.…
La limite d'utilisation de l'espace FabricPool est presque atteinte	AVERTISSEMENT	L'utilisation totale de l'espace FabricPool à l'échelle du cluster des magasins d'objets provenant de fournisseurs sous licence de capacité a presque atteint la limite sous licence.	Effectuez les actions correctives suivantes :…Vérifiez le pourcentage de la capacité sous licence utilisée par chaque niveau de stockage FabricPool à l'aide de la commande « storage aggregate object-store show-space ».…Supprimez les copies Snapshot des volumes avec la stratégie de hiérarchisation « snapshot » ou « backup » à l'aide de la commande « volume snapshot delete » pour libérer de l'espace.…Installez une nouvelle licence sur le cluster pour augmenter la capacité sous licence.

Limite d’utilisation de l’espace FabricPool atteinte	CRITIQUE	L’utilisation totale de l’espace FabricPool à l’échelle du cluster des magasins d’objets provenant de fournisseurs sous licence de capacité a atteint la limite de licence.	Effectuez les actions correctives suivantes :…Vérifiez le pourcentage de la capacité sous licence utilisée par chaque niveau de stockage FabricPool à l’aide de la commande « storage aggregate object-store show-space »….Supprimez les copies Snapshot des volumes avec la stratégie de hiérarchisation « snapshot » ou « backup » à l’aide de la commande « volume snapshot delete » pour libérer de l’espace.…Installez une nouvelle licence sur le cluster pour augmenter la capacité sous licence.

Échec de la restitution des agrégats	CRITIQUE	Cet événement se produit lors de la migration d'un agrégat dans le cadre d'un basculement de stockage (SFO), lorsque le nœud de destination ne peut pas atteindre les magasins d'objets.	Effectuez les actions correctives suivantes :… Vérifiez que votre LIF intercluster est en ligne et fonctionnel à l'aide de la commande « network interface show »…. Vérifiez la connectivité réseau au serveur de magasin d'objets à l'aide de la commande « ping » sur le LIF intercluster du nœud de destination. …Vérifiez que la configuration de votre magasin d'objets n'a pas changé et que les informations de connexion et de connectivité sont toujours exactes à l'aide de la commande « aggregate object-store config show »….Vous pouvez également remplacer l'erreur en spécifiant false pour le paramètre « require-partner-waiting » de la commande giveback.…Contactez le support technique NetApp pour obtenir plus d'informations ou une assistance.

Interconnexion HA en panne	AVERTISSEMENT	L'interconnexion haute disponibilité (HA) est en panne. Risque d'interruption de service lorsque le basculement n'est pas disponible.	Les actions correctives dépendent du nombre et du type de liens d'interconnexion HA pris en charge par la plate-forme, ainsi que de la raison pour laquelle l'interconnexion est en panne. …Si les liaisons sont interrompues :…Vérifiez que les deux contrôleurs de la paire HA sont opérationnels.…Pour les liaisons connectées en externe, assurez-vous que les câbles d'interconnexion sont correctement connectés et que les modules enfichables à petit facteur de forme (SFP), le cas échéant, sont correctement installés sur les deux contrôleurs.…Pour les liaisons connectées en interne, désactivez et réactivez les liaisons, l'une après l'autre, en utilisant les commandes « ic link off » et « ic link on ». …Si les liens sont désactivés, activez-les en utilisant la commande « ic link on ». …Si un homologue n'est pas connecté, désactivez et réactivez les liens, l'un après l'autre, en utilisant les commandes « ic link off » et « ic link on ».…Contactez le support technique NetApp si le problème persiste.

Nombre maximal de sessions par utilisateur dépassé	AVERTISSEMENT	Vous avez dépassé le nombre maximal de sessions autorisées par utilisateur sur une connexion TCP. Toute demande d'établissement d'une session sera refusée jusqu'à ce que certaines sessions soient libérées. …	Effectuez les actions correctives suivantes : …Inspectez toutes les applications qui s'exécutent sur le client et fermez celles qui ne fonctionnent pas correctement. …Redémarrez le client. …Vérifiez si le problème est causé par une application nouvelle ou existante : …Si l'application est nouvelle, définissez un seuil plus élevé pour le client en utilisant la commande « cifs option modify -max -opens-same-file-per -tree ». Dans certains cas, les clients fonctionnent comme prévu, mais nécessitent un seuil plus élevé. Vous devez disposer de privilèges avancés pour définir un seuil plus élevé pour le client. …Si le problème est causé par une application existante, il peut y avoir un problème avec le client. Contactez le support technique NetApp pour plus d'informations ou d'assistance.

Nombre maximal de fois par fichier ouvert dépassé	AVERTISSEMENT	Vous avez dépassé le nombre maximal de fois que vous pouvez ouvrir le fichier via une connexion TCP. Toute demande d'ouverture de ce fichier sera refusée jusqu'à ce que vous fermiez certaines instances ouvertes du fichier. Cela indique généralement un comportement anormal de l'application.	Effectuez les actions correctives suivantes :…Inspectez les applications qui s'exécutent sur le client à l'aide de cette connexion TCP. Le client peut fonctionner de manière incorrecte en raison de l'application qui s'exécute dessus. Redémarrez le client. Vérifiez si le problème est causé par une application nouvelle ou existante : Si l'application est nouvelle, définissez un seuil plus élevé pour le client en utilisant la commande « cifs option modify -max -opens-same-file-per -tree ». Dans certains cas, les clients fonctionnent comme prévu, mais nécessitent un seuil plus élevé. Vous devez disposer de privilèges avancés pour définir un seuil plus élevé pour le client. …Si le problème est causé par une application existante, il peut y avoir un problème avec le client. Contactez le support technique NetApp pour plus d'informations ou d'assistance.

Conflit de nom NetBIOS	CRITIQUE	Le service de noms NetBIOS a reçu une réponse négative à une demande d'enregistrement de nom, provenant d'une machine distante. Cela est généralement dû à un conflit dans le nom NetBIOS ou dans un alias. Par conséquent, les clients risquent de ne pas pouvoir accéder aux données ou de se connecter au bon nœud de service de données dans le cluster.	Effectuez l'une des actions correctives suivantes :…En cas de conflit dans le nom NetBIOS ou dans un alias, effectuez l'une des opérations suivantes :…Supprimez l'alias NetBIOS en double à l'aide de la commande « vserver cifs delete -aliases alias -vserver vserver »….Renommez un alias NetBIOS en supprimant le nom en double et en ajoutant un alias avec un nouveau nom à l'aide de la commande « vserver cifs create -aliases alias -vserver vserver ». …S'il n'y a pas d'alias configuré et qu'il y a un conflit dans le nom NetBIOS, renommez le serveur CIFS en utilisant les commandes « vserver cifs delete -vserver vserver » et « vserver cifs create -cifs-server netbiosname ». REMARQUE : la suppression d'un serveur CIFS peut rendre les données inaccessibles. …Supprimez le nom NetBIOS ou renommez le NetBIOS sur la machine distante.
Pool de stockage NFSv4 épuisé	CRITIQUE	Un pool de stockage NFSv4 a été épuisé.	Si le serveur NFS ne répond pas pendant plus de 10 minutes après cet événement, contactez le support technique NetApp .

Aucun moteur d'analyse enregistré	CRITIQUE	Le connecteur antivirus a notifié à ONTAP qu'il ne dispose pas d'un moteur d'analyse enregistré. Cela peut entraîner l'indisponibilité des données si l'option « scan-mandatory » est activée.	Effectuez les actions correctives suivantes :…Assurez-vous que le logiciel du moteur d'analyse installé sur le serveur antivirus est compatible avec ONTAP.…Assurez-vous que le logiciel du moteur d'analyse est en cours d'exécution et configuré pour se connecter au connecteur antivirus via une boucle de rappel locale.
Pas de connexion Vscan	CRITIQUE	ONTAP n'a pas de connexion Vscan pour répondre aux demandes d'analyse antivirus. Cela peut entraîner l'indisponibilité des données si l'option « scan-mandatory » est activée.	Assurez-vous que le pool de scanners est correctement configuré et que les serveurs antivirus sont actifs et connectés à ONTAP.
Espace de volume racine du nœud faible	CRITIQUE	Le système a détecté que le volume racine est dangereusement bas en termes d'espace. Le nœud n'est pas entièrement opérationnel. Les LIF de données peuvent avoir basculé au sein du cluster, ce qui limite l'accès NFS et CIFS sur le nœud. La capacité administrative est limitée aux procédures de récupération locales permettant au nœud de libérer de l'espace sur le volume racine.	Effectuez les actions correctives suivantes :… Libérez de l'espace sur le volume racine en supprimant les anciennes copies Snapshot, en supprimant les fichiers dont vous n'avez plus besoin du répertoire /mroot ou en augmentant la capacité du volume racine.… Redémarrez le contrôleur.… Contactez le support technique NetApp pour plus d'informations ou d'assistance.
Partage administrateur inexistant	CRITIQUE	Problème Vscan : un client a tenté de se connecter à un partage ONTAP_ADMIN$ inexistant.	Assurez-vous que Vscan est activé pour l'ID SVM mentionné. L'activation de Vscan sur un SVM entraîne la création automatique du partage ONTAP_ADMIN$ pour le SVM.

Espace de noms NVMe insuffisant	CRITIQUE	Un espace de noms NVMe a été mis hors ligne en raison d'une erreur d'écriture causée par un manque d'espace.	Ajoutez de l'espace au volume, puis mettez l'espace de noms NVMe en ligne à l'aide de la commande « vserver nvme namespace modify ».
Période de grâce NVMe-oF active	AVERTISSEMENT	Cet événement se produit quotidiennement lorsque le protocole NVMe over Fabrics (NVMe-oF) est utilisé et que la période de grâce de la licence est active. La fonctionnalité NVMe-oF nécessite une licence après l'expiration de la période de grâce de la licence. La fonctionnalité NVMe-oF est désactivée lorsque la période de grâce de la licence est terminée.	Contactez votre représentant commercial pour obtenir une licence NVMe-oF et l'ajouter au cluster, ou supprimez toutes les instances de configuration NVMe-oF du cluster.
Période de grâce NVMe-oF expirée	AVERTISSEMENT	La période de grâce de la licence NVMe over Fabrics (NVMe-oF) est terminée et la fonctionnalité NVMe-oF est désactivée.	Contactez votre représentant commercial pour obtenir une licence NVMe-oF et l'ajouter au cluster.
Début de la période de grâce NVMe-oF	AVERTISSEMENT	La configuration NVMe over Fabrics (NVMe-oF) a été détectée lors de la mise à niveau vers le logiciel ONTAP 9.5. La fonctionnalité NVMe-oF nécessite une licence après l'expiration de la période de grâce de la licence.	Contactez votre représentant commercial pour obtenir une licence NVMe-oF et l'ajouter au cluster.
Hôte du magasin d'objets non résoluble	CRITIQUE	Le nom d'hôte du serveur de magasin d'objets ne peut pas être résolu en une adresse IP. Le client du magasin d'objets ne peut pas communiquer avec le serveur du magasin d'objets sans résoudre une adresse IP. Par conséquent, les données peuvent être inaccessibles.	Vérifiez la configuration DNS pour vérifier que le nom d'hôte est correctement configuré avec une adresse IP.

LIF intercluster du magasin d'objets en panne	CRITIQUE	Le client du magasin d'objets ne trouve pas de LIF opérationnel pour communiquer avec le serveur du magasin d'objets. Le nœud n'autorisera pas le trafic client du magasin d'objets tant que le LIF intercluster ne sera pas opérationnel. Par conséquent, les données peuvent être inaccessibles.	Effectuez les actions correctives suivantes :…Vérifiez l'état du LIF intercluster à l'aide de la commande « network interface show -role intercluster »….Vérifiez que le LIF intercluster est configuré correctement et opérationnel.…Si un LIF intercluster n'est pas configuré, ajoutez-le à l'aide de la commande « network interface create -role intercluster ».
Non-concordance des signatures du magasin d'objets	CRITIQUE	La signature de la demande envoyée au serveur de magasin d'objets ne correspond pas à la signature calculée par le client. Par conséquent, les données peuvent être inaccessibles.	Vérifiez que la clé d'accès secrète est correctement configurée. S'il est configuré correctement, contactez le support technique NetApp pour obtenir de l'aide.

Délai d’expiration de READDIR	CRITIQUE	Une opération de fichier READDIR a dépassé le délai d’exécution autorisé dans WAFL. Cela peut être dû à des répertoires très volumineux ou peu nombreux. Des mesures correctives sont recommandées.	Effectuez les actions correctives suivantes :…Recherchez des informations spécifiques aux répertoires récents dont les opérations de fichier READDIR ont expiré en utilisant la commande CLI nodeshell de privilège « diag » suivante : wafl readdir notice show.…Vérifiez si les répertoires sont indiqués comme clairsemés ou non :…Si un répertoire est indiqué comme clairsemé, il est recommandé de copier le contenu du répertoire dans un nouveau répertoire pour supprimer la clairsemée du fichier de répertoire. …Si un répertoire n’est pas indiqué comme étant clairsemé et que le répertoire est volumineux, il est recommandé de réduire la taille du fichier de répertoire en réduisant le nombre d’entrées de fichier dans le répertoire.

Échec de la relocalisation des agrégats	CRITIQUE	Cet événement se produit lors du déplacement d'un agrégat, lorsque le nœud de destination ne peut pas atteindre les magasins d'objets.	Effectuez les actions correctives suivantes :… Vérifiez que votre LIF intercluster est en ligne et fonctionnel à l'aide de la commande « network interface show »…. Vérifiez la connectivité réseau au serveur de magasin d'objets à l'aide de la commande « ping » sur le LIF intercluster du nœud de destination. …Vérifiez que la configuration de votre magasin d'objets n'a pas changé et que les informations de connexion et de connectivité sont toujours exactes à l'aide de la commande « aggregate object-store config show »….Vous pouvez également contourner l'erreur en utilisant le paramètre « override-destination-checks » de la commande de relocation.…Contactez le support technique NetApp pour obtenir plus d'informations ou une assistance.
Échec de la copie fantôme	CRITIQUE	Une opération de service de sauvegarde et de restauration de Volume Shadow Copy Service (VSS) de Microsoft Server a échoué.	Vérifiez les éléments suivants à l'aide des informations fournies dans le message d'événement :… La configuration de la copie fantôme est-elle activée ?… Les licences appropriées sont-elles installées ? …Sur quels partages l'opération de cliché instantané est-elle effectuée ?…Le nom du partage est-il correct ?…Le chemin du partage existe-t-il ?…Quels sont les états de l'ensemble de clichés instantanés et de ses clichés instantanés ?

Panne d’alimentation du commutateur de stockage	AVERTISSEMENT	Il manque une alimentation dans le commutateur du cluster. La redondance est réduite, le risque de panne en cas de nouvelle panne de courant est réduit.	Effectuez les actions correctives suivantes :… Assurez-vous que le bloc d’alimentation secteur, qui alimente le commutateur de cluster, est sous tension.… Assurez-vous que le cordon d’alimentation est connecté au bloc d’alimentation.… Contactez le support technique NetApp si le problème persiste.
Trop d’authentifications CIFS	AVERTISSEMENT	De nombreuses négociations d’authentification ont eu lieu simultanément. Il y a 256 demandes de nouvelles sessions incomplètes de ce client.	Recherchez pourquoi le client a créé 256 nouvelles demandes de connexion ou plus. Vous devrez peut-être contacter le fournisseur du client ou de l’application pour déterminer pourquoi l’erreur s’est produite.
Accès utilisateur non autorisé au partage administrateur	AVERTISSEMENT	Un client a tenté de se connecter au partage privilégié ONTAP_ADMIN$ même si son utilisateur connecté n’est pas un utilisateur autorisé.	Effectuez les actions correctives suivantes :… Assurez-vous que le nom d’utilisateur et l’adresse IP mentionnés sont configurés dans l’un des pools de scanners Vscan actifs.… Vérifiez la configuration du pool de scanners actuellement actif à l’aide de la commande « vserver vscan scanner pool show-active ».

Virus détecté	AVERTISSEMENT	Un serveur Vscan a signalé une erreur au système de stockage. Cela indique généralement qu'un virus a été détecté. Cependant, d'autres erreurs sur le serveur Vscan peuvent provoquer cet événement.…L'accès client au fichier est refusé. Le serveur Vscan peut, selon ses paramètres et sa configuration, nettoyer le fichier, le mettre en quarantaine ou le supprimer.	Vérifiez le journal du serveur Vscan signalé dans l'événement « syslog » pour voir s'il a réussi à nettoyer, mettre en quarantaine ou supprimer le fichier infecté. Si cela n'est pas possible, un administrateur système devra peut-être supprimer manuellement le fichier.
Volume hors ligne	INFO	Ce message indique qu'un volume est mis hors ligne.	Remettez le volume en ligne.
Volume restreint	INFO	Cet événement indique qu'un volume flexible est rendu restreint.	Remettez le volume en ligne.
L'arrêt de la machine virtuelle de stockage a réussi	INFO	Ce message s'affiche lorsqu'une opération « vserver stop » réussit.	Utilisez la commande « vserver start » pour démarrer l'accès aux données sur une machine virtuelle de stockage.
Panique du nœud	AVERTISSEMENT	Cet événement est émis lorsqu'une panique se produit	Contactez le support client NetApp .

Retour en haut

Moniteurs de journaux anti-ransomware

Nom du moniteur	Gravité	Description	Action corrective
Surveillance anti-ransomware de la machine virtuelle de stockage désactivée	AVERTISSEMENT	La surveillance anti-ransomware pour la VM de stockage est désactivée. Activez l'anti-ransomware pour protéger la machine virtuelle de stockage.	Aucune
Surveillance anti-ransomware des machines virtuelles de stockage activée (mode d'apprentissage)	INFO	La surveillance anti-ransomware pour la VM de stockage est activée en mode apprentissage.	Aucune

Surveillance anti-ransomware du volume activée	INFO	La surveillance anti-ransomware du volume est activée.	Aucune
Surveillance anti-ransomware du volume désactivée	AVERTISSEMENT	La surveillance anti-ransomware du volume est désactivée. Activez l'anti-ransomware pour protéger le volume.	Aucune
Surveillance anti-ransomware du volume activée (mode d'apprentissage)	INFO	La surveillance anti-ransomware du volume est activée en mode apprentissage.	Aucune
Surveillance anti-ransomware du volume interrompue (mode d'apprentissage)	AVERTISSEMENT	La surveillance anti-ransomware du volume est suspendue en mode apprentissage.	Aucune
Surveillance anti-ransomware du volume suspendue	AVERTISSEMENT	La surveillance anti-ransomware du volume est suspendue.	Aucune
Désactivation de la surveillance anti-ransomware du volume	AVERTISSEMENT	La surveillance anti-ransomware du volume est désactivée.	Aucune
Activité de ransomware détectée	CRITIQUE	Pour protéger les données du ransomware détecté, une copie instantanée a été prise et peut être utilisée pour restaurer les données d'origine. Votre système génère et transmet un message AutoSupport ou « appel à domicile » au support technique NetApp et à toutes les destinations configurées. Le message AutoSupport améliore la détermination et la résolution des problèmes.	Reportez-vous au « NOM DU DOCUMENT FINAL » pour prendre des mesures correctives en cas d'activité de ransomware.

Retour en haut

Moniteurs FSx pour NetApp ONTAP

Nom du moniteur	Seuils	Description du moniteur	Action corrective

La capacité du volume FSx est pleine	Avertissement à > 85 %…Critique à > 95 %	La capacité de stockage d'un volume est nécessaire pour stocker les données d'application et de client. Plus les données stockées dans le volume ONTAP sont nombreuses, moins il y a de disponibilité de stockage pour les données futures. Si la capacité de stockage des données dans un volume atteint la capacité de stockage totale, le client peut être incapable de stocker des données en raison d'un manque de capacité de stockage. La surveillance du volume de capacité de stockage utilisé garantit la continuité des services de données.	Des mesures immédiates sont nécessaires pour minimiser les interruptions de service si le seuil critique est dépassé :…1. Envisagez de supprimer les données qui ne sont plus nécessaires pour libérer de l'espace
FSx Volume Latence élevée	Avertissement à > 1 000 µs… Critique à > 2 000 µs	Les volumes sont des objets qui servent le trafic d'E/S souvent généré par des applications sensibles aux performances, notamment les applications DevOps, les répertoires personnels et les bases de données. Des latences de volume élevées signifient que les applications elles-mêmes peuvent en souffrir et être incapables d'accomplir leurs tâches. La surveillance des latences de volume est essentielle pour maintenir des performances cohérentes des applications.	Des mesures immédiates sont nécessaires pour minimiser les interruptions de service si le seuil critique est dépassé :…1. Si une politique QoS est attribuée au volume, évaluez ses seuils de limite au cas où ils entraîneraient une limitation de la charge de travail du volume… Prévoyez de prendre prochainement les mesures suivantes si le seuil d'avertissement est dépassé :…1. Si une politique QoS est attribuée au volume, évaluez ses seuils de limite au cas où ils entraîneraient une limitation de la charge de travail du volume.…2. Si le nœud subit également une utilisation élevée, déplacez le volume vers un autre nœud ou réduisez la charge de travail totale du nœud.

Limite d'inodes de volume FSx	Avertissement à > 85 %…Critique à > 95 %	Les volumes qui stockent des fichiers utilisent des nœuds d'index (inode) pour stocker les métadonnées des fichiers. Lorsqu'un volume épuise son allocation d'inode, aucun fichier supplémentaire ne peut y être ajouté. Une alerte d'avertissement indique qu'une action planifiée doit être entreprise pour augmenter le nombre d'inodes disponibles. Une alerte critique indique que l'épuisement de la limite de fichier est imminent et que des mesures d'urgence doivent être prises pour libérer des inodes afin d'assurer la continuité du service	Des mesures immédiates sont nécessaires pour minimiser les interruptions de service si le seuil critique est dépassé :…1. Envisagez d'augmenter la valeur des inodes pour le volume. Si la valeur des inodes est déjà au maximum, envisagez de diviser le volume en deux volumes ou plus, car le système de fichiers a dépassé la taille maximale… Prévoyez de prendre prochainement les mesures suivantes si le seuil d'avertissement est dépassé :…1. Envisagez d'augmenter la valeur des inodes pour le volume. Si la valeur des inodes est déjà au maximum, envisagez de diviser le volume en deux volumes ou plus, car le système de fichiers a dépassé la taille maximale.
Surcharge de quota Qtree du volume FSx	Avertissement à > 95 %…Critique à > 100 %	Volume Qtree Quota Overcommit spécifie le pourcentage auquel un volume est considéré comme surengagé par les quotas qtree. Le seuil défini pour le quota qtree est atteint pour le volume. La surveillance du dépassement de quota du volume qtree garantit que l'utilisateur reçoit un service de données ininterrompu.	Si le seuil critique est dépassé, des mesures immédiates doivent être prises pour minimiser les interruptions de service : 1. Supprimez les données indésirables… Lorsque le seuil d'avertissement est dépassé, envisagez d'augmenter l'espace du volume.

L’espace de réserve des instantanés FSx est plein	Avertissement à > 90 %…Critique à > 95 %	La capacité de stockage d’un volume est nécessaire pour stocker les données d’application et de client. Une partie de cet espace, appelée espace réservé aux instantanés, est utilisée pour stocker des instantanés qui permettent de protéger les données localement. Plus les données nouvelles et mises à jour sont stockées dans le volume ONTAP , plus la capacité de snapshot est utilisée et moins la capacité de stockage de snapshot sera disponible pour les données nouvelles ou mises à jour futures. Si la capacité des données d’instantané dans un volume atteint l’espace de réserve total d’instantané, le client peut être incapable de stocker de nouvelles données d’instantané et le niveau de protection des données dans le volume peut être réduit. La surveillance de la capacité de snapshot du volume utilisé garantit la continuité des services de données.	Des mesures immédiates sont nécessaires pour minimiser les interruptions de service si le seuil critique est dépassé :…1. Envisagez de configurer des instantanés pour utiliser l’espace de données dans le volume lorsque la réserve d’instantanés est pleine…2. Envisagez de supprimer certains anciens instantanés qui ne sont peut-être plus nécessaires pour libérer de l’espace… Prévoyez de prendre prochainement les mesures suivantes si le seuil d’avertissement est dépassé :…1. Envisagez d’augmenter l’espace de réserve d’instantanés dans le volume pour s’adapter à la croissance…2. Envisagez de configurer des instantanés pour utiliser l’espace de données dans le volume lorsque la réserve d’instantanés est pleine.

Taux d'échec du cache de volume FSx	Avertissement à > 95 %…Critique à > 100 %	Le ratio de manque de cache de volume est le pourcentage de demandes de lecture provenant des applications clientes qui sont renvoyées depuis le disque au lieu d'être renvoyées depuis le cache. Cela signifie que le volume a atteint le seuil défini.	Si le seuil critique est dépassé, des mesures immédiates doivent être prises pour minimiser les interruptions de service : 1. Déplacez certaines charges de travail hors du nœud du volume pour réduire la charge d'E/S 2. Réduisez la demande de charges de travail de priorité inférieure sur le même nœud via des limites de QoS… Envisagez des actions immédiates lorsque le seuil d'avertissement est dépassé : 1. Déplacez certaines charges de travail hors du nœud du volume pour réduire la charge d'E/S 2. Réduisez la demande de charges de travail de priorité inférieure sur le même nœud via des limites QoS 3. Modifier les caractéristiques de la charge de travail (taille des blocs, mise en cache des applications, etc.)

Retour en haut

Moniteurs K8s

Nom du moniteur	Description	Mesures correctives	Gravité/Seuil

Latence de volume persistante élevée	Des latences de volume persistantes élevées signifient que les applications elles-mêmes peuvent en souffrir et être incapables d'accomplir leurs tâches. La surveillance des latences de volume persistantes est essentielle pour maintenir des performances cohérentes des applications. Les latences suivantes sont attendues en fonction du type de support : SSD jusqu'à 1 à 2 millisecondes ; SAS jusqu'à 8 à 10 millisecondes et disque dur SATA 17 à 20 millisecondes.	**Actions immédiates** Si le seuil critique est dépassé, envisagez des actions immédiates pour minimiser les interruptions de service : si une politique de qualité de service (QoS) est attribuée au volume, évaluez ses seuils de limite au cas où ils entraîneraient une limitation de la charge de travail du volume. **Actions à effectuer prochainement** Si le seuil d'avertissement est dépassé, planifiez les actions immédiates suivantes : 1. Si le pool de stockage connaît également une utilisation élevée, déplacez le volume vers un autre pool de stockage. 2. Si une politique QoS est attribuée au volume, évaluez ses seuils de limite au cas où ils entraîneraient une limitation de la charge de travail du volume. 3. Si le contrôleur subit également une utilisation élevée, déplacez le volume vers un autre contrôleur ou réduisez la charge de travail totale du contrôleur.	Avertissement à > 6 000 µs Critique à > 12 000 µs
Saturation élevée de la mémoire du cluster	La saturation de la mémoire allouable du cluster est élevée. La saturation du processeur du cluster est calculée comme la somme de l'utilisation de la mémoire divisée par la somme de la mémoire allouable sur tous les nœuds K8.	Ajouter des nœuds. Corrigez tous les nœuds non planifiés. Ajustez la taille des pods pour libérer de la mémoire sur les nœuds.	Avertissement à > 80 % Critique à > 90 %
Échec de la connexion du POD	Cette alerte se produit lorsqu'une pièce jointe de volume avec POD échoue.		Avertissement

Taux de retransmission élevé	Taux de retransmission TCP élevé	Vérifiez la congestion du réseau - Identifiez les charges de travail qui consomment beaucoup de bande passante réseau. Vérifiez l'utilisation élevée du processeur Pod. Vérifiez les performances du réseau matériel.	Avertissement à > 10 % Critique à > 25 %
Capacité élevée du système de fichiers du nœud	Capacité élevée du système de fichiers du nœud	- Augmentez la taille des disques de nœuds pour garantir qu'il y a suffisamment d'espace pour les fichiers d'application. - Réduire l'utilisation des fichiers d'application.	Avertissement à > 80 % Critique à > 90 %
Gigue élevée du réseau de charge de travail	Gigue TCP élevée (variations élevées de latence/temps de réponse)	Vérifiez la congestion du réseau. Identifiez les charges de travail qui consomment beaucoup de bande passante réseau. Vérifiez l'utilisation élevée du processeur Pod. Vérifier les performances du réseau matériel	Avertissement à > 30 ms Critique à > 50 ms

Débit de volume persistant	Les seuils MBPS sur les volumes persistants peuvent être utilisés pour alerter un administrateur lorsque les volumes persistants dépassent les attentes de performances prédéfinies, ce qui peut avoir un impact sur d'autres volumes persistants. L'activation de ce moniteur générera des alertes adaptées au profil de débit typique des volumes persistants sur SSD. Ce moniteur couvrira tous les volumes persistants de votre locataire. Les valeurs de seuil d'avertissement et de critique peuvent être ajustées en fonction de vos objectifs de surveillance en dupliquant ce moniteur et en définissant des seuils adaptés à votre classe de stockage. Un moniteur dupliqué peut être davantage ciblé sur un sous-ensemble des volumes persistants de votre locataire.	**Actions immédiates** Si le seuil critique est dépassé, planifiez des actions immédiates pour minimiser les interruptions de service : 1. Introduisez les limites QoS MBPS pour le volume. 2. Vérifiez l'application qui pilote la charge de travail sur le volume pour détecter d'éventuelles anomalies. **Actions à effectuer prochainement** Si le seuil d'avertissement est dépassé, prévoyez de prendre les mesures immédiates suivantes : 1. Introduisez les limites QoS MBPS pour le volume. 2. Vérifiez l'application qui pilote la charge de travail sur le volume pour détecter d'éventuelles anomalies.	Avertissement à > 10 000 Mo/s Critique à > 15 000 Mo/s
Conteneur menacé de rupture de stock	Les limites de mémoire du conteneur sont définies trop bas. Le conteneur risque d'être expulsé (Out of Memory Kill).	Augmenter les limites de mémoire du conteneur.	Avertissement à > 95 %
Réduction de la charge de travail	La charge de travail n'a pas de pods sains.		Critique à < 1
Échec de la liaison de la réclamation de volume persistant	Cette alerte se produit lorsqu'une liaison échoue sur un PVC.		Avertissement
Les limites de mémoire de ResourceQuota sont sur le point d'être dépassées	Les limites de mémoire pour l'espace de noms sont sur le point de dépasser ResourceQuota		Avertissement à > 80 % Critique à > 90 %
Demandes de mémoire ResourceQuota sur le point d'être dépassées	Les demandes de mémoire pour l'espace de noms sont sur le point de dépasser ResourceQuota		Avertissement à > 80 % Critique à > 90 %

Échec de la création du nœud	Le nœud n'a pas pu être planifié en raison d'une erreur de configuration.	Consultez le journal des événements Kubernetes pour connaître la cause de l'échec de la configuration.	Primordial
Échec de la récupération du volume persistant	Le volume n'a pas réussi sa récupération automatique.		Avertissement @ > 0 B
Limitation du processeur du conteneur	Les limites du processeur du conteneur sont définies trop bas. Les processus de conteneurs sont ralentis.	Augmenter les limites du processeur du conteneur.	Avertissement à > 95 % Critique à > 98 %
Échec de la suppression de l'équilibreur de charge de service			Avertissement
IOPS de volume persistant	Les seuils IOPS sur les volumes persistants peuvent être utilisés pour alerter un administrateur lorsque les volumes persistants dépassent les attentes de performances prédéfinies. L'activation de ce moniteur générera des alertes adaptées au profil IOPS typique des volumes de persistance. Ce moniteur couvrira tous les volumes persistants de votre locataire. Les valeurs de seuil d'avertissement et de critique peuvent être ajustées en fonction de vos objectifs de surveillance en dupliquant ce moniteur et en définissant des seuils adaptés à votre charge de travail.	**Actions immédiates** Si le seuil critique est dépassé, planifiez des actions immédiates pour minimiser les interruptions de service : 1. Introduisez les limites IOPS QoS pour le volume. 2. Vérifiez l'application qui pilote la charge de travail sur le volume pour détecter d'éventuelles anomalies. **Actions à effectuer prochainement** Si le seuil d'avertissement est dépassé, planifiez les actions immédiates suivantes : 1. Introduisez les limites IOPS QoS pour le volume. 2. Vérifiez l'application qui pilote la charge de travail sur le volume pour détecter d'éventuelles anomalies.	Avertissement à > 20 000 E/S Critique à > 25 000 E/S
Échec de la mise à jour de l'équilibreur de charge de service			Avertissement
Échec du montage du POD	Cette alerte se produit lorsqu'un montage échoue sur un POD.		Avertissement

Pression PID du nœud	Les identifiants de processus disponibles sur le nœud (Linux) sont tombés en dessous d'un seuil d'éviction.	Recherchez et corrigez les pods qui génèrent de nombreux processus et privent le nœud d'ID de processus disponibles. Configurez PodPidsLimit pour protéger votre nœud contre les pods ou les conteneurs qui génèrent trop de processus.	Critique @ > 0
Échec de l'extraction de l'image du pod	Kubernetes n'a pas réussi à extraire l'image du conteneur de pod.	- Assurez-vous que l'image du pod est correctement orthographiée dans la configuration du pod. - Vérifiez que la balise d'image existe dans votre registre. - Vérifiez les informations d'identification du registre d'images. - Vérifiez les problèmes de connectivité du registre. - Vérifiez que vous n'atteignez pas les limites de débit imposées par les fournisseurs de registre public.	Avertissement
Le travail dure trop longtemps	Le travail dure trop longtemps		Avertissement à > 1 h Critique à > 5 h
Mémoire de nœud élevée	L'utilisation de la mémoire du nœud est élevée	Ajouter des nœuds. Corrigez tous les nœuds non planifiés. Ajustez la taille des pods pour libérer de la mémoire sur les nœuds.	Avertissement à > 85 % Critique à > 90 %
Les limites du processeur ResourceQuota sont sur le point d'être dépassées	Les limites du processeur pour l'espace de noms sont sur le point de dépasser ResourceQuota		Avertissement à > 80 % Critique à > 90 %
Boucle de crash de pod arrière	Le Pod s'est écrasé et a tenté de redémarrer plusieurs fois.		Critique @ > 3
CPU du nœud élevé	L'utilisation du processeur du nœud est élevée.	Ajouter des nœuds. Corrigez tous les nœuds non planifiés. Ajustez la taille des pods pour libérer du CPU sur les nœuds.	Avertissement à > 80 % Critique à > 90 %

Latence du réseau de charge de travail RTT élevée	Latence TCP RTT (Round Trip Time) élevée	Vérifiez la congestion du réseau ▒ Identifiez les charges de travail qui consomment beaucoup de bande passante réseau. Vérifiez l'utilisation élevée du processeur Pod. Vérifiez les performances du réseau matériel.	Avertissement à > 150 ms Critique à > 300 ms
Échec du travail	La tâche n'a pas été terminée avec succès en raison d'une panne ou d'un redémarrage du nœud, d'un épuisement des ressources, d'un délai d'expiration de la tâche ou d'un échec de planification du pod.	Vérifiez les journaux d'événements Kubernetes pour connaître les causes d'échec.	Avertissement @ > 1
Volume persistant plein en quelques jours	Le volume persistant manquera d'espace dans quelques jours	-Augmentez la taille du volume pour garantir qu'il y a suffisamment d'espace pour les fichiers d'application. -Réduire la quantité de données stockées dans les applications.	Avertissement à < 8 jours Critique à < 3 jours
Pression de la mémoire des nœuds	Le nœud manque de mémoire. La mémoire disponible a atteint le seuil d'expulsion.	Ajouter des nœuds. Corrigez tous les nœuds non planifiés. Ajustez la taille des pods pour libérer de la mémoire sur les nœuds.	Critique @ > 0
Nœud non prêt	Le nœud n'est pas prêt depuis 5 minutes	Vérifiez que le nœud dispose de suffisamment de ressources CPU, mémoire et disque. Vérifiez la connectivité du réseau du nœud. Vérifiez les journaux d'événements Kubernetes pour connaître les causes d'échec.	Critique à < 1
Capacité de volume persistante élevée	La capacité utilisée par le backend de volume persistant est élevée.	- Augmentez la taille du volume pour garantir qu'il y a suffisamment d'espace pour les fichiers d'application. - Réduire la quantité de données stockées dans les applications.	Avertissement à > 80 % Critique à > 90 %

Échec de la création de l'équilibreur de charge de service	Échec de la création de l'équilibreur de charge de service		Primordial
Incompatibilité de réplication de charge de travail	Certains pods ne sont actuellement pas disponibles pour un déploiement ou un DaemonSet.		Avertissement @ > 1
Les requêtes CPU ResourceQuota sont sur le point d'être dépassées	Les demandes CPU pour l'espace de noms sont sur le point de dépasser ResourceQuota		Avertissement à > 80 % Critique à > 90 %
Taux de retransmission élevé	Taux de retransmission TCP élevé	Vérifiez la congestion du réseau - Identifiez les charges de travail qui consomment beaucoup de bande passante réseau. Vérifiez l'utilisation élevée du processeur Pod. Vérifiez les performances du réseau matériel.	Avertissement à > 10 % Critique à > 25 %
Pression du disque du nœud	L'espace disque disponible et les inodes sur le système de fichiers racine ou le système de fichiers image du nœud ont satisfait un seuil d'expulsion.	- Augmentez la taille des disques de nœuds pour garantir qu'il y a suffisamment d'espace pour les fichiers d'application. - Réduire l'utilisation des fichiers d'application.	Critique @ > 0
Saturation élevée du processeur du cluster	La saturation du processeur allouable au cluster est élevée. La saturation du processeur du cluster est calculée comme la somme de l'utilisation du processeur divisée par la somme du processeur allouable sur tous les nœuds K8.	Ajouter des nœuds. Corrigez tous les nœuds non planifiés. Ajustez la taille des pods pour libérer du CPU sur les nœuds.	Avertissement à > 80 % Critique à > 90 %

Retour en haut

Moniteurs de journaux de modifications

Nom du moniteur	Gravité	Description du moniteur
Volume interne découvert	Informatif	Ce message s'affiche lorsqu'un volume interne est découvert.
Volume interne modifié	Informatif	Ce message s'affiche lorsqu'un volume interne est modifié.

Nœud de stockage découvert	Informatif	Ce message s'affiche lorsqu'un nœud de stockage est découvert.
Nœud de stockage supprimé	Informatif	Ce message s'affiche lorsqu'un nœud de stockage est supprimé.
Pool de stockage découvert	Informatif	Ce message s'affiche lorsqu'un pool de stockage est découvert.
Machine virtuelle de stockage découverte	Informatif	Ce message s'affiche lorsqu'une machine virtuelle de stockage est découverte.
Machine virtuelle de stockage modifiée	Informatif	Ce message s'affiche lorsqu'une machine virtuelle de stockage est modifiée.

Retour en haut

Moniteurs de collecte de données

Nom du moniteur	Description	Action corrective
Arrêt de l'unité d'acquisition	Les unités d'acquisition Data Infrastructure Insights redémarrent périodiquement dans le cadre de mises à niveau pour introduire de nouvelles fonctionnalités. Cela se produit une fois par mois ou moins dans un environnement typique. Une alerte d'avertissement indiquant qu'une unité d'acquisition s'est arrêtée doit être suivie peu de temps après par une résolution indiquant que l'unité d'acquisition nouvellement redémarrée a terminé un enregistrement auprès de Data Infrastructure Insights. En général, ce cycle d'arrêt à enregistrement prend entre 5 et 15 minutes.	Si l'alerte se produit fréquemment ou dure plus de 15 minutes, vérifiez le fonctionnement du système hébergeant l'unité d'acquisition, le réseau et tout proxy connectant l'AU à Internet.
Échec du collecteur	L'enquête d'un collecteur de données a rencontré une situation d'échec inattendue.	Visitez la page du collecteur de données dans Data Infrastructure Insights pour en savoir plus sur la situation.

Avertissement aux collectionneurs	Cette alerte peut généralement survenir en raison d'une configuration erronée du collecteur de données ou du système cible. Revoyez les configurations pour éviter de futures alertes. Cela peut également être dû à une récupération de données incomplètes alors que le collecteur de données a rassemblé toutes les données qu'il pouvait. Cela peut se produire lorsque les situations changent pendant la collecte de données (par exemple, une machine virtuelle présente au début de la collecte de données est supprimée pendant la collecte de données et avant que ses données ne soient capturées).	Vérifiez la configuration du collecteur de données ou du système cible. Notez que le moniteur pour Collector Warning peut envoyer plus d'alertes que les autres types de moniteurs. Il est donc recommandé de ne définir aucun destinataire d'alerte, sauf si vous effectuez un dépannage.

Retour en haut

Moniteurs de sécurité

Nom du moniteur	Seuil	Description du moniteur	Action corrective
Transport HTTPS AutoSupport désactivé	Avertissement @ < 1	AutoSupport prend en charge HTTPS, HTTP et SMTP pour les protocoles de transport. En raison de la nature sensible des messages AutoSupport , NetApp recommande fortement d'utiliser HTTPS comme protocole de transport par défaut pour l'envoi de messages AutoSupport au support NetApp .	Pour définir HTTPS comme protocole de transport pour les messages AutoSupport , exécutez la commande ONTAP suivante :…system node autosupport modify -transport https
Chiffres non sécurisés en cluster pour SSH	Avertissement @ < 1	Indique que SSH utilise des chiffrements non sécurisés, par exemple des chiffrements commençant par *cbc.	Pour supprimer les chiffrements CBC, exécutez la commande ONTAP suivante :…security ssh remove -vserver <admin vserver> -ciphers aes256-cbc,aes192-cbc,aes128-cbc,3des-cbc

Bannière de connexion au cluster désactivée	Avertissement @ < 1	Indique que la bannière de connexion est désactivée pour les utilisateurs accédant au système ONTAP . L'affichage d'une bannière de connexion est utile pour établir les attentes en matière d'accès et d'utilisation du système.	Pour configurer la bannière de connexion d'un cluster, exécutez la commande ONTAP suivante :…security login banner modify -vserver <admin svm> -message "Accès restreint aux utilisateurs autorisés"
Communication entre pairs du cluster non chiffrée	Avertissement @ < 1	Lors de la réplication de données pour la reprise après sinistre, la mise en cache ou la sauvegarde, vous devez protéger ces données pendant le transport sur le réseau d'un cluster ONTAP à un autre. Le chiffrement doit être configuré sur les clusters source et de destination.	Pour activer le chiffrement sur les relations homologues de cluster créées avant ONTAP 9.6, le cluster source et de destination doivent être mis à niveau vers la version 9.6. Utilisez ensuite la commande « cluster peer modify » pour modifier les homologues du cluster source et de destination afin d'utiliser le chiffrement de peering de cluster. Consultez le Guide de renforcement de la sécurité NetApp pour ONTAP 9 pour plus de détails.
Utilisateur administrateur local par défaut activé	Avertissement @ > 0	NetApp recommande de verrouiller (désactiver) tous les comptes d'utilisateur administrateur par défaut (intégrés) inutiles avec la commande lock. Il s'agit principalement de comptes par défaut pour lesquels les mots de passe n'ont jamais été mis à jour ou modifiés.	Pour verrouiller le compte « admin » intégré, exécutez la commande ONTAP suivante :…security login lock -username admin
Mode FIPS désactivé	Avertissement @ < 1	Lorsque la conformité FIPS 140-2 est activée, TLSv1 et SSLv3 sont désactivés et seuls TLSv1.1 et TLSv1.2 restent activés. ONTAP vous empêche d'activer TLSv1 et SSLv3 lorsque la conformité FIPS 140-2 est activée.	Pour activer la conformité FIPS 140-2 sur un cluster, exécutez la commande ONTAP suivante en mode privilège avancé :…security config modify -interface SSL -is -fips-enabled true

Transfert de journaux non chiffré	Avertissement @ < 1	Le déchargement des informations syslog est nécessaire pour limiter la portée ou l'empreinte d'une violation à un seul système ou à une seule solution. Par conséquent, NetApp recommande de décharger en toute sécurité les informations syslog vers un emplacement de stockage ou de conservation sécurisé.	Une fois qu'une destination de transfert de journal est créée, son protocole ne peut pas être modifié. Pour passer à un protocole chiffré, supprimez et recréez la destination de transfert de journal à l'aide de la commande ONTAP suivante :…cluster log-forwarding create -destination <destination ip> -protocol tcp-encrypted
Mot de passe haché MD5	Avertissement @ > 0	NetApp recommande fortement d'utiliser la fonction de hachage SHA-512 plus sécurisée pour les mots de passe des comptes utilisateurs ONTAP . Les comptes utilisant la fonction de hachage MD5 moins sécurisée doivent migrer vers la fonction de hachage SHA-512.	NetApp recommande fortement aux comptes utilisateurs de migrer vers la solution SHA-512 plus sécurisée en demandant aux utilisateurs de modifier leurs mots de passe.…pour verrouiller les comptes avec des mots de passe qui utilisent la fonction de hachage MD5, exécutez la commande ONTAP suivante :…security login lock -vserver * -username * -hash-function md5
Aucun serveur NTP n'est configuré	Avertissement @ < 1	Indique que le cluster n'a pas de serveurs NTP configurés. Pour la redondance et un service optimal, NetApp recommande d'associer au moins trois serveurs NTP au cluster.	Pour associer un serveur NTP au cluster, exécutez la commande ONTAP suivante : cluster time-service ntp server create -server <ntp server host name or IP address>
Le nombre de serveurs NTP est faible	Avertissement @ < 3	Indique que le cluster possède moins de 3 serveurs NTP configurés. Pour la redondance et un service optimal, NetApp recommande d'associer au moins trois serveurs NTP au cluster.	Pour associer un serveur NTP au cluster, exécutez la commande ONTAP suivante :…cluster time-service ntp server create -server <nom d'hôte ou adresse IP du serveur NTP>

Shell distant activé	Avertissement @ > 0	Remote Shell n'est pas une méthode sécurisée pour établir un accès en ligne de commande à la solution ONTAP . Le shell distant doit être désactivé pour un accès distant sécurisé.	NetApp recommande Secure Shell (SSH) pour un accès distant sécurisé.…Pour désactiver le shell distant sur un cluster, exécutez la commande ONTAP suivante en mode de privilège avancé :…security protocol modify -application rsh- enabled false
Journal d'audit de la machine virtuelle de stockage désactivé	Avertissement @ < 1	Indique que la journalisation d'audit est désactivée pour SVM.	Pour configurer le journal d'audit d'un serveur virtuel, exécutez la commande ONTAP suivante :…vserver audit enable -vserver <svm>
Chiffres non sécurisés de la machine virtuelle de stockage pour SSH	Avertissement @ < 1	Indique que SSH utilise des chiffrements non sécurisés, par exemple des chiffrements commençant par *cbc.	Pour supprimer les chiffrements CBC, exécutez la commande ONTAP suivante :…security ssh remove -vserver <vserver> -ciphers aes256-cbc,aes192-cbc,aes128-cbc,3des-cbc
Bannière de connexion à la machine virtuelle de stockage désactivée	Avertissement @ < 1	Indique que la bannière de connexion est désactivée pour les utilisateurs accédant aux SVM sur le système. L'affichage d'une bannière de connexion est utile pour établir les attentes en matière d'accès et d'utilisation du système.	Pour configurer la bannière de connexion d'un cluster, exécutez la commande ONTAP suivante :…security login banner modify -vserver <svm> -message "Accès restreint aux utilisateurs autorisés"
Protocole Telnet activé	Avertissement @ > 0	Telnet n'est pas une méthode sécurisée pour établir un accès en ligne de commande à la solution ONTAP . Telnet doit être désactivé pour un accès distant sécurisé.	NetApp recommande Secure Shell (SSH) pour un accès à distance sécurisé. Pour désactiver Telnet sur un cluster, exécutez la commande ONTAP suivante en mode privilège avancé :…security protocol modify -application telnet -enabled false

Retour en haut

Contrôleurs de la protection des données

Nom du moniteur	Seuils	Description du moniteur	Action corrective
Espace insuffisant pour la copie de l'instantané Lun	(Filtre contains_luns = Oui) Avertissement à > 95 %…Critique à > 100 %	La capacité de stockage d'un volume est nécessaire pour stocker les données d'application et de client. Une partie de cet espace, appelée espace réservé aux instantanés, est utilisée pour stocker des instantanés qui permettent de protéger les données localement. Plus les données nouvelles et mises à jour sont stockées dans le volume ONTAP , plus la capacité de snapshot est utilisée et moins la capacité de stockage de snapshot sera disponible pour les données nouvelles ou mises à jour futures. Si la capacité des données de snapshot dans un volume atteint l'espace de réserve total de snapshot, le client peut être incapable de stocker de nouvelles données de snapshot et réduire le niveau de protection des données dans les LUN du volume. La surveillance de la capacité de snapshot du volume utilisé garantit la continuité des services de données.	**Actions immédiates** Si le seuil critique est dépassé, envisagez des actions immédiates pour minimiser les interruptions de service : 1. Configurez les instantanés pour utiliser l'espace de données dans le volume lorsque la réserve d'instantanés est pleine. 2. Supprimez certains anciens instantanés indésirables pour libérer de l'espace. **Actions à effectuer prochainement** Si le seuil d'avertissement est dépassé, prévoyez de prendre les mesures immédiates suivantes : 1. Augmentez l'espace de réserve d'instantanés dans le volume pour s'adapter à la croissance. 2. Configurez les instantanés pour utiliser l'espace de données dans le volume lorsque la réserve d'instantanés est pleine.

Décalage relationnel SnapMirror	Avertissement à > 150 %… Critique à > 300 %	Le décalage de relation SnapMirror est la différence entre l'horodatage de l'instantané et l'heure sur le système de destination. Lag_time_percent est le rapport entre le temps de latence et l'intervalle de planification de la politique SnapMirror . Si le temps de latence est égal à l'intervalle de planification, lag_time_percent sera de 100 %. Si la politique SnapMirror n'a pas de planification, lag_time_percent ne sera pas calculé.	Surveillez l'état de SnapMirror à l'aide de la commande « snapmirror show ». Vérifiez l'historique des transferts SnapMirror à l'aide de la commande « snapmirror show-history »

Retour en haut

Moniteurs de volume de nuages (CVO)

Nom du moniteur	Gravité de l'IC	Description du moniteur	Action corrective
Disque CVO hors service	INFO	Cet événement se produit lorsqu'un disque est retiré du service parce qu'il a été marqué comme défectueux, est en cours de nettoyage ou est entré dans le centre de maintenance.	Aucune

Échec de la restitution du pool de stockage par CVO	CRITIQUE	Cet événement se produit lors de la migration d'un agrégat dans le cadre d'un basculement de stockage (SFO), lorsque le nœud de destination ne peut pas atteindre les magasins d'objets.	Effectuez les actions correctives suivantes : Vérifiez que votre LIF intercluster est en ligne et fonctionnel à l'aide de la commande « network interface show ». Vérifiez la connectivité réseau au serveur de magasin d'objets en utilisant la commande « ping » sur le LIF intercluster du nœud de destination. Vérifiez que la configuration de votre magasin d'objets n'a pas changé et que les informations de connexion et de connectivité sont toujours exactes à l'aide de la commande « aggregate object-store config show ». Alternativement, vous pouvez remplacer l'erreur en spécifiant false pour le paramètre « require-partner-waiting » de la commande giveback. Contactez le support technique NetApp pour plus d'informations ou d'assistance.

Interconnexion CVO HA en panne	AVERTISSEMENT	L'interconnexion haute disponibilité (HA) est en panne. Risque d'interruption de service lorsque le basculement n'est pas disponible.	Les actions correctives dépendent du nombre et du type de liens d'interconnexion HA pris en charge par la plate-forme, ainsi que de la raison pour laquelle l'interconnexion est en panne. Si les liens sont interrompus : vérifiez que les deux contrôleurs de la paire HA sont opérationnels. Pour les liaisons connectées en externe, assurez-vous que les câbles d'interconnexion sont correctement connectés et que les connecteurs à petit facteur de forme (SFP), le cas échéant, sont correctement installés sur les deux contrôleurs. Pour les liens connectés en interne, désactivez et réactivez les liens, l'un après l'autre, en utilisant les commandes « ic link off » et « ic link on ». Si les liens sont désactivés, activez-les en utilisant la commande « ic link on ». Si un pair n'est pas connecté, désactivez et réactivez les liens, l'un après l'autre, en utilisant les commandes « ic link off » et « ic link on ». Contactez le support technique NetApp si le problème persiste.

Nombre maximal de sessions CVO par utilisateur dépassé	AVERTISSEMENT	Vous avez dépassé le nombre maximal de sessions autorisées par utilisateur sur une connexion TCP. Toute demande d'établissement d'une session sera refusée jusqu'à ce que certaines sessions soient libérées.	Effectuez les actions correctives suivantes : inspectez toutes les applications qui s'exécutent sur le client et fermez celles qui ne fonctionnent pas correctement. Redémarrez le client. Vérifiez si le problème est causé par une application nouvelle ou existante : si l'application est nouvelle, définissez un seuil plus élevé pour le client en utilisant la commande « cifs option modify -max -opens-same-file-per -tree ». Dans certains cas, les clients fonctionnent comme prévu, mais nécessitent un seuil plus élevé. Vous devez disposer de privilèges avancés pour définir un seuil plus élevé pour le client. Si le problème est causé par une application existante, il peut y avoir un problème avec le client. Contactez le support technique NetApp pour plus d'informations ou d'assistance.

Conflit de nom NetBIOS CVO	CRITIQUE	Le service de noms NetBIOS a reçu une réponse négative à une demande d'enregistrement de nom, provenant d'une machine distante. Cela est généralement dû à un conflit dans le nom NetBIOS ou dans un alias. Par conséquent, les clients risquent de ne pas pouvoir accéder aux données ou de se connecter au bon nœud de service de données dans le cluster.	Effectuez l'une des actions correctives suivantes : S'il existe un conflit dans le nom NetBIOS ou un alias, effectuez l'une des opérations suivantes : Supprimez l'alias NetBIOS en double à l'aide de la commande « vserver cifs delete -aliases alias -vserver vserver ». Renommez un alias NetBIOS en supprimant le nom en double et en ajoutant un alias avec un nouveau nom à l'aide de la commande « vserver cifs create -aliases alias -vserver vserver ». S'il n'y a pas d'alias configuré et qu'il y a un conflit dans le nom NetBIOS, renommez le serveur CIFS en utilisant les commandes « vserver cifs delete -vserver vserver » et « vserver cifs create -cifs -server netbiosname ». REMARQUE : la suppression d'un serveur CIFS peut rendre les données inaccessibles. Supprimez le nom NetBIOS ou renommez le NetBIOS sur la machine distante.
Pool de stockage CVO NFSv4 épuisé	CRITIQUE	Un pool de stockage NFSv4 a été épuisé.	Si le serveur NFS ne répond pas pendant plus de 10 minutes après cet événement, contactez le support technique NetApp .
Panique du nœud CVO	AVERTISSEMENT	Cet événement est émis lorsqu'une panique se produit	Contactez le support client NetApp .

Faible volume d'espace racine du nœud CVO	CRITIQUE	Le système a détecté que le volume racine est dangereusement bas en termes d'espace. Le nœud n'est pas entièrement opérationnel. Les LIF de données peuvent avoir basculé au sein du cluster, ce qui limite l'accès NFS et CIFS sur le nœud. La capacité administrative est limitée aux procédures de récupération locales permettant au nœud de libérer de l'espace sur le volume racine.	Effectuez les actions correctives suivantes : libérez de l'espace sur le volume racine en supprimant les anciennes copies Snapshot, en supprimant les fichiers dont vous n'avez plus besoin du répertoire /mroot ou en augmentant la capacité du volume racine. Redémarrez le contrôleur. Contactez le support technique NetApp pour plus d'informations ou d'assistance.
Partage administratif inexistant du CVO	CRITIQUE	Problème Vscan : un client a tenté de se connecter à un partage ONTAP_ADMIN$ inexistant.	Assurez-vous que Vscan est activé pour l'ID SVM mentionné. L'activation de Vscan sur un SVM entraîne la création automatique du partage ONTAP_ADMIN$ pour le SVM.
Hôte du magasin d'objets CVO non résoluble	CRITIQUE	Le nom d'hôte du serveur de magasin d'objets ne peut pas être résolu en une adresse IP. Le client du magasin d'objets ne peut pas communiquer avec le serveur du magasin d'objets sans résoudre une adresse IP. Par conséquent, les données peuvent être inaccessibles.	Vérifiez la configuration DNS pour vérifier que le nom d'hôte est correctement configuré avec une adresse IP.
LIF intercluster du magasin d'objets CVO en panne	CRITIQUE	Le client du magasin d'objets ne trouve pas de LIF opérationnel pour communiquer avec le serveur du magasin d'objets. Le nœud n'autorisera pas le trafic client du magasin d'objets tant que le LIF intercluster ne sera pas opérationnel. Par conséquent, les données peuvent être inaccessibles.	Effectuez les actions correctives suivantes : Vérifiez l'état LIF intercluster à l'aide de la commande « network interface show -role intercluster ». Vérifiez que le LIF intercluster est correctement configuré et opérationnel. Si un LIF intercluster n'est pas configuré, ajoutez-le à l'aide de la commande « network interface create -role intercluster ».

Non-concordance des signatures du magasin d'objets CVO	CRITIQUE	La signature de la demande envoyée au serveur de magasin d'objets ne correspond pas à la signature calculée par le client. Par conséquent, les données peuvent être inaccessibles.	Vérifiez que la clé d'accès secrète est correctement configurée. S'il est configuré correctement, contactez le support technique NetApp pour obtenir de l'aide.
Mémoire du moniteur QoS CVO au maximum	CRITIQUE	La mémoire dynamique du sous-système QoS a atteint sa limite pour le matériel de la plate-forme actuelle. Certaines fonctionnalités QoS peuvent fonctionner avec une capacité limitée.	Supprimez certaines charges de travail ou flux actifs pour libérer de la mémoire. Utilisez la commande « statistics show -object workload -counter ops » pour déterminer quelles charges de travail sont actives. Les charges de travail actives affichent des opérations non nulles. Utilisez ensuite la commande « workload delete <workload_name> » plusieurs fois pour supprimer des charges de travail spécifiques. Vous pouvez également utiliser la commande « stream delete -workload <nom de la charge de travail> * » pour supprimer les flux associés de la charge de travail active.

Délai d’expiration de CVO READDIR	CRITIQUE	Une opération de fichier READDIR a dépassé le délai d’exécution autorisé dans WAFL. Cela peut être dû à des répertoires très volumineux ou peu nombreux. Des mesures correctives sont recommandées.	Effectuez les actions correctives suivantes : recherchez des informations spécifiques aux répertoires récents dont les opérations de fichier READDIR ont expiré en utilisant la commande CLI nodeshell de privilège « diag » suivante : wafl readdir notice show. Vérifiez si les répertoires sont indiqués comme clairsemés ou non : si un répertoire est indiqué comme clairsemé, il est recommandé de copier le contenu du répertoire dans un nouveau répertoire pour supprimer la clairsemée du fichier de répertoire. Si un répertoire n’est pas indiqué comme clairsemé et que le répertoire est volumineux, il est recommandé de réduire la taille du fichier de répertoire en réduisant le nombre d’entrées de fichier dans le répertoire.

Échec de la relocalisation du pool de stockage CVO	CRITIQUE	Cet événement se produit lors du déplacement d'un agrégat, lorsque le nœud de destination ne peut pas atteindre les magasins d'objets.	Effectuez les actions correctives suivantes : Vérifiez que votre LIF intercluster est en ligne et fonctionnel à l'aide de la commande « network interface show ». Vérifiez la connectivité réseau au serveur de magasin d'objets en utilisant la commande « ping » sur le LIF intercluster du nœud de destination. Vérifiez que la configuration de votre magasin d'objets n'a pas changé et que les informations de connexion et de connectivité sont toujours exactes à l'aide de la commande « aggregate object-store config show ». Vous pouvez également remplacer l'erreur en utilisant le paramètre « override-destination-checks » de la commande de relocalisation. Contactez le support technique NetApp pour plus d'informations ou d'assistance.
Échec de la copie fantôme CVO	CRITIQUE	Une opération de service de sauvegarde et de restauration de Volume Shadow Copy Service (VSS) de Microsoft Server a échoué.	Vérifiez les éléments suivants à l'aide des informations fournies dans le message d'événement : la configuration de la copie fantôme est-elle activée ? Les licences appropriées sont-elles installées ? Sur quelles actions l'opération de cliché instantané est-elle effectuée ? Le nom de l'action est-il correct ? Le chemin de partage existe-t-il ? Quels sont les états de l'ensemble de copies fantômes et de ses copies fantômes ?

L’arrêt de la machine virtuelle de stockage CVO a réussi	INFO	Ce message s’affiche lorsqu’une opération « vserver stop » réussit.	Utilisez la commande « vserver start » pour démarrer l’accès aux données sur une machine virtuelle de stockage.
CVO Trop d’authentification CIFS	AVERTISSEMENT	De nombreuses négociations d’authentification ont eu lieu simultanément. Il y a 256 demandes de nouvelles sessions incomplètes de ce client.	Recherchez pourquoi le client a créé 256 nouvelles demandes de connexion ou plus. Vous devrez peut-être contacter le fournisseur du client ou de l’application pour déterminer pourquoi l’erreur s’est produite.
Disques non attribués CVO	INFO	Le système possède des disques non attribués : la capacité est gaspillée et votre système peut être soumis à une mauvaise configuration ou à une modification partielle de la configuration.	Effectuez les actions correctives suivantes : déterminez quels disques ne sont pas attribués à l’aide de la commande « disk show -n ». Affectez les disques à un système en utilisant la commande « disk assign ».
Accès utilisateur non autorisé CVO au partage administrateur	AVERTISSEMENT	Un client a tenté de se connecter au partage privilégié ONTAP_ADMIN$ même si son utilisateur connecté n’est pas un utilisateur autorisé.	Effectuez les actions correctives suivantes : assurez-vous que le nom d’utilisateur et l’adresse IP mentionnés sont configurés dans l’un des pools de scanners Vscan actifs. Vérifiez la configuration du pool de scanners actuellement active à l’aide de la commande « vserver vscan scanner pool show-active ».

Virus CVO détecté	AVERTISSEMENT	Un serveur Vscan a signalé une erreur au système de stockage. Cela indique généralement qu'un virus a été détecté. Cependant, d'autres erreurs sur le serveur Vscan peuvent provoquer cet événement. L'accès du client au fichier est refusé. Le serveur Vscan peut, selon ses paramètres et sa configuration, nettoyer le fichier, le mettre en quarantaine ou le supprimer.	Vérifiez le journal du serveur Vscan signalé dans l'événement « syslog » pour voir s'il a réussi à nettoyer, mettre en quarantaine ou supprimer le fichier infecté. Si cela n'est pas possible, un administrateur système devra peut-être supprimer manuellement le fichier.
Volume CVO hors ligne	INFO	Ce message indique qu'un volume est mis hors ligne.	Remettez le volume en ligne.
Volume CVO restreint	INFO	Cet événement indique qu'un volume flexible est rendu restreint.	Remettez le volume en ligne.

Retour en haut

Moniteurs de journaux médiateurs SnapMirror for Business Continuity (SMBC)

Nom du moniteur	Gravité	Description du moniteur	Action corrective
Ajout du médiateur ONTAP	INFO	Ce message s'affiche lorsque ONTAP Mediator est ajouté avec succès sur un cluster.	Aucune
Médiateur ONTAP non accessible	CRITIQUE	Ce message s'affiche lorsque le médiateur ONTAP est réutilisé ou que le package Médiateur n'est plus installé sur le serveur Médiateur. Par conséquent, le basculement de SnapMirror n'est pas possible.	Supprimez la configuration du médiateur ONTAP actuel à l'aide de la commande « snapmirror mediator remove ». Reconfigurez l'accès au médiateur ONTAP à l'aide de la commande « snapmirror mediator add ».
Suppression du médiateur ONTAP	INFO	Ce message s'affiche lorsque ONTAP Mediator est supprimé avec succès d'un cluster.	Aucune

Médiateur ONTAP inaccessible	AVERTISSEMENT	Ce message s'affiche lorsque le médiateur ONTAP est inaccessible sur un cluster. Par conséquent, le basculement de SnapMirror n'est pas possible.	Vérifiez la connectivité réseau au médiateur ONTAP en utilisant les commandes « network ping » et « network traceroute ». Si le problème persiste, supprimez la configuration du médiateur ONTAP actuel à l'aide de la commande « snapmirror mediator remove ». Reconfigurez l'accès au médiateur ONTAP à l'aide de la commande « snapmirror mediator add ».
Le certificat SMBC CA a expiré	CRITIQUE	Ce message s'affiche lorsque le certificat de l'autorité de certification (CA) ONTAP Mediator a expiré. Par conséquent, toute communication ultérieure avec le médiateur de ONTAP ne sera plus possible.	Supprimez la configuration du médiateur ONTAP actuel à l'aide de la commande « snapmirror mediator remove ». Mettre à jour un nouveau certificat CA sur le serveur ONTAP Mediator. Reconfigurez l'accès au médiateur ONTAP à l'aide de la commande « snapmirror mediator add ».
Expiration du certificat SMBC CA	AVERTISSEMENT	Ce message s'affiche lorsque le certificat de l'autorité de certification (CA) ONTAP Mediator doit expirer dans les 30 prochains jours.	Avant l'expiration de ce certificat, supprimez la configuration du médiateur ONTAP actuel à l'aide de la commande « snapmirror mediator remove ». Mettre à jour un nouveau certificat CA sur le serveur ONTAP Mediator. Reconfigurez l'accès au médiateur ONTAP à l'aide de la commande « snapmirror mediator add ».

Certificat client SMBC expiré	CRITIQUE	Ce message s'affiche lorsque le certificat client ONTAP Mediator a expiré. Par conséquent, toute communication ultérieure avec le médiateur de ONTAP ne sera plus possible.	Supprimez la configuration du médiateur ONTAP actuel à l'aide de la commande « snapmirror mediator remove ». Reconfigurez l'accès au médiateur ONTAP à l'aide de la commande « snapmirror mediator add ».
Expiration du certificat client SMBC	AVERTISSEMENT	Ce message s'affiche lorsque le certificat client ONTAP Mediator doit expirer dans les 30 prochains jours.	Avant l'expiration de ce certificat, supprimez la configuration du médiateur ONTAP actuel à l'aide de la commande « snapmirror mediator remove ». Reconfigurez l'accès au médiateur ONTAP à l'aide de la commande « snapmirror mediator add ».
Relation SMBC désynchronisée Remarque : UM n'a pas celui-ci	CRITIQUE	Ce message s'affiche lorsqu'une relation SnapMirror for Business Continuity (SMBC) change de statut de « synchronisé » à « désynchronisé ». En raison de ce RPO=0, la protection des données sera perturbée.	Vérifiez la connexion réseau entre les volumes source et de destination. Surveillez l'état de la relation SMBC en utilisant la commande « snapmirror show » sur la destination et en utilisant la commande « snapmirror list-destinations » sur la source. La resynchronisation automatique tentera de ramener la relation à l'état « synchronisé ». Si la resynchronisation échoue, vérifiez que tous les nœuds du cluster sont en quorum et sont sains.

Certificat du serveur SMBC expiré	CRITIQUE	Ce message s'affiche lorsque le certificat du serveur ONTAP Mediator a expiré. Par conséquent, toute communication ultérieure avec le médiateur de ONTAP ne sera plus possible.	Supprimez la configuration du médiateur ONTAP actuel à l'aide de la commande « snapmirror mediator remove ». Mettre à jour un nouveau certificat de serveur sur le serveur ONTAP Mediator. Reconfigurez l'accès au médiateur ONTAP à l'aide de la commande « snapmirror mediator add ».
Expiration du certificat du serveur SMBC	AVERTISSEMENT	Ce message s'affiche lorsque le certificat du serveur ONTAP Mediator doit expirer dans les 30 prochains jours.	Avant l'expiration de ce certificat, supprimez la configuration du médiateur ONTAP actuel à l'aide de la commande « snapmirror mediator remove ». Mettre à jour un nouveau certificat de serveur sur le serveur ONTAP Mediator. Reconfigurez l'accès au médiateur ONTAP à l'aide de la commande « snapmirror mediator add ».

Retour en haut

Moniteurs d'alimentation, de pulsation et de système divers supplémentaires

Nom du moniteur	Gravité	Description du moniteur	Action corrective
Découverte d'une alimentation pour étagère à disques	INFORMATIF	Ce message s'affiche lorsqu'un bloc d'alimentation est ajouté à l'étagère de disques.	AUCUN
Étagères de disques Alimentation retirée	INFORMATIF	Ce message s'affiche lorsqu'un bloc d'alimentation est retiré de l'étagère de disque.	AUCUN
Commutation automatique non planifiée de MetroCluster désactivée	CRITIQUE	Ce message s'affiche lorsque la fonction de basculement automatique non planifié est désactivée.	Exécutez la commande « metrocluster modify -node-name <nodename> -automatic-switchover -onfailure true » pour chaque nœud du cluster pour activer le basculement automatique.

Nom du moniteur	Gravité	Description du moniteur	Action corrective
Pont de stockage MetroCluster inaccessible	CRITIQUE	Le pont de stockage n'est pas accessible via le réseau de gestion	1) Si le pont est surveillé par SNMP, vérifiez que le LIF de gestion des nœuds est actif à l'aide de la commande « network interface show ». Vérifiez que le pont est actif en utilisant la commande « network ping ». 2) Si le pont est surveillé en bande, vérifiez le câblage de la structure vers le pont, puis vérifiez que le pont est sous tension.
Température anormale du pont MetroCluster (en dessous du seuil critique)	CRITIQUE	Le capteur sur le pont Fibre Channel signale une température inférieure au seuil critique.	1) Vérifiez l'état de fonctionnement des ventilateurs sur le pont de stockage. 2) Vérifiez que le pont fonctionne dans les conditions de température recommandées.
Température anormale du pont MetroCluster (supérieure au seuil critique)	CRITIQUE	Le capteur sur le pont Fibre Channel signale une température supérieure au seuil critique.	1) Vérifiez l'état de fonctionnement du capteur de température du châssis sur le pont de stockage à l'aide de la commande « storage bridge show -cooling ». 2) Vérifiez que le pont de stockage fonctionne dans les conditions de température recommandées.
L'agrégat MetroCluster laissé pour compte	AVERTISSEMENT	L'agrégat a été laissé sur place lors du virage.	1) Vérifiez l'état agrégé en utilisant la commande « aggr show ». 2) Si l'agrégat est en ligne, restituez-le à son propriétaire d'origine en utilisant la commande « metrocluster switchback ».

Nom du moniteur	Gravité	Description du moniteur	Action corrective
Tous les liens entre les partenaires du Metrocluster sont interrompus	CRITIQUE	Les adaptateurs d'interconnexion RDMA et les LIF intercluster ont des connexions rompues avec le cluster appairé ou le cluster appairé est en panne.	1) Assurez-vous que les LIF interclusters sont opérationnels. Réparez les LIF interclusters s'ils sont en panne. 2) Vérifiez que le cluster appairé est opérationnel à l'aide de la commande « cluster peer ping ». Consultez le Guide de récupération après sinistre de MetroCluster si le cluster appairé est en panne. 3) Pour le fabric MetroCluster, vérifiez que les ISL du fabric back-end sont opérationnels. Réparez les ISL du tissu back-end s'ils sont en panne. 4) Pour les configurations MetroCluster non fabric, vérifiez que le câblage est correct entre les adaptateurs d'interconnexion RDMA. Reconfigurez le câblage si les liaisons sont coupées.
Les partenaires de MetroCluster ne sont pas joignables via le réseau de peering	CRITIQUE	La connectivité au cluster homologue est interrompue.	1) Assurez-vous que le port est connecté au bon réseau/commutateur. 2) Assurez-vous que le LIF intercluster est connecté au cluster homologue. 3) Assurez-vous que le cluster appairé est opérationnel en utilisant la commande « cluster peer ping ». Consultez le Guide de récupération après sinistre de MetroCluster si le cluster appairé est en panne.

Nom du moniteur	Gravité	Description du moniteur	Action corrective
Toutes les liaisons du commutateur MetroCluster Inter sont interrompues	CRITIQUE	Toutes les liaisons inter-commutateurs (ISL) sur le commutateur de stockage sont hors service.	1) Réparez les ISL de la structure principale sur le commutateur de stockage. 2) Assurez-vous que le commutateur partenaire est activé et que ses ISL sont opérationnels. 3) Assurez-vous que les équipements intermédiaires, tels que les périphériques xWDM, sont opérationnels.
Liaison SAS entre le nœud MetroCluster et la pile de stockage interrompue	AVERTISSEMENT	L'adaptateur SAS ou son câble connecté peut être en cause.	1. Vérifiez que l'adaptateur SAS est en ligne et en cours d'exécution. 2. Vérifiez que la connexion du câble physique est sécurisée et fonctionnelle, et remplacez le câble si nécessaire. 3. Si l'adaptateur SAS est connecté à des étagères de disques, assurez-vous que les IOM et les disques sont correctement installés.
Les liens initiateurs de MetroClusterFC sont hors service	CRITIQUE	L'adaptateur initiateur FC est en cause.	1. Assurez-vous que le lien initiateur FC n'a pas été altéré. 2. Vérifiez l'état opérationnel de l'adaptateur initiateur FC à l'aide de la commande « system node run -node local -command storage show adapter ».
Liaison d'interconnexion FC-VI interrompue	CRITIQUE	Le lien physique sur le port FC-VI est hors ligne.	1. Assurez-vous que la liaison FC-VI n'a pas été altéré. 2. Vérifiez que l'état physique de l'adaptateur FC-VI est « Up » en utilisant la commande « metrocluster interconnect adapter show ». 3. Si la configuration inclut des commutateurs fabric, assurez-vous qu'ils sont correctement câblés et configurés.

Nom du moniteur	Gravité	Description du moniteur	Action corrective
Disques de rechange MetroCluster abandonnés	AVERTISSEMENT	Le disque de rechange a été laissé sur place lors du changement de direction.	Si le disque n'est pas défectueux, restituez-le à son propriétaire d'origine en utilisant la commande « metrocluster switchback ».
Port du pont de stockage MetroCluster en panne	CRITIQUE	Le port sur le pont de stockage est hors ligne.	1) Vérifiez l'état opérationnel des ports sur le pont de stockage en utilisant la commande « storage bridge show -ports ». 2) Vérifiez la connectivité logique et physique au port.
Panne des ventilateurs du commutateur de stockage MetroCluster	CRITIQUE	Le ventilateur du commutateur de stockage est tombé en panne.	1) Assurez-vous que les ventilateurs du commutateur fonctionnent correctement en utilisant la commande « storage switch show -cooling ». 2) Assurez-vous que les FRU du ventilateur sont correctement insérés et opérationnels.
Commutateur de stockage MetroCluster inaccessible	CRITIQUE	Le commutateur de stockage n'est pas accessible via le réseau de gestion.	1) Assurez-vous que le LIF de gestion des nœuds est actif en utilisant la commande « network interface show ». 2) Assurez-vous que le commutateur est actif en utilisant la commande « network ping ». 3) Assurez-vous que le commutateur est accessible via SNMP en vérifiant ses paramètres SNMP après vous être connecté au commutateur.

Nom du moniteur	Gravité	Description du moniteur	Action corrective
Panne d’alimentation du commutateur MetroCluster	CRITIQUE	Un bloc d’alimentation sur le commutateur de stockage n’est pas opérationnel.	1) Vérifiez les détails de l’erreur en utilisant la commande « storage switch show -error -switch -name <swtich name> ». 2) Identifiez le bloc d’alimentation défectueux en utilisant la commande « storage switch show -power -switch-name <switch name> ». 3) Assurez-vous que le bloc d’alimentation est correctement inséré dans le châssis du commutateur de stockage et qu’il est entièrement opérationnel.
Défaillance des capteurs de température du commutateur MetroCluster	CRITIQUE	Le capteur du commutateur Fibre Channel est tombé en panne.	1) Vérifiez l’état de fonctionnement des capteurs de température sur le commutateur de stockage en utilisant la commande « storage switch show -cooling ». 2) Vérifiez que le commutateur fonctionne dans les conditions de température recommandées.
Température anormale du commutateur MetroCluster	CRITIQUE	Le capteur de température du commutateur Fibre Channel a signalé une température anormale.	1) Vérifiez l’état de fonctionnement des capteurs de température sur le commutateur de stockage en utilisant la commande « storage switch show -cooling ». 2) Vérifiez que le commutateur fonctionne dans les conditions de température recommandées.

Nom du moniteur	Gravité	Description du moniteur	Action corrective
Battement de cœur du processeur de service manqué	INFORMATIF	Ce message s'affiche lorsque ONTAP ne reçoit pas le signal « pulsation » attendu du processeur de service (SP). Parallèlement à ce message, les fichiers journaux du SP seront envoyés pour débogage. ONTAP réinitialisera le SP pour tenter de restaurer la communication. Le SP sera indisponible pendant deux minutes maximum pendant son redémarrage.	Contactez le support technique NetApp .
Arrêt du battement de cœur du processeur de service	AVERTISSEMENT	Ce message s'affiche lorsque ONTAP ne reçoit plus de pulsations du processeur de service (SP). Selon la conception matérielle, le système peut continuer à fournir des données ou décider de s'arrêter pour éviter toute perte de données ou tout dommage matériel. Le système continue de fournir des données, mais comme le SP ne fonctionne peut-être pas, le système ne peut pas envoyer de notifications d'appareils en panne, d'erreurs de démarrage ou d'erreurs de test automatique de mise sous tension (POST) du micrologiciel ouvert (OFW). Si votre système est configuré pour le faire, il génère et transmet un message AutoSupport (ou « appel à domicile ») au support technique NetApp et aux destinations configurées. La livraison réussie d'un message AutoSupport améliore considérablement la détermination et la résolution des problèmes.	Si le système s'est arrêté, essayez un cycle d'alimentation dur : retirez le contrôleur du châssis, remettez-le en place, puis rallumez le système. Contactez le support technique NetApp si le problème persiste après le cycle d'alimentation ou pour toute autre condition pouvant nécessiter une attention particulière.

Retour en haut

Plus d'informations

- "Affichage et suppression des alertes"

Notifications Webhook

Notification à l'aide de Webhooks

Les webhooks permettent aux utilisateurs d'envoyer des notifications d'alerte à diverses applications à l'aide d'un canal webhook personnalisé.

De nombreuses applications commerciales prennent en charge les webhooks comme interface d'entrée standard, par exemple : Slack, PagerDuty, Teams et Discord prennent tous en charge les webhooks. En prenant en charge un canal webhook générique et personnalisable, Data Infrastructure Insights peut prendre en charge bon nombre de ces canaux de diffusion. Des informations sur les webhooks peuvent être trouvées sur ces sites Web d'application. Par exemple, Slack fournit"ce guide utile" .

Vous pouvez créer plusieurs canaux webhook, chaque canal ciblant un objectif différent ; applications distinctes, destinataires différents, etc.

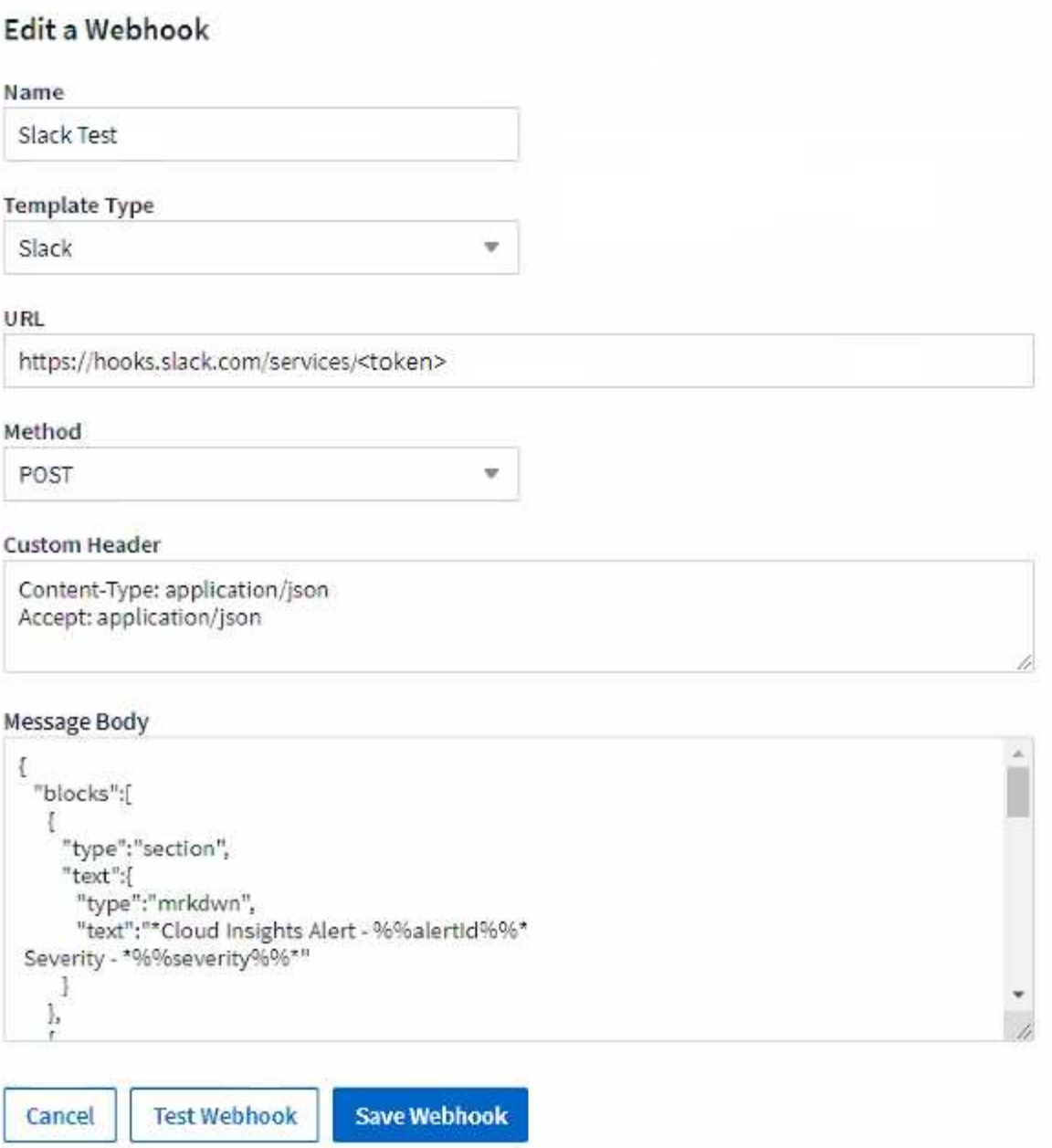
L'instance de canal webhook est composée des éléments suivants :

Nom	Nom unique
URL	URL cible du webhook, y compris le préfixe *http://* ou *https://* ainsi que les paramètres d'URL
Méthode	GET, POST - La valeur par défaut est POST
En-tête personnalisé	Spécifiez ici toutes les lignes d'en-tête personnalisées
Corps du message	Mettez le corps de votre message ici
Paramètres d'alerte par défaut	Répertorie les paramètres par défaut du webhook
Paramètres et secrets personnalisés	Les paramètres et secrets personnalisés vous permettent d'ajouter des paramètres uniques et des éléments sécurisés tels que des mots de passe

Créer un Webhook

Pour créer un webhook Data Infrastructure Insights , accédez à **Admin > Notifications** et sélectionnez l'onglet **Webhooks**.

L'image suivante montre un exemple de webhook configuré pour Slack :



Saisissez les informations appropriées pour chacun des champs et cliquez sur « Enregistrer » lorsque vous avez terminé.

Vous pouvez également cliquer sur le bouton « Tester le Webhook » pour tester la connexion. Notez que cela enverra le « Corps du message » (sans substitutions) à l'URL définie selon la méthode sélectionnée.

Les webhooks Data Infrastructure Insights comprennent un certain nombre de paramètres par défaut. De plus, vous pouvez créer vos propres paramètres ou secrets personnalisés.

Default Alert Parameters

Name	Description
%%alertDescription%%	Alert description
%%alertId%%	Alert ID
%%alertRelativeUrl%%	Relative URL to the Alert page. To build alert link use https://%%cloudInsightsHostName%%%%alertRelativeUrl%%
%%metricName%%	Monitored metric
%%monitorName%%	Monitor name
%%objectType%%	Monitored object type
%%severity%%	Alert severity level
%%alertCondition%%	Alert condition
%%triggerTime%%	Alert trigger time in GMT ('Tue, 27 Oct 2020 01:20:30 GMT')
%%triggerTimeEpoch%%	Alert trigger time in Epoch format (milliseconds)
%%triggeredOn%%	Triggered On (key:value pairs separated by commas)
%%value%%	Metric value that triggered the alert
%%cloudInsightsLogoUrl%%	Cloud Insights logo URL
%%cloudInsightsHostname%%	Cloud Insights Hostname (concatenate with relative URL to build alert link)

Custom Parameters and Secrets

Name	Value	Description
No Data Available		

+ Parameter

Paramètres : que sont-ils et comment les utiliser ?

Les paramètres d'alerte sont des valeurs dynamiques renseignées par alerte. Par exemple, le paramètre *%%TriggeredOn%%* sera remplacé par l'objet sur lequel l'alerte a été déclenchée.

Vous pouvez ajouter n'importe quel attribut d'objet (par exemple, le nom de stockage) en tant que paramètre à un webhook. Par exemple, vous pouvez définir des paramètres pour le nom du volume et le nom du stockage dans une description de webhook comme : « Latence élevée pour le volume : *%%relatedObject.volume.name%%*, Stockage : *%%relatedObject.storage.name%%* ».

Notez que dans cette section, les substitutions ne sont *pas* effectuées lorsque vous cliquez sur le bouton « Tester le Webhook » ; le bouton envoie une charge utile qui affiche les *%%* substitutions mais ne les remplace pas par des données.

Paramètres et secrets personnalisés

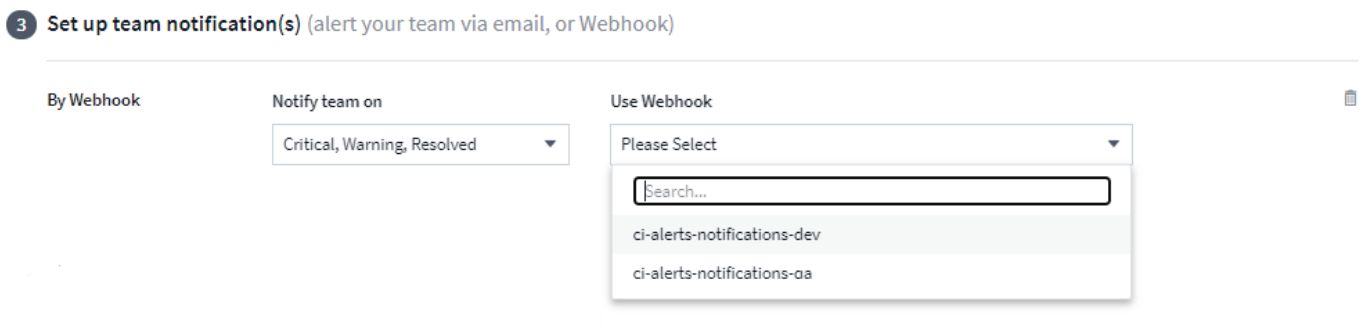
Dans cette section, vous pouvez ajouter tous les paramètres personnalisés et/ou secrets que vous souhaitez. Pour des raisons de sécurité, si un secret est défini, seul le créateur du webhook peut modifier ce canal de webhook. Il est en lecture seule pour les autres. Vous pouvez utiliser des secrets dans les URL/en-têtes comme *%%<secret_name>%%*.

Page de liste des Webhooks

Sur la page de liste des Webhooks, les champs Nom, Créé par, Créé le, Statut, Sécurisé et Dernier signalement sont affichés.

Choisir une notification Webhook dans un moniteur

Pour choisir la notification webhook dans un"moniteur" , allez dans **Alertes > Gérer les moniteurs** et sélectionnez le moniteur souhaité ou ajoutez un nouveau moniteur. Dans la section *Configurer les notifications d'équipe*, choisissez *Webhook* comme méthode de livraison. Sélectionnez les niveaux d'alerte (Critique, Avertissement, Résolu), puis choisissez le webhook souhaité.



Exemples de webhooks :

Webhooks pour"Mou" Webhooks pour"PagerDuty" Webhooks pour"Équipes" Webhooks pour"Discorde"

Exemple de webhook pour Discord

Les webhooks permettent aux utilisateurs d'envoyer des notifications d'alerte à diverses applications à l'aide d'un canal webhook personnalisé. Cette page fournit un exemple de configuration de webhooks pour Discord.

Cette page fait référence à des instructions de tiers, qui peuvent être sujettes à modification. Reportez-vous à la"Documentation Discord" pour les informations les plus récentes.

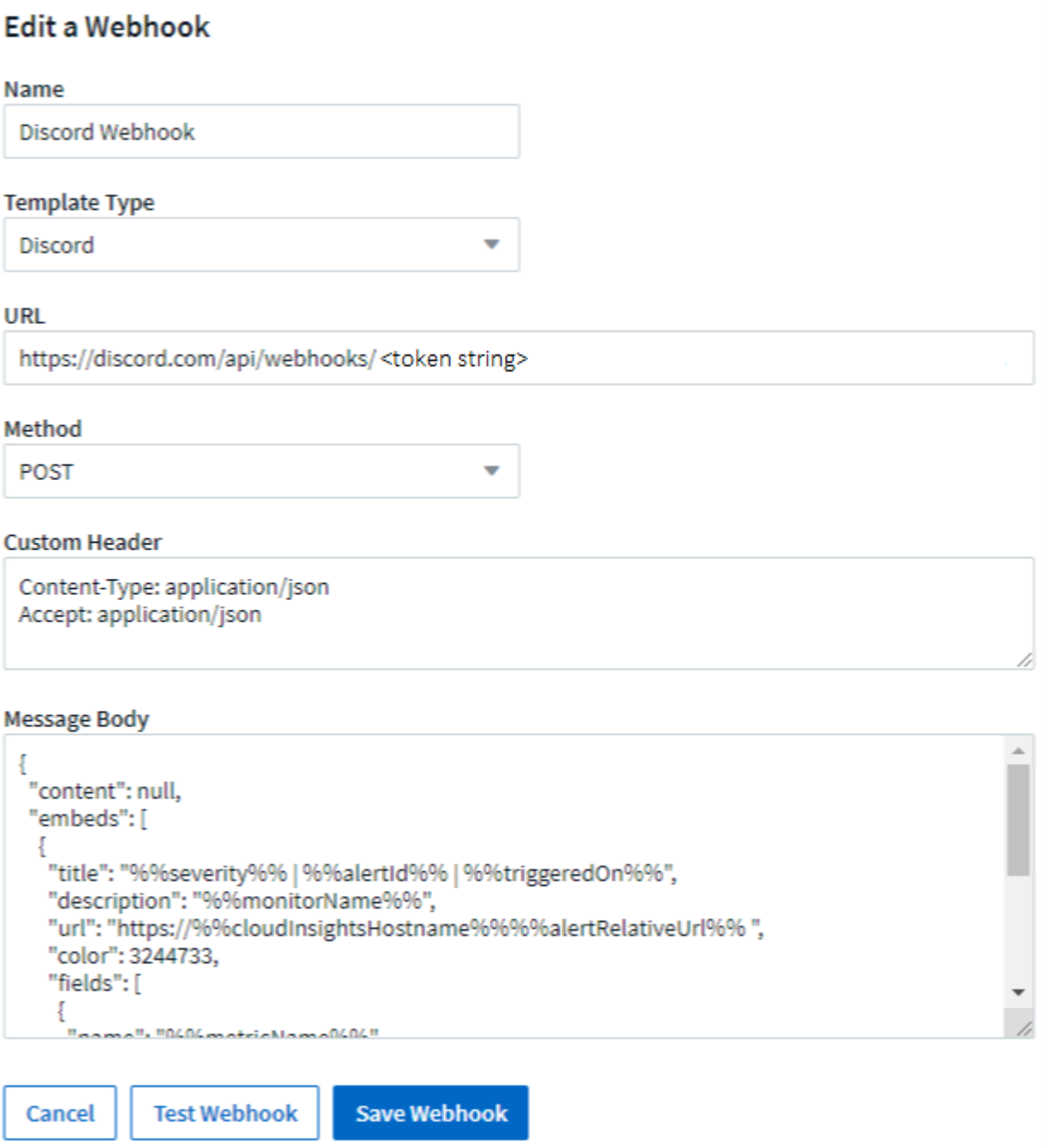
Configuration de Discord :

- Dans Discord, sélectionnez le serveur, sous Canaux texte, sélectionnez Modifier le canal (icône en forme d'engrenage)
- Sélectionnez **Intégrations > Afficher les webhooks** et cliquez sur **Nouveau webhook**

- Copiez l'URL du Webhook. Vous devrez coller ceci dans la configuration du webhook Data Infrastructure Insights .

Créer un webhook Data Infrastructure Insights :

1. Dans Data Infrastructure Insights, accédez à **Admin > Notifications** et sélectionnez l'onglet **Webhooks**. Cliquez sur **+Webhook** pour créer un nouveau webhook.
2. Donnez au webhook un nom significatif, tel que « Discord ».
3. Dans la liste déroulante *Type de modèle*, sélectionnez **Discord**.
4. Collez l'URL ci-dessus dans le champ *URL*.

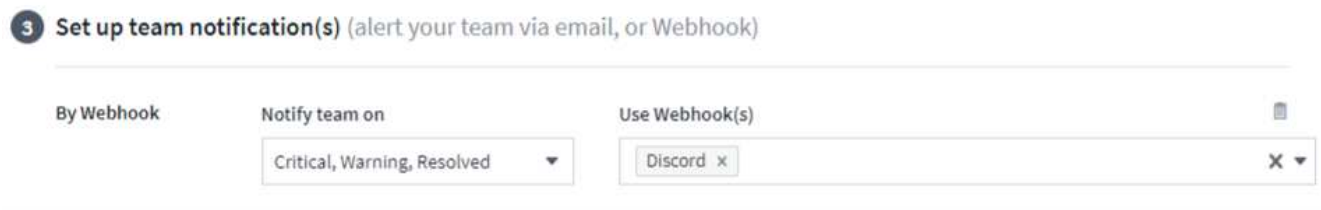


Afin de tester le webhook, remplacez temporairement la valeur de l'URL dans le corps du message par n'importe quelle URL valide (telle que *https://netapp.com*), puis cliquez sur le bouton *Tester le Webhook*. Assurez-vous de réinitialiser le corps du message une fois le test terminé.

Notifications via Webhook

Pour notifier des événements via un webhook, dans Data Infrastructure Insights, accédez à **Alertes > Moniteurs** et cliquez sur **+Moniteur** pour créer un nouveau"moniteur" .

- Sélectionnez une métrique et définissez les conditions du moniteur.
- Sous *Configurer les notifications d'équipe*, choisissez la méthode de livraison **Webhook**.
- Choisissez le webhook « Discord » pour les événements souhaités (Critique, Avertissement, Résolu)



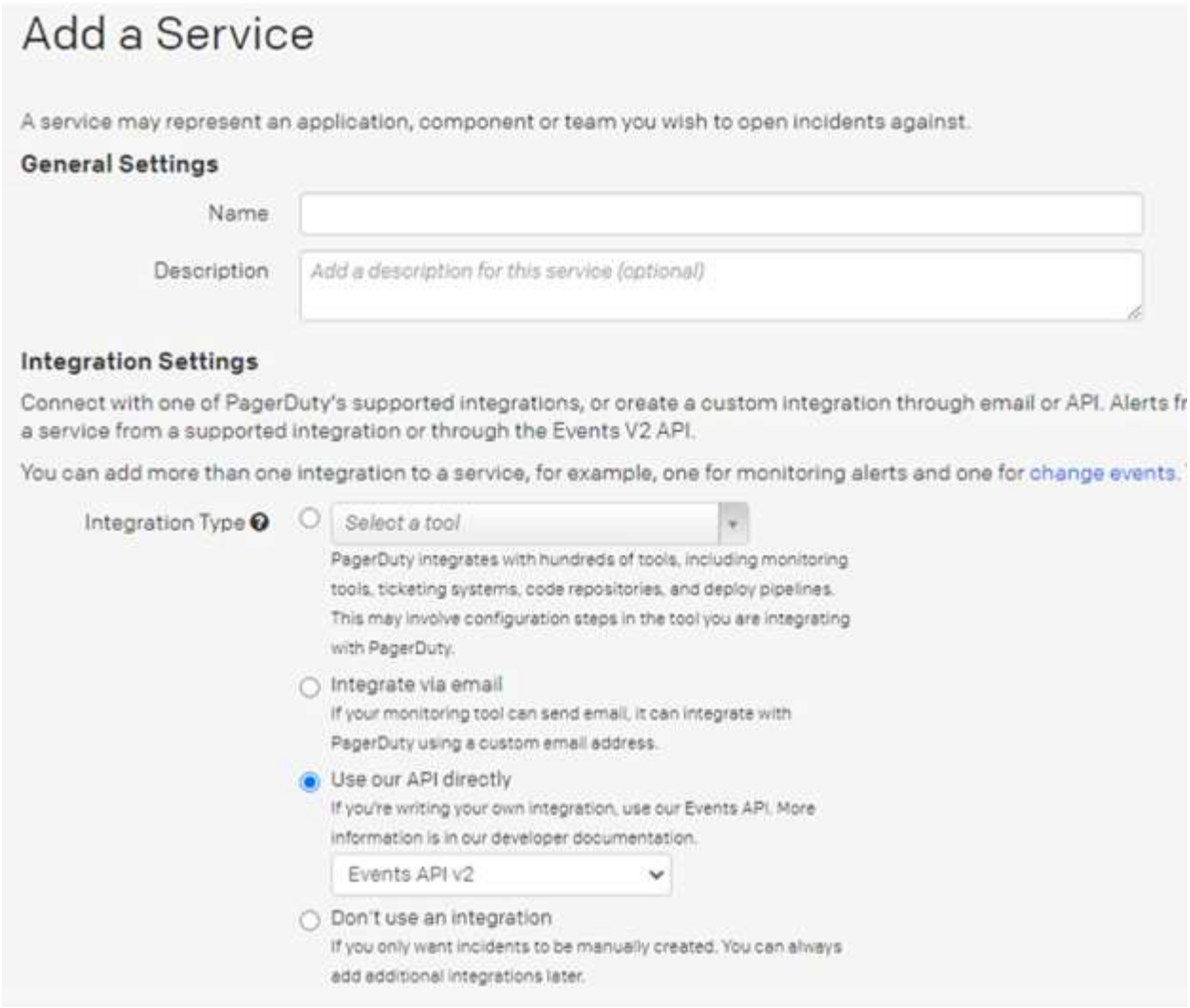
Exemple de webhook pour PagerDuty

Les webhooks permettent aux utilisateurs d'envoyer des notifications d'alerte à diverses applications à l'aide d'un canal webhook personnalisé. Cette page fournit un exemple de configuration de webhooks pour PagerDuty.

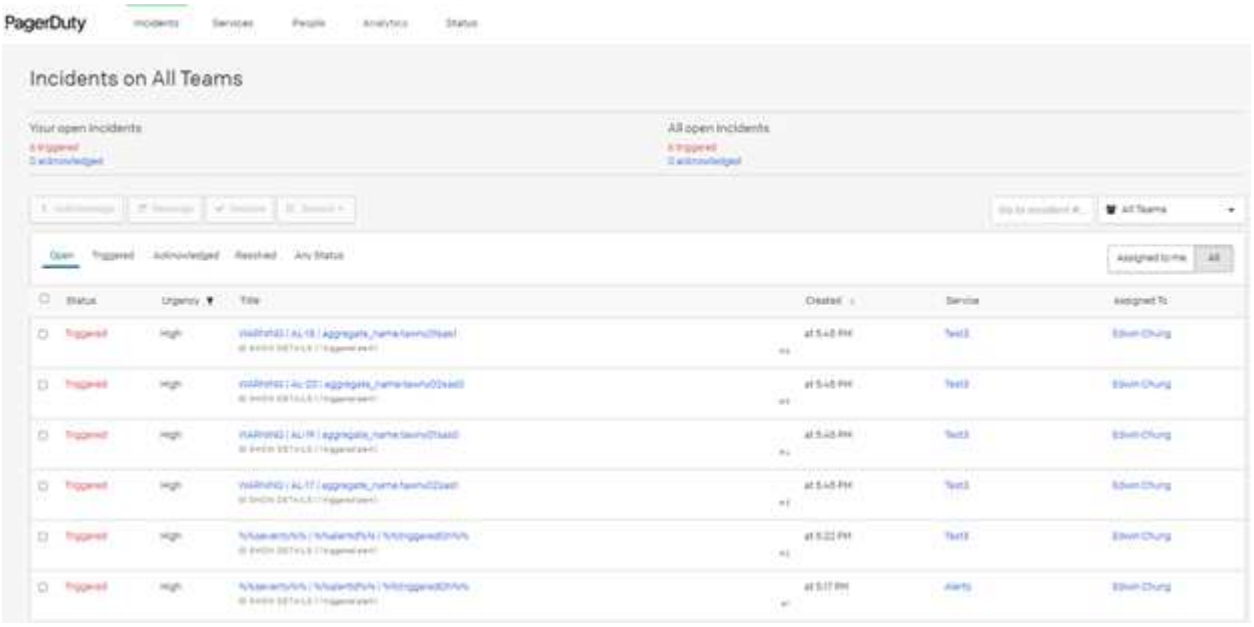
Cette page fait référence à des instructions de tiers, qui peuvent être sujettes à modification. Reportez-vous à la"Documentation de PagerDuty" pour les informations les plus récentes.

Configuration de PagerDuty :

1. Dans PagerDuty, accédez à **Services > Répertoire des services** et cliquez sur le bouton **+Nouveau service**
2. Saisissez un *Nom* et sélectionnez *Utiliser directement notre API*. Cliquez sur *Ajouter un service*.

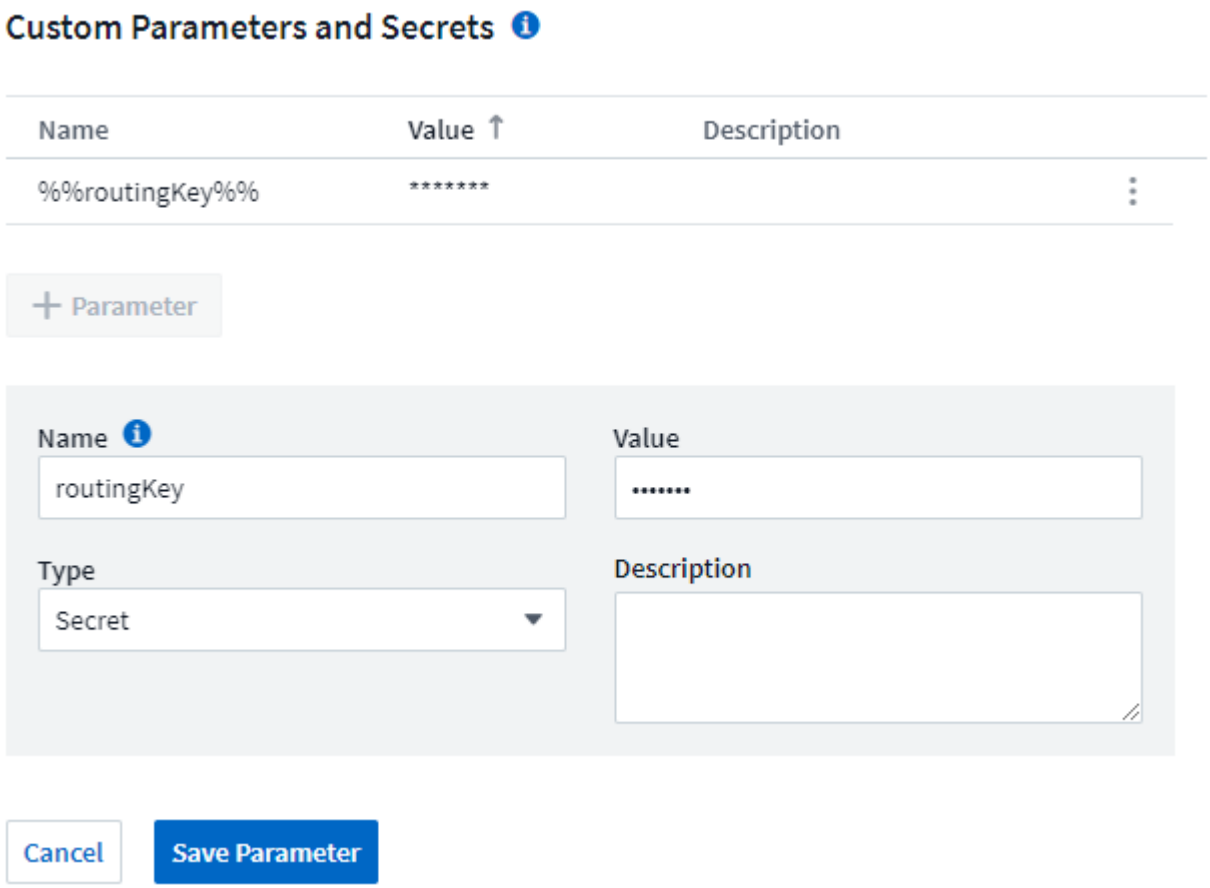


3. Cliquez sur l'onglet *Intégrations* pour voir la **Clé d'intégration**. Vous aurez besoin de cette clé lorsque vous créerez le webhook Data Infrastructure Insights ci-dessous.
4. Accédez à **Incidents** ou **Services** pour afficher les alertes.



Créer un webhook Data Infrastructure Insights :

1. Dans Data Infrastructure Insights, accédez à **Admin > Notifications** et sélectionnez l'onglet **Webhooks**. Cliquez sur **+Webhook** pour créer un nouveau webhook.
2. Donnez au webhook un nom significatif, tel que « Déclencheur PagerDuty ». Vous utiliserez ce webhook pour les événements de niveau critique et d'avertissement.
3. Dans la liste déroulante *Type de modèle*, sélectionnez **PagerDuty**.
4. Créez un secret de paramètre personnalisé nommé *routingKey* et définissez la valeur sur la valeur PagerDuty *Integration Key* ci-dessus.



Répétez ces étapes pour créer un webhook « PagerDuty Resolve » pour les événements résolus.

PagerDuty vers les Data Infrastructure Insights, cartographie des champs

Le tableau et l'image suivants montrent le mappage des champs entre PagerDuty et Data Infrastructure Insights:

PagerDuty	Data Infrastructure Insights
Touche d'alerte	ID d'alerte
Source	Déclenché sur
Composant	Nom métrique
Groupe	Type d'objet

PagerDuty	Data Infrastructure Insights
Classe	Nom du moniteur

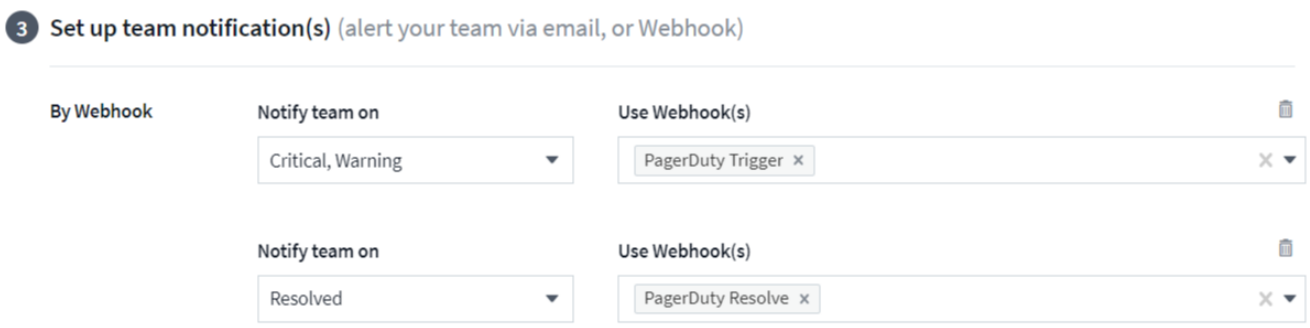
Message Body

```
{
 "dedup_key": "%%alertId%%",
 "event_action": "trigger",
 "links": [
  {
   "href": "https://%%cloudInsightsHostname%%%%alertRelativeUrl%%",
   "text": "'%%metricName%%' value of %%value%% (%%alertCondition%%) for
%%triggeredOn%%"
  }
 ],
 "payload": {
  "class": "%%monitorName%%",
  "component": "%%metricName%%",
  "group": "%%objectType%%",
  "severity": "critical",
  "source": "%%triggeredOn%%",
  "summary": "%%severity%% | %%alertId%% | %%triggeredOn%%"
 },
 "routing_key": "%%routingKey%%"
}
```

Notifications via Webhook

Pour notifier des événements via un webhook, dans Data Infrastructure Insights, accédez à **Alertes > Moniteurs** et cliquez sur **+Moniteur** pour créer un nouveau"moniteur" .

- Sélectionnez une métrique et définissez les conditions du moniteur.
- Sous *Configurer les notifications d'équipe*, choisissez la méthode de livraison **Webhook**.
- Choisissez le webhook « PagerDuty Trigger » pour les événements de niveau critique et d'avertissement.
- Choisissez « PagerDuty Resolve » pour les événements résolus.



La définition de notifications distinctes pour les événements déclencheurs et les événements résolus est une bonne pratique, car PagerDuty gère les événements déclencheurs différemment des événements résolus.

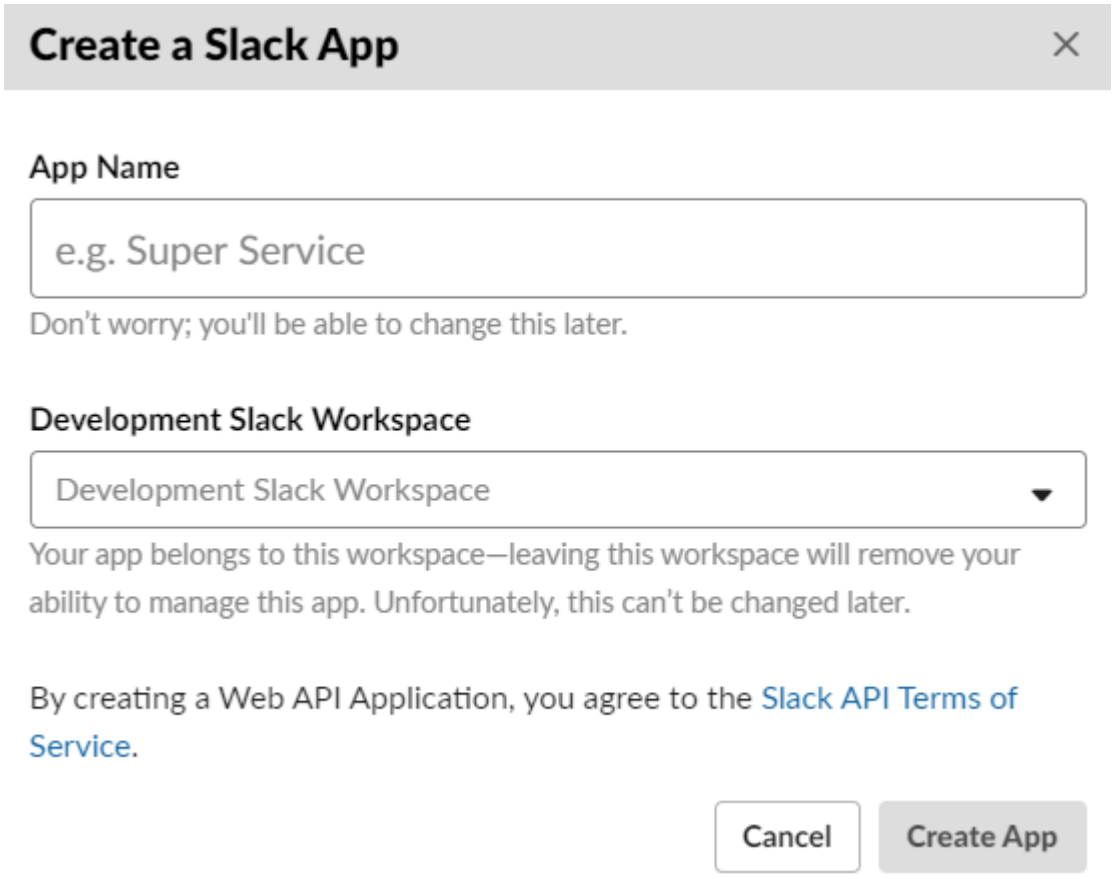
Exemple de webhook pour Slack

Les webhooks permettent aux utilisateurs d'envoyer des notifications d'alerte à diverses applications à l'aide d'un canal webhook personnalisé. Cette page fournit un exemple de configuration de webhooks pour Slack.

Cette page fait référence à des instructions de tiers, qui peuvent être sujettes à modification. Reportez-vous à la"Documentation Slack" pour les informations les plus récentes.

Exemple de Slack :

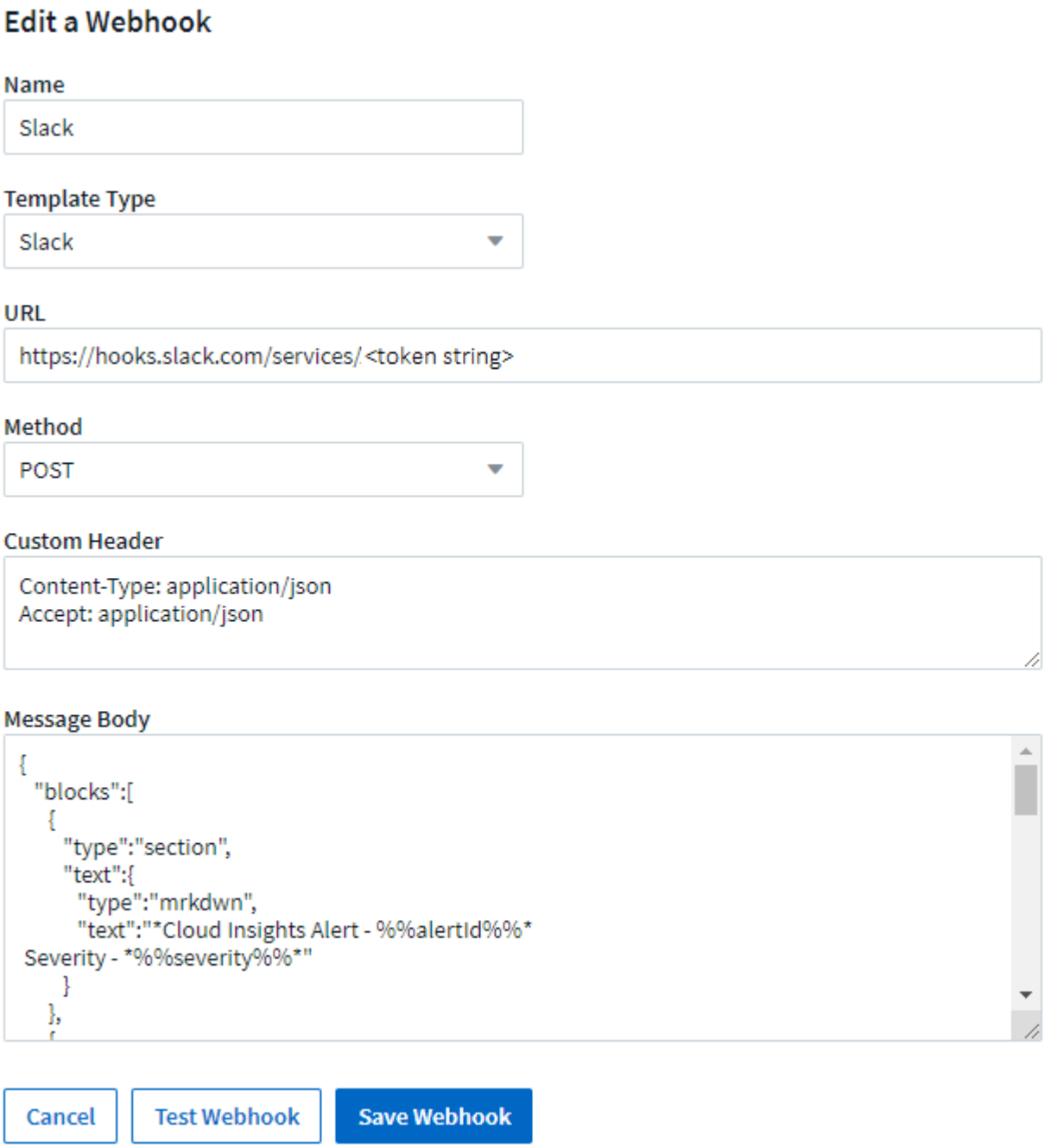
- Aller à https://api.slack.com/apps et créez une nouvelle application. Donnez-lui un nom significatif et sélectionnez l'espace de travail Slack.



- Accédez à Webhooks entrants, cliquez sur *Activer les Webhooks entrants*, Demander à *Ajouter un nouveau Webhook* et sélectionnez le canal sur lequel publier.
- Copiez l'URL du Webhook. Vous devrez coller ceci dans la configuration du webhook Data Infrastructure Insights .

Créer un webhook Data Infrastructure Insights :

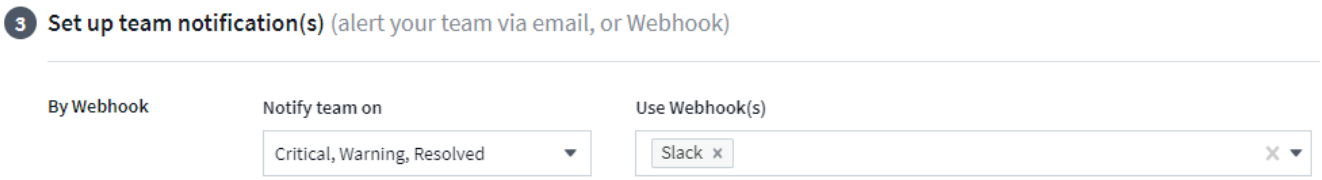
1. Dans Data Infrastructure Insights, accédez à **Admin > Notifications** et sélectionnez l'onglet **Webhooks**. Cliquez sur **+Webhook** pour créer un nouveau webhook.
2. Donnez au webhook un nom significatif, tel que « Slack Webhook ».
3. Dans la liste déroulante *Type de modèle*, sélectionnez **Slack**.
4. Collez l'URL ci-dessus dans le champ *URL*.



Notifications via Webhook

Pour notifier des événements via un webhook, dans Data Infrastructure Insights, accédez à **Alertes > Moniteurs** et cliquez sur **+Moniteur** pour créer un nouveau"moniteur" .

- Sélectionnez une métrique et définissez les conditions du moniteur.
- Sous *Configurer les notifications d'équipe*, choisissez la méthode de livraison **Webhook**.
- Choisissez le webhook « Slack » pour les événements souhaités (Critique, Avertissement, Résolu)



Plus d'informations :

- Pour modifier le format et la mise en page du message, voir https://api.slack.com/messaging/composing
- Gestion des erreurs : https://api.slack.com/messaging/webhooks#handling_errors

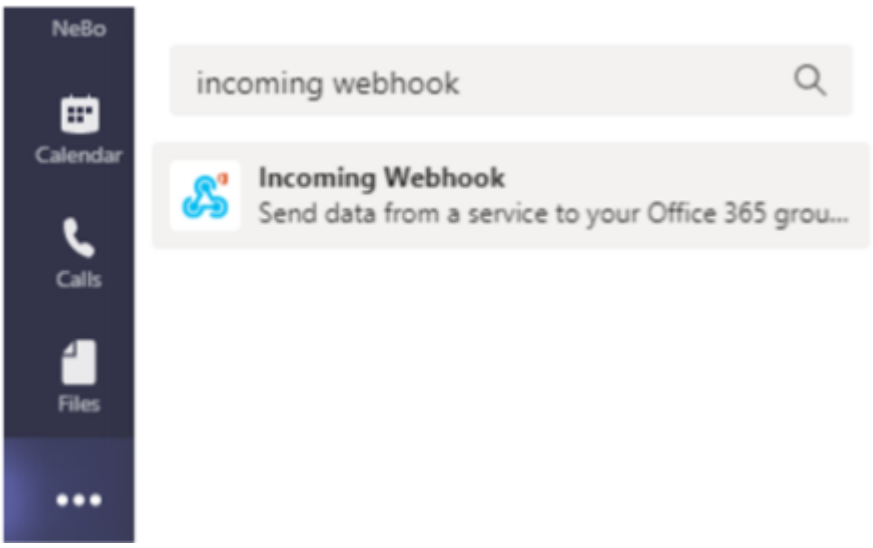
Exemple de webhook pour Microsoft Teams

Les webhooks permettent aux utilisateurs d'envoyer des notifications d'alerte à diverses applications à l'aide d'un canal webhook personnalisé. Cette page fournit un exemple de configuration de webhooks pour Teams.

Cette page fait référence à des instructions de tiers, qui peuvent être sujettes à modification. Reportez-vous à la"Documentation des équipes" pour les informations les plus récentes.

Configuration des équipes :

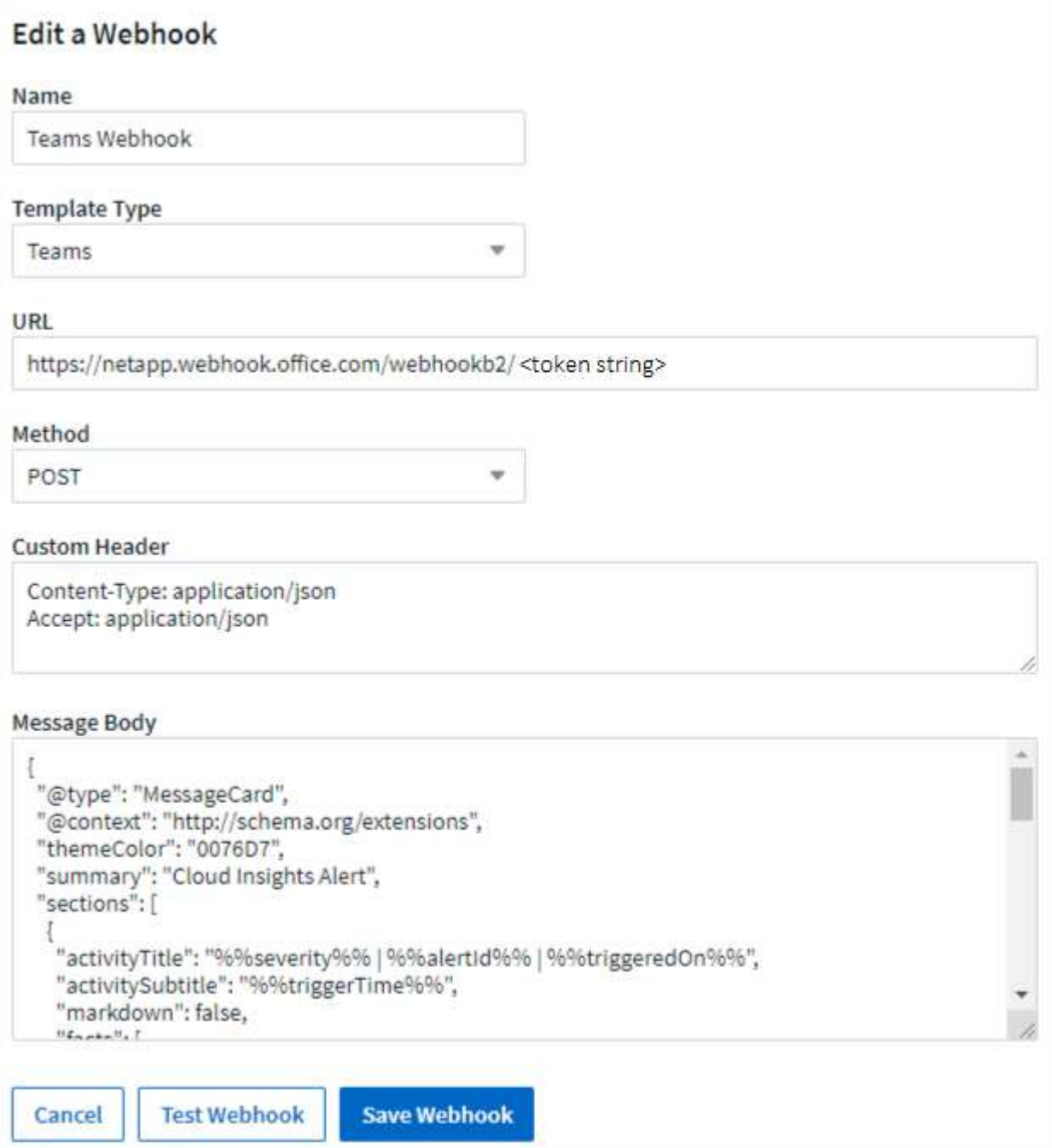
1. Dans Teams, sélectionnez le kebab et recherchez Webhook entrant.



2. Sélectionnez **Ajouter à une équipe > Sélectionner une équipe > Configurer un connecteur**.
3. Copiez l'URL du Webhook. Vous devrez coller ceci dans la configuration du webhook Data Infrastructure Insights .

Créer un webhook Data Infrastructure Insights :

1. Dans Data Infrastructure Insights, accédez à **Admin > Notifications** et sélectionnez l'onglet **Webhooks**. Cliquez sur **+Webhook** pour créer un nouveau webhook.
2. Donnez au webhook un nom significatif, tel que « Webhook Équipes ».
3. Dans la liste déroulante *Type de modèle*, sélectionnez **Équipes**.



1. Collez l'URL ci-dessus dans le champ *URL*.

Notifications via Webhook

Pour notifier des événements via un webhook, dans Data Infrastructure Insights, accédez à **Alertes > Moniteurs** et cliquez sur **+Moniteur** pour créer un nouveau"moniteur" .

- Sélectionnez une métrique et définissez les conditions du moniteur.
- Sous *Configurer les notifications d'équipe*, choisissez la méthode de livraison **Webhook**.
- Choisissez le webhook « Équipes » pour les événements souhaités (Critique, Avertissement, Résolu)