Surveille et alerte

Cloud Insights

NetApp
April 16, 2024

This PDF was generated from https://docs.netapp.com/fr-fr/cloudinsights/task_create_monitor.html on April 16, 2024. Always check docs.netapp.com for the latest.

Sommaire

Surveille et alerte 1
Alertes avec les moniteurs 1
Affichage et gestion des alertes à partir des moniteurs 9
Configuration des notifications par e-mail 12
Moniteurs système 14

Surveille et alerte

Alertes avec les moniteurs

Vous créez des moniteurs pour définir des seuils qui déclenchent des alertes pour vous informer des problèmes liés aux ressources de votre réseau. Par exemple, vous pouvez créer un moniteur pour signaler la latence d'écriture *node* pour n'importe lequel d'une multitude de protocoles.

Les moniteurs et alertes sont disponibles dans toutes les éditions Cloud Insights. Cependant, l'édition de base est soumise aux conditions suivantes : * vous ne pouvez avoir que cinq moniteurs personnalisés actifs à la fois. Tous les moniteurs au-delà de cinq seront créés ou déplacés à l'état *Pause*. * Les moniteurs de metrics VMDK, Virtual machine, Host et DataStore ne sont pas pris en charge. Si des moniteurs ont été créés pour ces mesures, ils seront mis en pause et ne peuvent pas être repris lors de la rétrogradation vers l'édition de base.

Les moniteurs vous permettent de définir des seuils sur les metrics générés par des objets d'infrastructure tels que le stockage, les serveurs virtuels, EC2 et les ports, ainsi que pour les données « intégration », telles que celles collectées pour Kubernetes, les metrics avancés ONTAP et les plug-ins Telegraf. Ces *mesures* permettent de vous alerter lorsque les seuils de niveau d'avertissement ou de niveau critique sont croisés.

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

Cloud Insights fournit un certain nombre de "Moniteurs définis par le système" ainsi, en fonction de votre environnement.

Meilleures pratiques en matière de sécurité

Les alertes Cloud Insights mettent en évidence les points de données et les tendances dans votre environnement. Cloud 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 la personne qui reçoit la notification ou a accès à l'alerte.

Moniteur de mesures ou de journaux ?

1. Dans le menu Cloud Insights, cliquez sur **alertes > gérer les moniteurs**

   La page de liste moniteurs s'affiche et affiche les moniteurs actuellement configurés.

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

Lorsque vous ajoutez un nouveau moniteur, vous êtes invité à créer un moniteur métrique ou un moniteur de journal.

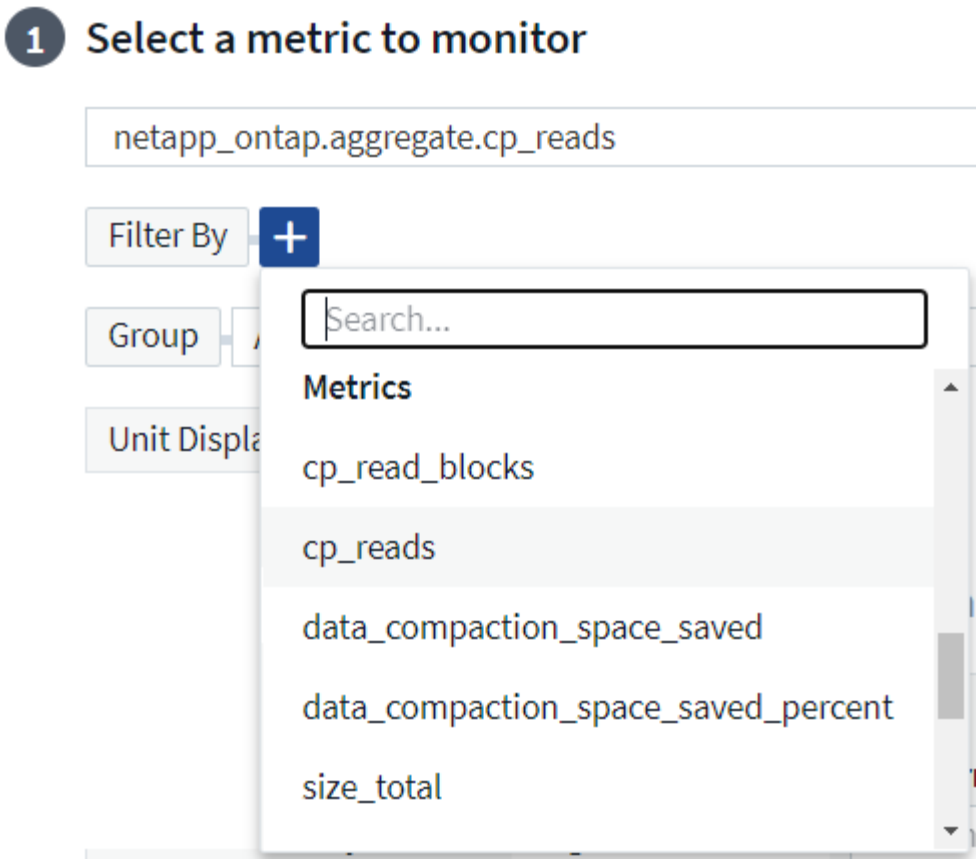
- *Metric* surveille l'alerte sur les déclencheurs liés à l'infrastructure ou aux performances
- *Log* surveille l'alerte sur l'activité liée au journal

Après avoir sélectionné 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 mesure à surveiller.

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



Lors de l'utilisation des données d'intégration (Kubernetes, ONTAP Advanced Data, etc.), le filtrage des mesures supprime les points de données individuels/non inégalés 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 peuvent potentiellement supprimer l'objet entier du graphique.

Pour créer un moniteur multicondition (par exemple, IOPS > X et latence > y), définissez la première condition comme un seuil et la deuxième condition comme un filtre.

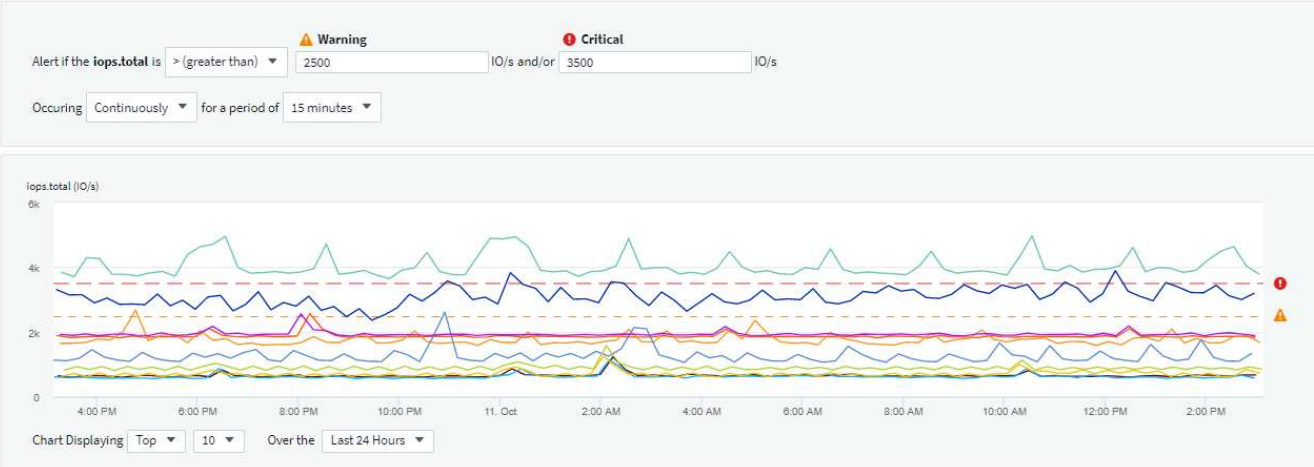
Définissez les conditions du moniteur.

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

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

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

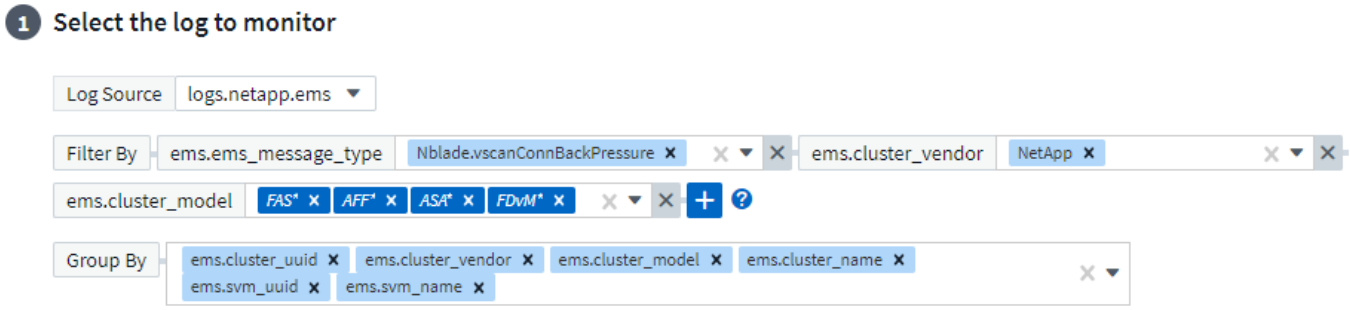
   Vous pouvez choisir de déclencher une alerte au moment où un seuil est atteint ou d'attendre que le seuil ait été atteint pendant un certain temps. Dans notre exemple, nous ne voulons pas être alerté chaque fois que le nombre total d'IOPS est supérieur au niveau Avertissement ou critique, mais uniquement lorsqu'un objet surveillé dépasse en permanence l'un de ces niveaux pendant au moins 15 minutes.



Surveillance des journaux

Lors de la création d'un moniteur **Log Monitor**, 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 de surveillance du journal ne peut pas être vide.



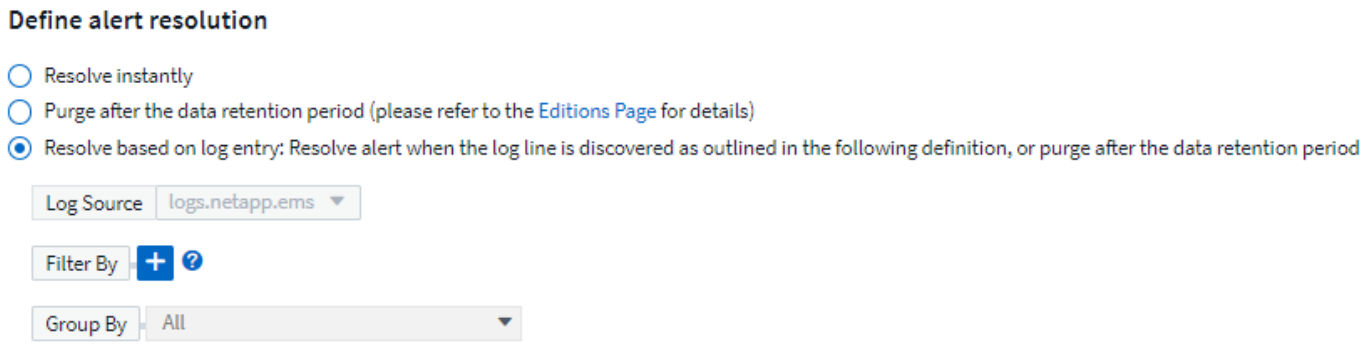
Définir le comportement de l'alerte

Vous pouvez créer le moniteur pour qu'il vous alerte avec un niveau de gravité de *critique*, *Avertissement* ou *information*, lorsque les conditions définies ci-dessus se produisent une fois (c'est-à-dire immédiatement), ou attendre que les conditions se produisent 2 fois ou plus.

Définir le comportement de résolution d'alerte

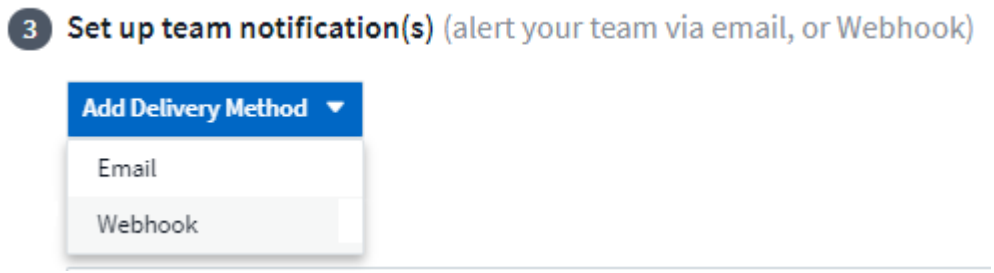
Vous pouvez choisir la façon dont une alerte de surveillance de journal est résolue. Trois choix sont proposés :

- Résolution instantanée
- Purger après la période de conservation des données (reportez-vous à la page Editions pour plus de détails). Notez que le moniteur n'a pas de condition de résolution par définition. Une alerte restera donc *active* et supprimera toutes les alertes suivantes avec *group_by* correspondant générées par ce moniteur, jusqu'à ce que la période de conservation des données soit terminée.
- Résoudre en fonction de l'entrée de journal : résoudre l'alerte lorsque la ligne de journal est découverte comme indiqué dans la définition suivante, ou purger après la période de conservation des données.



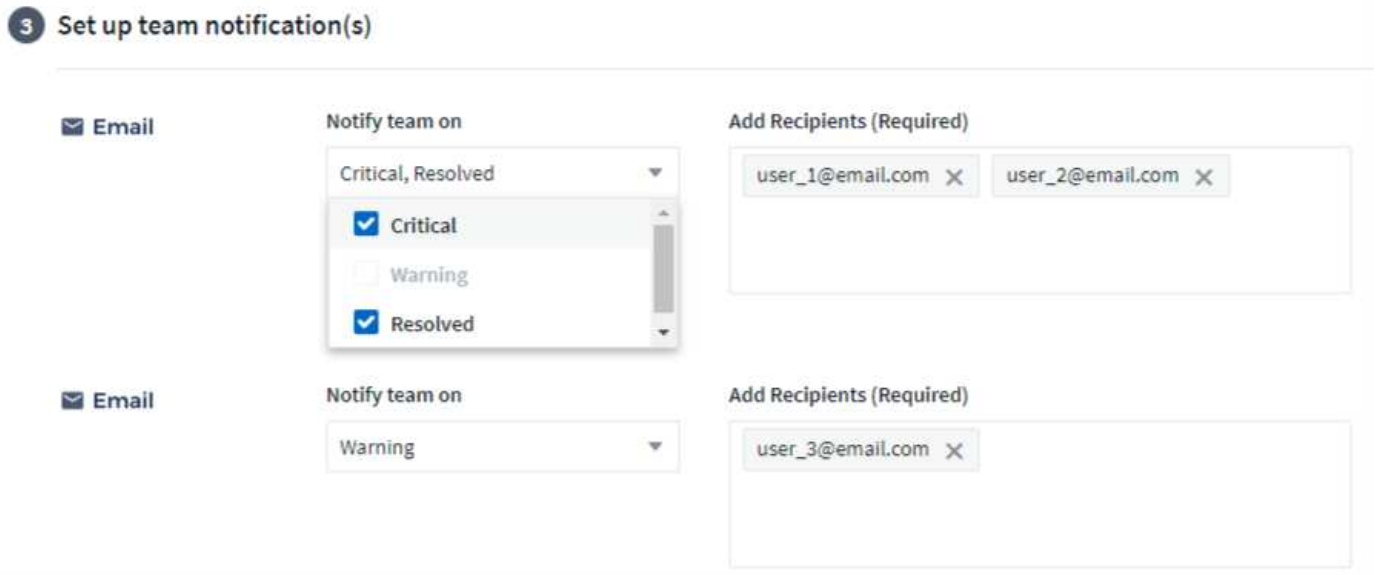
Sélectionnez le type de notification et les destinataires

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



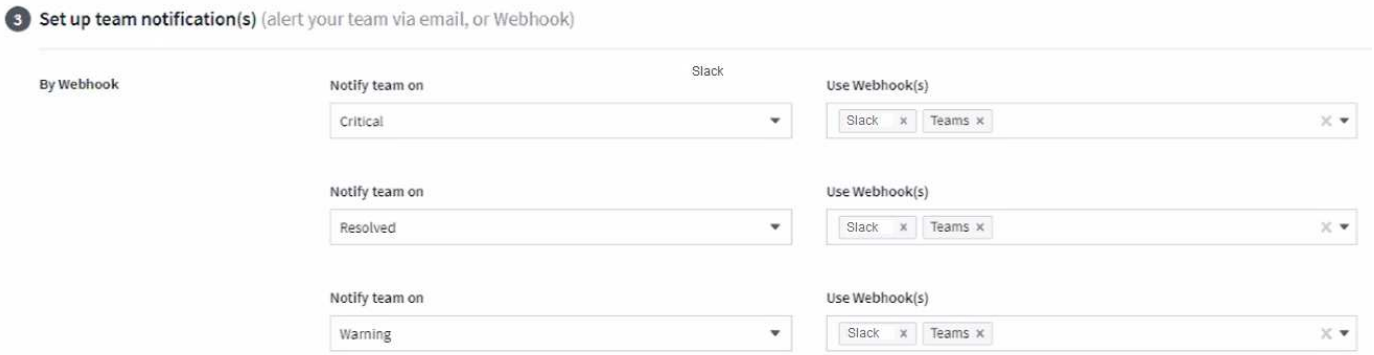
Alertes par e-mail:

Spécifiez les destinataires de l'e-mail pour les notifications d'alerte. Si vous le souhaitez, vous pouvez choisir différents destinataires pour les alertes d'avertissement ou critiques.



Alertes via Webhook:

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

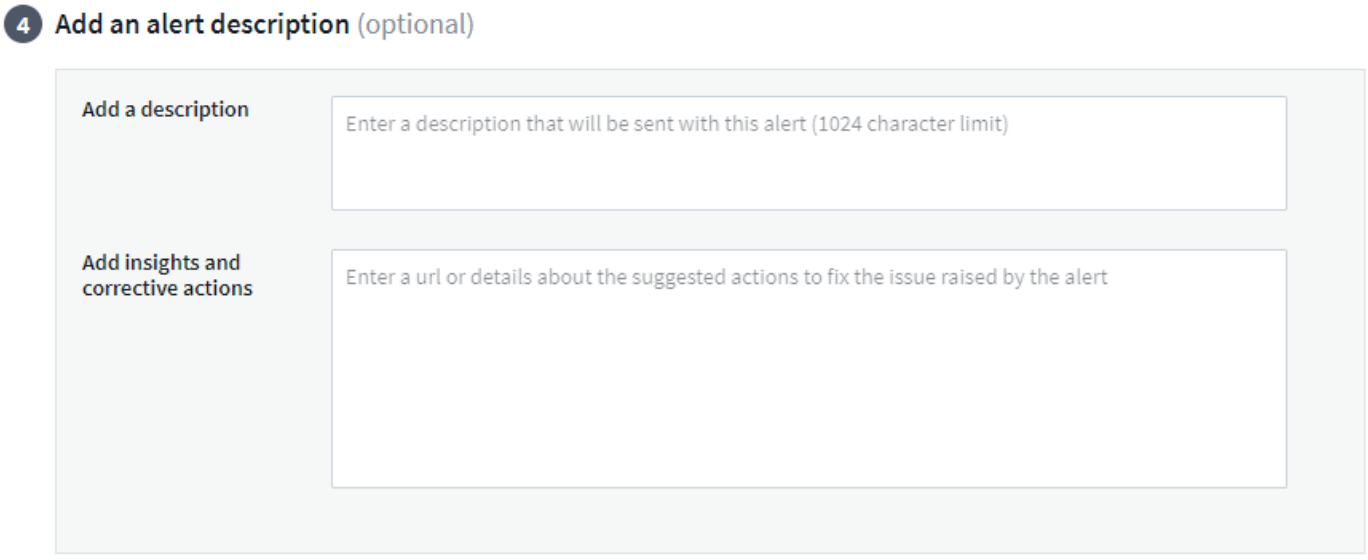


Les notifications ONTAP Data Collector prévalent sur toute notification Monitor spécifique pertinente au cluster/Data Collector. La liste des destinataires que vous définissez pour le Data Collector lui-même recevra les alertes du Data Collector. Si aucune alerte de collecte de données n'est active, des 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 comporter jusqu'à 1024 caractères et sera envoyée avec l'alerte. Le champ d'action corrective peut contenir jusqu'à 67,000 caractères et sera affiché dans la section récapitulative de la page d'accueil de l'alerte.

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



Enregistrez votre moniteur

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

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

Liste des moniteurs

La page Monitor répertorie les moniteurs actuellement configurés, avec les informations suivantes :

- Nom du moniteur
- État
- Objet/mesure surveillé
- Conditions du moniteur

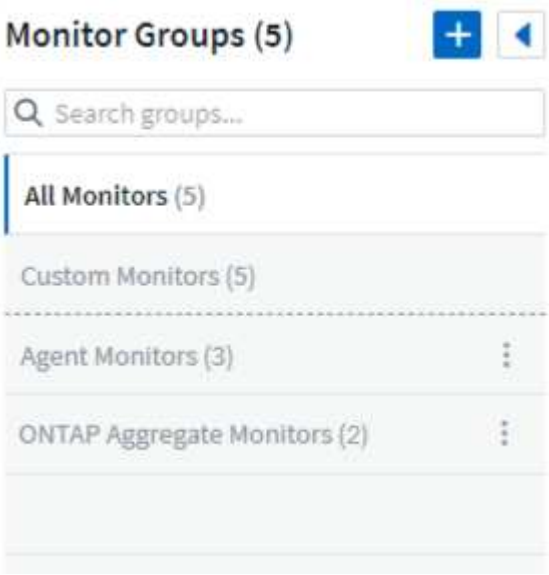
Vous pouvez choisir de suspendre temporairement la surveillance d'un type d'objet en cliquant sur le menu à droite du moniteur et en sélectionnant **Pause**. Lorsque vous êtes prêt à reprendre la surveillance, cliquez sur **reprendre**.

Vous pouvez copier un moniteur en sélectionnant **Dupliquer** dans le menu. Vous pouvez ensuite modifier le nouveau moniteur et modifier l'objet/la mesure, le filtre, les conditions, les destinataires de l'e-mail, 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 moniteurs dédié au stockage de votre environnement ou de moniteurs pertinents à une liste de destinataires donnée.



Les groupes de moniteurs suivants sont affichés. Le nombre de moniteurs contenus dans un groupe s'affiche en regard 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 Cloud Insights.
- Cloud Insights affiche également un certain nombre de **groupes de moniteurs système**, qui répertorieront un ou plusieurs groupes de "moniteurs définis par le système", Y compris les moniteurs de charge de travail et d'infrastructure ONTAP.

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

Moniteurs suspendus

Ce groupe s'affiche uniquement si Cloud 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 des moniteurs suspendus lorsque le problème à l'origine de la suspension est résolu.

Moniteurs définis par le système

Ces groupes affichent les moniteurs fournis par Cloud Insights, tant que votre environnement contient les périphériques et/ou la disponibilité du journal 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, volumes, etc.) ou pour les charges de travail (moniteurs de journaux), ou pour d'autres groupes. NetApp évalue en permanence les besoins des clients et les fonctionnalités des produits et les met à jour ou ajoute aux contrôles système et aux groupes 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 pouvez souhaiter créer un groupe pour tous vos moniteurs de stockage.

Pour créer un nouveau groupe de moniteurs personnalisé, cliquez sur le bouton **"+" Créer un nouveau groupe de moniteurs**. Entrez 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*.

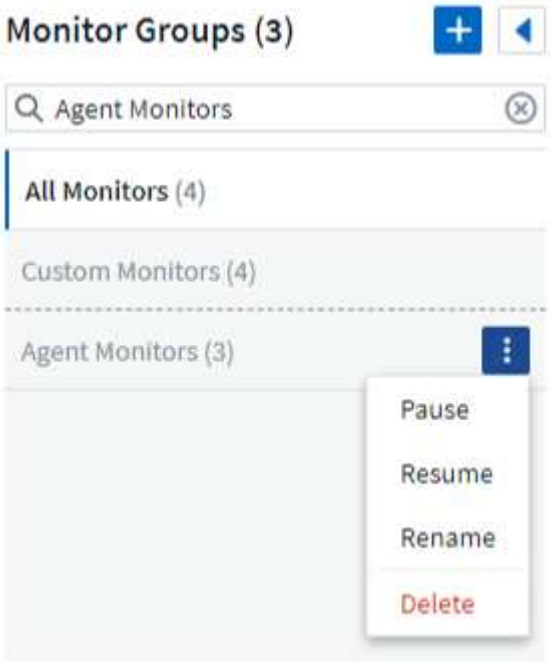
Supprimer les moniteurs en cliquant sur un groupe et en sélectionnant *Supprimer du groupe* dans le menu. Vous ne pouvez pas supprimer de moniteurs du groupe *tous les moniteurs* ou *moniteurs personnalisés*. Pour supprimer un moniteur de ces groupes, vous devez le supprimer lui-même.

La suppression d'un moniteur d'un groupe ne supprime pas le moniteur de Cloud Insights. Pour supprimer complètement un moniteur, sélectionnez-le et cliquez sur *Delete*. Ceci le supprime également du groupe auquel il appartenait et n'est plus disponible pour aucun utilisateur.

Vous pouvez également déplacer un moniteur vers un autre groupe de la même manière, en sélectionnant *Move to Group*.

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 Cloud Insights ; ils sont toujours disponibles dans *tous les moniteurs*.



Moniteurs définis par le système

Cloud Insights inclut un certain nombre de contrôles définis par le système, à la fois pour les metrics et les journaux. Les moniteurs système disponibles dépendent des collecteurs de données présents dans votre environnement. De ce fait, les moniteurs disponibles dans Cloud Insights peuvent changer à mesure que des collecteurs de données sont ajoutés ou que leurs configurations ont changé.

Afficher le "Moniteurs définis par le système" Pour obtenir des descriptions des moniteurs inclus avec Cloud Insights.

Plus d'informations

- "Affichage et rejet des alertes"

Affichage et gestion des alertes à partir des moniteurs

Cloud Insights affiche les alertes lorsque "seuils surveillés" sont dépassées.

Les moniteurs et alertes sont disponibles dans Cloud 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 des 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 « vitesse » :
   - **ID d'alerte** : ID d'alerte unique généré par le système
   - **Déclenché Time** : heure à laquelle le moniteur concerné a déclenché l'alerte
   - **Gravité actuelle** (onglet alertes actives) : gravité actuelle de l'alerte active
   - **Gravité supérieure** (onglet alertes résolues); gravité maximale de l'alerte avant sa résolution
   - **Moniteur** : moniteur configuré pour déclencher l'alerte
   - **Déclenché le** : objet sur lequel le seuil surveillé a été dépassé
   - **État** : état d'alerte actuel, *New* ou *In Process*
   - **État actif** : *actif* ou *résolu*
   - **Condition** : condition de seuil qui a déclenché l'alerte
   - **Métrique** : la mesure 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 situé à droite de l'alerte et en choisissant l'une des options suivantes :

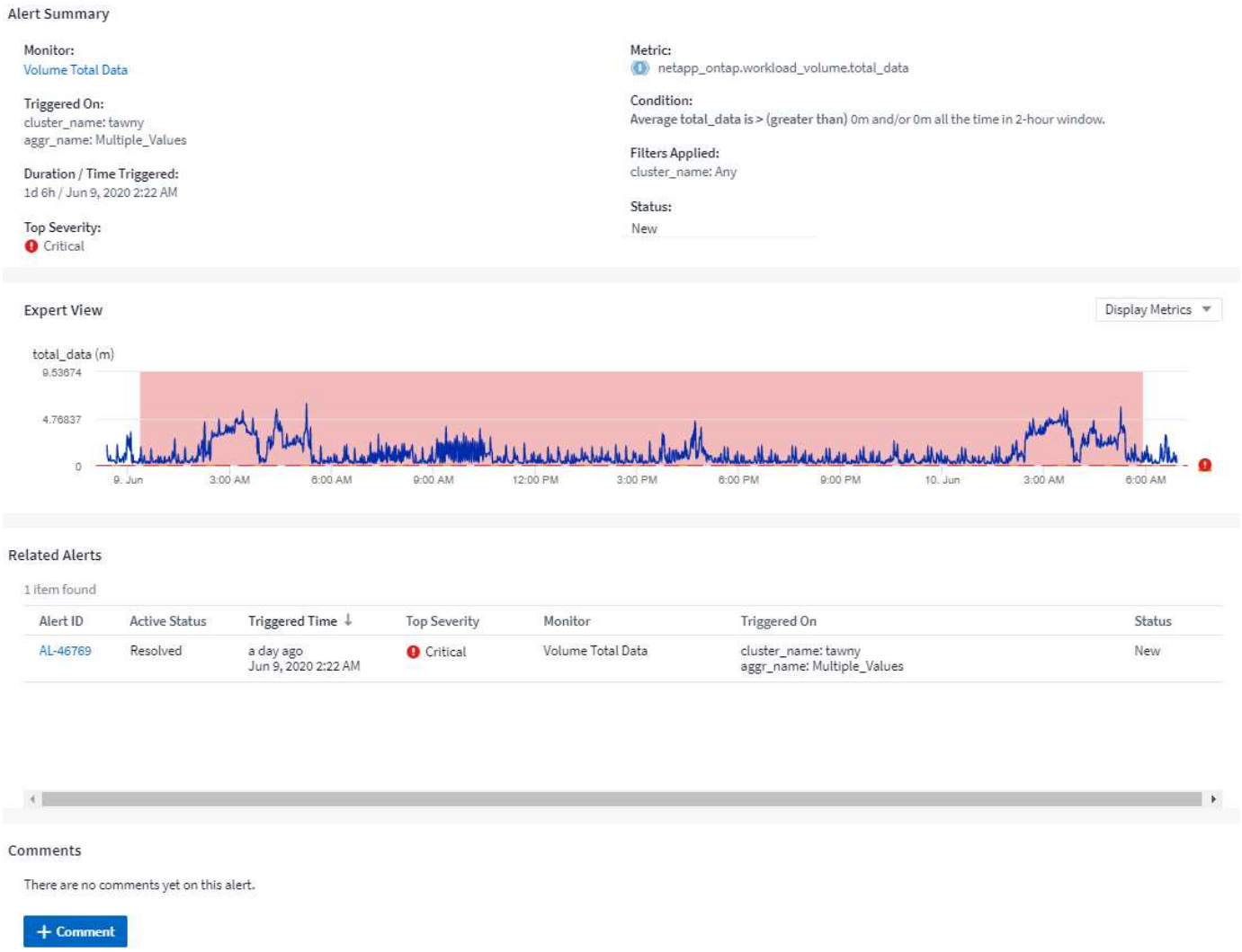
- **En cours** pour indiquer que l'alerte est en cours d'enquête ou doit être maintenue ouverte
- **Rejeter** pour supprimer l'alerte de la liste des alertes actives.

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

Cliquez sur un ID d'alerte pour ouvrir la page Détails de l'alerte.

Page de détails de l'alerte

La page Détails de l'alerte fournit des détails supplémentaires sur l'alerte, y compris un *Summary*, une *Expert View* affichant des graphiques liés aux données de l'objet, des *Related Assets* et *Comments* saisis par les enquêteurs de l'alerte.



Alertes lorsque des données sont manquantes

Dans un système en temps réel tel que Cloud 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 :

- la prochaine donnée à arriver
- un minuteur à tirer lorsqu'il n'y a pas de point de données et que vous avez attendu assez longtemps

Comme c'est le cas avec une arrivée lente des données, ou sans arrivée de données, le mécanisme de temporisation doit prendre le relais car le taux d'arrivée des données est insuffisant pour déclencher des alertes en « temps réel ». La question se pose donc généralement : « combien de temps dois-je attendre avant de fermer la fenêtre d'analyse et de voir ce que j'ai ? » Si vous attendez trop longtemps, vous ne générez pas les alertes assez vite pour être utile.

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

Alertes « actives en permanence »

Il est possible de configurer un moniteur de façon à ce que la condition existe toujours * sur l'objet surveillé—

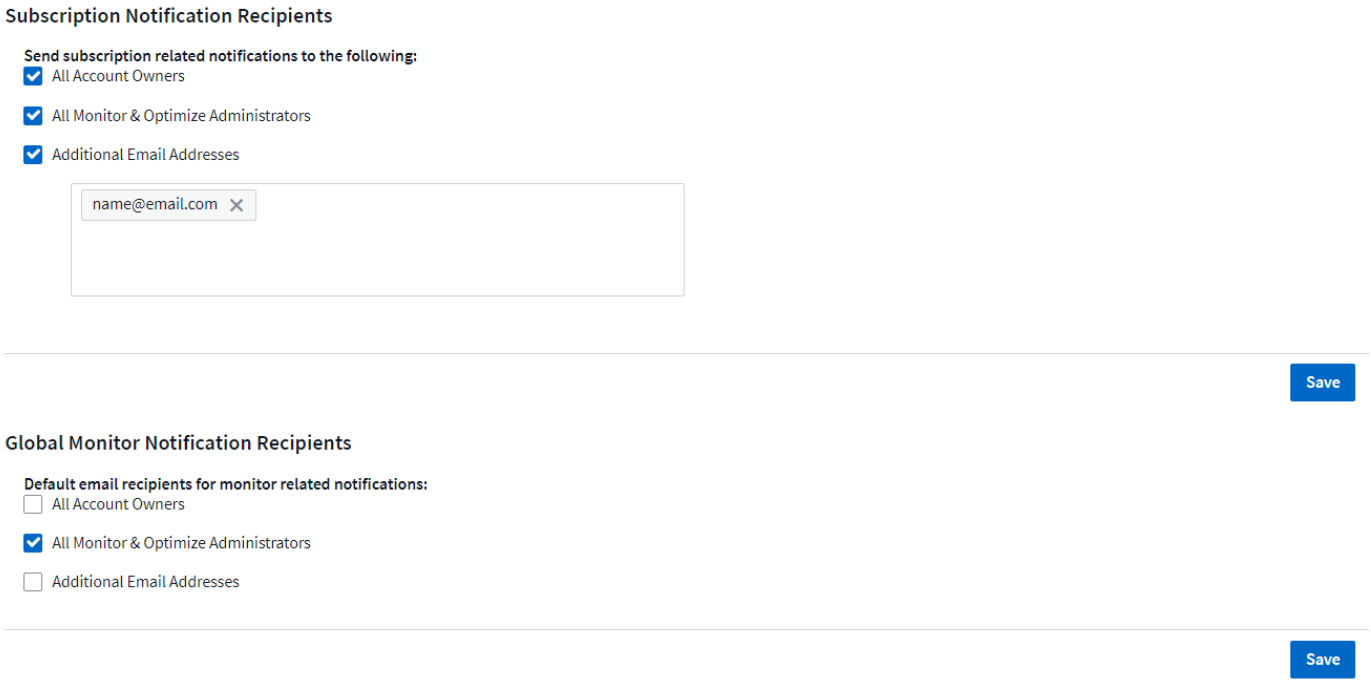
par exemple, IOPS > 1 ou latence > 0. Ils sont souvent créés sous forme de moniteurs « test » puis oubliés. Ces moniteurs créent des alertes qui restent ouvertes en permanence sur les objets constitutifs, ce qui peut entraîner des problèmes de stabilité et de contrainte du système au fil du temps.

Pour éviter cela, Cloud Insights fermera automatiquement toute alerte « active en permanence » après 7 jours. Notez que les conditions sous-jacentes du moniteur peuvent (probablement) continuer à exister, ce qui provoque l'émission d'une nouvelle alerte presque immédiatement, mais cette fermeture d'alertes « toujours actives » réduit une partie de la contrainte système qui peut autrement se produire.

Configuration des notifications par e-mail

Vous pouvez configurer une liste d'e-mails pour les notifications relatives à un abonnement, ainsi qu'une liste globale de destinataires pour la notification des violations de seuil de la stratégie de performances.

Pour configurer les paramètres du destinataire de la notification, accédez à la page **Admin > Notifications** et sélectionnez l'onglet *Email*.



Destinataires de la notification d'abonnement

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

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

Voici des exemples de types de notifications pouvant être envoyées et d'actions utilisateur que vous pouvez effectuer.

Notification:	Action de l'utilisateur:
La version d'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 "Renouvellement automatique" est activé Contact "Ventes NetApp" pour renouveler l'abonnement
L'essai se termine dans 2 jours	Renouvelez l'essai à partir du "Abonnement" page. Vous pouvez renouveler une version d'évaluation une seule fois. Contactez "Ventes NetApp" pour souscrire un abonnement
La période d'essai ou l'abonnement a expiré le compte cessera de collecter les données dans 48 heures. Le compte sera supprimé après 48 heures	Contactez "Ventes NetApp" pour souscrire un abonnement

Liste globale des destinataires des alertes

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

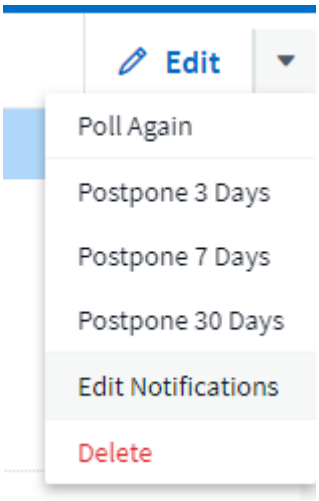
Pour configurer les destinataires d'alertes globales, sélectionnez les destinataires souhaités dans la section **destinataires de notification du moniteur global**.

Vous pouvez toujours remplacer la liste globale des destinataires d'un moniteur individuel lors de la création ou de la modification du moniteur.

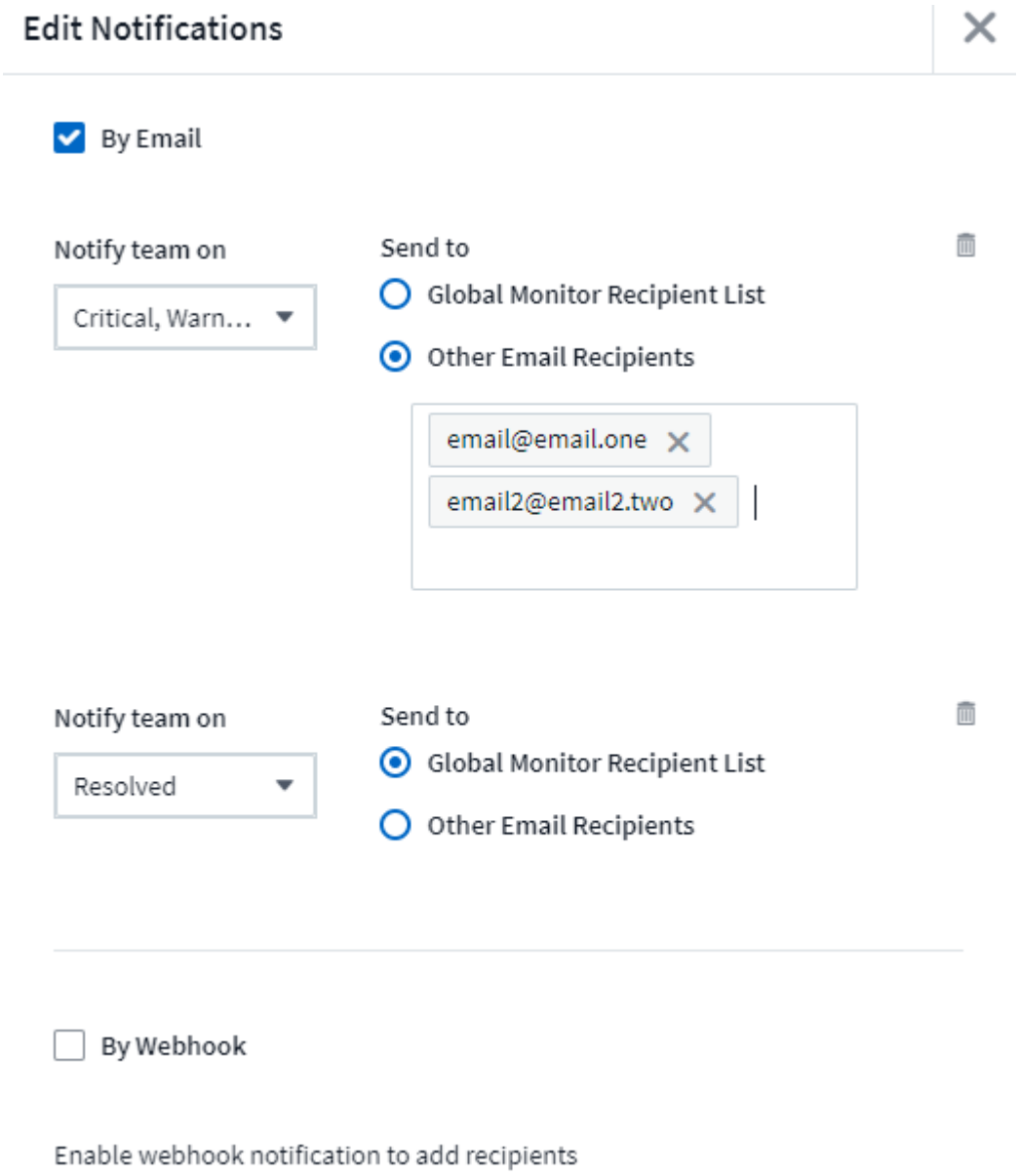
Les notifications ONTAP Data Collector prévalent sur toute notification Monitor spécifique pertinente au cluster/Data Collector. La liste des destinataires que vous définissez pour le Data Collector lui-même recevra les alertes du Data Collector. Si aucune alerte de collecte de données n'est active, des 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 le menu déroulant situé en haut à droite de la page d'accueil stockage.

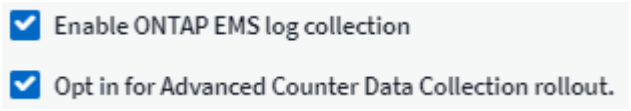


À partir de là, vous pouvez définir des notifications pour les alertes critiques, d'avertissement, d'information et/ou résolues. Chaque scénario peut avertir la liste des destinataires globaux ou les autres destinataires que vous choisissez.



Moniteurs système

Cloud Insights inclut un certain nombre de contrôles définis par le système, à la fois pour les metrics et les journaux. Les moniteurs système disponibles dépendent des collecteurs de données présents dans votre environnement. De ce fait, les moniteurs disponibles dans Cloud Insights peuvent changer à mesure que des collecteurs de données sont ajoutés ou que leurs configurations ont changé.

Par défaut, de nombreux moniteurs système sont en état *pause*. Vous pouvez activer un moniteur système en sélectionnant l'option *Resume* pour le moniteur. Assurez-vous que *la collecte avancée de données de compteur* et *l'activation de la collecte de journaux EMS ONTAP* sont activées dans le collecteur de données. Ces options se trouvent dans le Data Collector de ONTAP sous *Configuration avancée*: 

Description du moniteur

Les moniteurs définis par le système comprennent des mesures et des conditions prédéfinies, ainsi que des descriptions par défaut et des actions correctives, qui ne peuvent pas être modifiées. Vous pouvez *CAN* modifier la liste des destinataires de notification pour les moniteurs définis par le système. Pour afficher les mesures, 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 ni supprimés.

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

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

Les moniteurs système actuellement fournis avec Cloud Insights sont les suivants :

Moniteurs métriques

Nom du moniteur	Gravité	Description du moniteur	Action corrective

Taux d’utilisation des ports Fibre Channel élevé	PRIMORDIAL	Les ports Fibre Channel Protocol sont utilisés pour recevoir et transférer le trafic SAN entre le système hôte du client et les LUN ONTAP. Si l’utilisation du port est élevée, Ensuite, il deviendra un goulot d’étranglement et aura une incidence sur les performances des charges de travail sensibles du protocole Fibre Channel.…Une alerte d’avertissement indique que des actions planifiées doivent être prises pour équilibrer le trafic réseau.…Une alerte critique indique que l’interruption du service est imminente et que des mesures d’urgence doivent être prises pour équilibrer le réseau trafic pour assurer la continuité des services.	Si le seuil critique est atteint, prenez en compte les mesures immédiates pour limiter les interruptions de service : 1. Déplacez les charges de travail vers un autre port FCP le plus utilisé. 2. Limiter le trafic de certaines LUN uniquement au travail essentiel, soit via les stratégies de QoS dans ONTAP, soit la configuration côté hôte pour alléger l’utilisation des ports FCP.… Si le seuil d’avertissement est dépassé, prévoyez d’effectuer les actions suivantes : 1. Configurez davantage de ports FCP pour gérer le trafic de données afin que l’utilisation des ports soit répartie entre plusieurs ports. 2. Déplacez les charges de travail vers un autre port FCP le plus utilisé. 3. Limiter le trafic de certaines LUN uniquement à un travail essentiel, via les stratégies de QoS en ONTAP ou la configuration côté hôte pour simplifier l’utilisation des ports FCP.

Latence élevée de la LUN	PRIMORDIAL	Les LUN sont des objets qui servent le trafic d'E/S souvent pilotés par les applications sensibles aux performances telles que les bases de données. Des latences de LUN élevées signifient que les applications elles-mêmes pourraient souffrir et être incapables d'accomplir leurs tâches. Une alerte d'avertissement indique que des actions planifiées doivent être prises pour déplacer la LUN vers le nœud ou l'agrégat approprié. Une alerte critique indique que l'interruption du service est imminente et que des mesures d'urgence doivent être prises assurer la continuité des services Voici les latences attendues pour le type de support : SSD jusqu'à 1-2 millisecondes, SAS jusqu'à 8-10 millisecondes et disques durs SATA de 17-20 milliseconde	Si un seuil critique est atteint, envisagez les actions suivantes pour minimiser l'interruption de service : si la LUN ou son volume dispose d'une règle de qualité de service associée, évaluez ses limites de seuil et validez si elles provoquent le restrictions de la charge de travail LUN.… Si le seuil d'avertissement est dépassé, prévoyez d'effectuer les actions suivantes : 1. Si l'agrégat connaît également un taux d'utilisation élevé, déplacez le LUN vers un autre agrégat. 2. Si l'utilisation du nœud est également élevée, déplacez le volume vers un autre nœud ou réduisez la charge de travail totale du nœud. 3. Si une règle de qualité de service est associée à la LUN ou à son volume, évaluez ses limites de seuil et validez si la charge de travail de LUN doit être mise au ralenti.

Optimisation de l'utilisation des ports réseau élevée	PRIMORDIAL	Les ports réseau permettent de recevoir et de transférer le trafic protocole NFS, CIFS et iSCSI entre les systèmes hôtes du client et les volumes ONTAP. Si l'utilisation du port est élevée, cela devient un goulot d'étranglement et affecte à terme les performances de NFS, Les charges de travail CIFS et iSCSI… Une alerte d'avertissement indique que des actions planifiées doivent être entreprises pour équilibrer le trafic réseau.…Une alerte critique indique que l'interruption du service est imminente et que des mesures d'urgence doivent être prises pour équilibrer le trafic réseau afin d'assurer la continuité du service.	Si le seuil critique est atteint, prenez en compte les actions immédiates suivantes pour limiter les interruptions de service : 1. Limiter le trafic de certains volumes uniquement à un travail essentiel, soit via les stratégies de QoS dans ONTAP, soit l'analyse côté hôte pour diminuer 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, prenez en compte les actions immédiates suivantes : 1. Configurez davantage de ports réseau pour gérer le trafic de données afin que l'utilisation des ports soit répartie entre plusieurs ports. 2. Configurez un ou plusieurs volumes pour utiliser un autre port réseau moins utilisé.

Latence élevée du namespace NVMe	PRIMORDIAL	Les espaces de noms NVMe sont des objets qui servent le trafic d'E/S piloté par des applications sensibles aux performances, telles que les bases de données. Une latence élevée pour les espaces de noms NVMe signifie que les applications elles-mêmes sont susceptibles de subir des problèmes et qu'elles ne peuvent pas accomplir leurs tâches. Une alerte d'avertissement indique que des actions planifiées doivent être entreprises pour déplacer la LUN vers le nœud ou l'agrégat approprié. Une alerte critique indique que l'interruption du service est imminente et que des mesures d'urgence doivent être prises pour assurer la continuité des services.	Si un seuil critique est atteint, envisagez des actions immédiates pour minimiser les interruptions des services : si l'espace de noms NVMe ou son volume dispose d'une règle de QoS qui leur est attribuée, puis évaluez ses seuils de limite au cas où il entraîne le restriction du workload de l'espace de noms NVMe… Si le seuil d'avertissement est dépassé, envisagez d'effectuer les actions suivantes : 1. Si l'agrégat connaît également un taux d'utilisation élevé, déplacez le LUN vers un autre agrégat. 2. Si l'utilisation du nœud est également élevée, déplacez le volume vers un autre nœud ou réduisez la charge de travail totale du nœud. 3. Si une règle de qualité de service leur est attribuée, évaluez ses seuils de limite au cas où le workload d'espace de noms NVMe serait ralenti.

Capacité qtree saturée	PRIMORDIAL	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 quotas pour limiter la quantité de données stockées dans l'arborescence dans la capacité du volume.…Une alerte d'avertissement indique que l'action planifiée doit être prise pour augmenter l'espace.…Une alerte critique indique que l'interruption du service est imminente et imminente des mesures d'urgence doivent être prises pour libérer de l'espace afin d'assurer la continuité du service.	Si le seuil critique est atteint, prenez en compte les mesures immédiates pour limiter les interruptions de service : 1. Augmenter l'espace du qtree afin de faire face 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 suivantes : 1. Augmenter l'espace du qtree afin de faire face à la croissance. 2. Supprimez les données non souhaitées pour libérer de l'espace.

Limite matérielle de capacité qtree	PRIMORDIAL	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, utilisé pour stocker les données afin de contrôler la croissance des données utilisateur dans le volume et de ne pas dépasser sa capacité totale.…Un qtree maintient un quota de capacité de stockage souple qui permet à l'utilisateur d'être averti de manière proactive avant d'atteindre le total quota de capacité limité dans le qtree et incapable de stocker des données plus. La surveillance de la quantité de données stockées dans un qtree permet à l'utilisateur de recevoir un service de données sans interruption.	Si le seuil critique est atteint, prenez en compte les actions immédiates suivantes pour limiter les interruptions de service : 1. Augmenter le quota d'espace de l'arbre afin de s'adapter à la croissance 2. Demandez à l'utilisateur de supprimer des 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 les données afin de contrôler la croissance des données utilisateur dans le volume et de ne pas dépasser sa capacité totale.…Un qtree maintient un quota de capacité de stockage souple qui permet à l'utilisateur d'être averti de manière proactive avant d'atteindre le limite de quota de capacité totale dans le qtree, impossible de stocker des données plus. La surveillance de la quantité de données stockées dans un qtree permet à l'utilisateur de recevoir un service de données sans interruption.	Si le seuil d'avertissement est dépassé, prenez en compte les actions immédiates suivantes : 1. Augmenter le quota d'espace de l'arbre pour s'adapter à la croissance. 2. Demandez à l'utilisateur de supprimer des données indésirables dans l'arborescence pour libérer de l'espace.

Limite stricte des fichiers qtree	PRIMORDIAL	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 de nombre de fichiers qu'elle peut contenir pour maintenir une taille de système de fichiers gérable au sein du volume.…Un qtree conserve un quota de nombre de fichiers au-delà duquel les nouveaux fichiers de l'arborescence sont refusés. La surveillance du nombre de fichiers dans un qtree permet à l'utilisateur de recevoir un service de données sans interruption.	Si le seuil critique est atteint, prenez en compte les mesures immédiates pour limiter les interruptions de service : 1. Augmenter le quota de nombre de fichiers pour le qtree. 2. Supprimez les fichiers non désirés 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 d'un nombre de fichiers qu'il peut contenir afin de maintenir une taille de système de fichiers gérable au sein du volume.…Un qtree conserve un quota de numéro de fichier logiciel afin de fournir une alerte à l'utilisateur de manière proactive avant d'atteindre la limite de fichiers dans le qtree et impossible de stocker des fichiers supplémentaires. La surveillance du nombre de fichiers dans un qtree permet à l'utilisateur de recevoir un service de données sans interruption.	Si le seuil d'avertissement est dépassé, prévoyez de prendre les mesures suivantes : 1. Augmenter le quota de nombre de fichiers pour le qtree. 2. Supprimez les fichiers non désirés du système de fichiers qtree.

Espace de réserve Snapshot plein	PRIMORDIAL	La capacité de stockage d'un volume est nécessaire pour stocker les données des applications et des clients. Une partie de cet espace, appelée espace réservé pour les instantanés, est utilisée pour stocker des instantanés qui permettent de protéger les données localement. Plus les données stockées dans le volume ONTAP sont récentes, plus la capacité Snapshot est élevée et moins la capacité de stockage des copies Snapshot est disponible pour les données mises à jour ou nouvelles. Si la capacité des données snapshot d'un volume atteint l'espace total de réserve snapshot, il se peut que le client ne puisse pas stocker de nouvelles données snapshot et qu'il ne puisse pas réduire le niveau de protection des données du volume. La surveillance du volume utilisé permet la continuité des services de données.	Si le seuil critique est atteint, prenez en compte les mesures immédiates pour limiter les interruptions de service : 1. Configurez les instantanés pour utiliser l'espace de données dans le volume lorsque la réserve Snapshot est pleine. 2. Supprimez quelques snapshots indésirables plus anciens pour libérer de l'espace.… Si le seuil d'avertissement est dépassé, prévoyez de prendre les mesures suivantes : 1. Augmentez l'espace de réserve Snapshot au sein du volume pour faire face 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	PRIMORDIAL	Lorsqu'un pool de stockage (agrégat) est en cours de remplissage, les opérations d'E/S ralentissent et finissent par entraîner un incident lors d'une panne du stockage. Une alerte d'avertissement indique que l'action planifiée doit être prise prochainement pour restaurer un espace disponible minimal. Une alerte critique indique que l'interruption des services est imminente et que des mesures d'urgence doivent être prises pour libérer de l'espace afin d'assurer la continuité des services.	Si le seuil critique est atteint, prendre immédiatement en compte les actions suivantes pour minimiser les interruptions de service : 1. Supprimez des snapshots sur des volumes non critiques. 2. Supprimez des volumes ou des LUN qui ne sont pas des charges de travail 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. Déplacement d'un ou plusieurs volumes vers un autre emplacement de stockage 2. Ajoutez de la capacité de stockage supplémentaire. 3. Modifiez les paramètres d'efficacité du stockage ou procédez au Tiering des données inactives vers le stockage cloud.

Limite de performances du stockage	PRIMORDIAL	Lorsqu'un système de stockage atteint ses limites de performances, les opérations sont lentes, la latence augmente et les charges de travail et les applications peuvent tomber en panne. ONTAP évalue l'utilisation du pool de stockage pour les charges de travail et estime le pourcentage de performance consommé. Une alerte d'avertissement indique que des actions planifiées doivent être effectuées pour réduire la charge du pool de stockage afin de garantir que les pics de charge de travail du pool de stockage seront suffisants.…Une alerte critique indique que cela ces problèmes de performances sont imminents et des mesures d'urgence doivent être prises pour réduire la charge des pools de stockage afin d'assurer la continuité des services.	Si le seuil critique est atteint, prenez en compte les actions immédiates suivantes pour limiter les interruptions de service : 1. Suspendre les tâches planifiées telles que les snapshots ou la réplication SnapMirror. 2. Charges de travail non essentielles inactives.… Si le seuil d'avertissement est dépassé, effectuez immédiatement les actions suivantes : 1. Déplacez une ou plusieurs charges de travail vers un autre emplacement de stockage. 2. Ajouter plus de nœuds de stockage (AFF) ou de tiroirs disques (FAS) et redistribuer les charges de travail 3. Modifiez les caractéristiques des charges de travail (taille de bloc, mise en cache des applications).

Limite matérielle de capacité de quota utilisateur	PRIMORDIAL	ONTAP reconnaît les utilisateurs des systèmes Unix ou Windows qui sont autorisés à accéder aux volumes, aux fichiers ou aux 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 politique utilisateur ou 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 capacité utilisée dans le volume est juste avant d'atteindre le quota de capacité totale. Le contrôle de la quantité de données stockées dans un quota utilisateur ou groupe garantit que l'utilisateur reçoit un service de données ininterrompu.	Si le seuil critique est atteint, prenez en compte les actions immédiates suivantes pour limiter les interruptions de service : 1. Augmenter l'espace du quota de l'utilisateur ou du groupe pour faire face à la croissance. 2. Demandez à l'utilisateur ou au groupe de supprimer des données indésirables pour libérer de l'espace.

Quota utilisateur - limite logicielle de capacité	AVERTISSEMENT	ONTAP reconnaît l'utilisateur des systèmes Unix ou Windows qui sont autorisés à accéder aux volumes, aux fichiers ou aux 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 utilisateur ou groupe limite l'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 capacité utilisée dans le volume atteint le quota de capacité totale. Le contrôle de la quantité de données stockées dans un quota utilisateur ou groupe garantit que l'utilisateur reçoit un service de données ininterrompu.	Si le seuil d'avertissement est dépassé, prévoyez de prendre les mesures suivantes : 1. Augmenter l'espace du quota de l'utilisateur ou du groupe pour faire face à la croissance. 2. Supprimez les données non souhaitées pour libérer de l'espace.

Capacité du volume saturée	PRIMORDIAL	La capacité de stockage d'un volume est nécessaire pour stocker les données des applications et des clients. Plus le volume ONTAP est stocké, plus la disponibilité du stockage des données futures est faible. Si la capacité de stockage de données d'un volume atteint la capacité de stockage totale, cela peut conduire le client à ne pas pouvoir stocker les données en raison d'une capacité de stockage insuffisante. La surveillance du volume utilisé permet d'assurer la continuité des services de données.	Si le seuil critique est atteint, prenez en compte les actions immédiates suivantes pour limiter les interruptions de service : 1. Augmentation de l'espace du volume pour suivre la croissance. 2. Supprimez les données non souhaitées pour libérer de l'espace. 3. Si les copies snapshot occupent plus d'espace que la réserve snapshot, supprimez les anciens snapshots ou activez la suppression automatique de l'instantané de volume.…si le seuil d'avertissement est dépassé, prévoyez d'effectuer les actions immédiates suivantes : 1. Augmentation de l'espace du volume pour suivre la croissance 2. Si les copies snapshot occupent plus d'espace que la réserve de snapshots, supprimez les anciens snapshots ou activez la suppression automatique de l'instantané de volume.……

Limite des inodes de volume	PRIMORDIAL	Les volumes qui stockent des fichiers utilisent des nœuds d'index (inode) pour stocker les métadonnées de fichiers. Lorsqu'un volume épuise son allocation d'inode, Aucun autre fichier ne peut y être ajouté.…Une alerte d'avertissement indique que des actions planifiées doivent être prises pour augmenter le nombre d'inodes disponibles.…Une alerte critique indique que la limite de fichier est imminente et que des mesures d'urgence doivent être prises pour libérer des inodes afin d'assurer la continuité du service.	Si le seuil critique est atteint, prenez en compte les actions immédiates suivantes pour limiter 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 pour prendre en charge les systèmes de fichiers volumineux.… Si le seuil d'avertissement est dépassé, prévoyez de prendre les mesures 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 pour prendre en charge les systèmes de fichiers volumineux

Latence de volume élevée	PRIMORDIAL	Les volumes sont des objets qui servent le trafic d'E/S souvent pilotés par les applications sensibles aux performances, telles que les applications DevOps, les répertoires locaux et les bases de données. Une latence élevée signifie que les applications elles-mêmes risquent de subir des conséquences et d'être dans l'impossibilité d'accomplir leurs tâches. Pour maintenir des performances prévisibles au niveau des applications, il est essentiel de contrôler les latences des volumes. Les latences suivantes sont attendues pour le type de support : SSD jusqu'à 1-2 millisecondes ; SAS jusqu'à 8-10 millisecondes et disques durs SATA 17-20 millisecondes.	Si un seuil critique est atteint, envisagez d'effectuer quelques actions immédiates pour minimiser les interruptions de service : si une règle de QoS lui est attribuée, évaluez ses seuils limites au cas où il restreint la charge de travail du volume… Si le seuil d'avertissement est dépassé, prenez en compte les actions immédiates suivantes : 1. Si l'agrégat connaît également un taux d'utilisation élevé, déplacez le volume vers un autre agrégat. 2. Si une règle de qualité de service lui est attribuée, évaluez ses seuils de limite au cas où il restreint la charge de travail du volume. 3. Si l'utilisation du nœud est également 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

Latence élevée du nœud	AVERTISSEMENT / CRITIQUE	La latence du nœud a atteint les niveaux où elle peut affecter les performances des applications du nœud. Une latence de nœud moindre garantit la prévisibilité des performances des applications. Les latences attendues pour le type de support sont : SSD jusqu'à 1-2 millisecondes ; SAS jusqu'à 8-10 millisecondes et disques durs SATA 17-20 millisecondes.	Si un seuil critique est atteint, des mesures immédiates doivent être prises pour limiter les interruptions de service : 1. Suspension des tâches planifiées, des snapshots ou de la réplication SnapMirror 2. Réduisez les besoins des workloads à priorité faible grâce aux limites de qualité de service 3. Désactiver les charges de travail non essentielles considère les 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 les besoins des workloads à priorité faible grâce aux limites de qualité de service 3. Ajout de nœuds de stockage (AFF) ou de tiroirs disques (FAS) et redistribution des charges de travail 4. Modifier les caractéristiques des charges de travail (taille de bloc, mise en cache des applications, etc.)

Limite de performance du nœud	AVERTISSEMENT / CRITIQUE	L'utilisation des performances du nœud a atteint les niveaux où elle peut affecter les performances des E/S et des applications prises en charge par le nœud. Des nœuds peu performants garantissent la prévisibilité des performances des applications.	Des mesures immédiates doivent être prises pour minimiser les interruptions de service si un seuil critique est atteint : 1. Suspension des tâches planifiées, des snapshots ou de la réplication SnapMirror 2. Réduisez les besoins des workloads à priorité faible grâce aux limites de qualité de service 3. Inactiver les charges de travail non essentielles tenez compte des 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 les besoins des workloads à priorité faible grâce aux limites de qualité de service 3. Ajout de nœuds de stockage (AFF) ou de tiroirs disques (FAS) et redistribution des charges de travail 4. Modifier les caractéristiques des charges de travail (taille de bloc, mise en cache des applications, etc.)

Latence élevée des machines virtuelles de stockage	AVERTISSEMENT / CRITIQUE	La latence des VM de stockage a atteint les niveaux où elle peut affecter les performances des applications sur la VM de stockage. La faible latence des machines virtuelles de stockage garantit la prévisibilité des performances des applications. Les latences attendues pour le type de support sont : SSD jusqu'à 1-2 millisecondes ; SAS jusqu'à 8-10 millisecondes et disques durs SATA 17-20 millisecondes.	Si le seuil critique est atteint, évaluez immédiatement les limites de seuil des volumes de la machine virtuelle de stockage auxquels une règle de qualité de service est attribuée, afin de vérifier s'il est en cause, les charges de travail des volumes seront immédiatement mises en œuvre en cas de dépassement du seuil d'avertissement : 1. Si l'agrégat connaît également une exploitation élevée, déplacez certains volumes de la machine virtuelle de stockage vers un autre agrégat. 2. Pour les volumes de la machine virtuelle de stockage auxquels une règle de qualité de service est attribuée, évaluez les limites de seuil si les charges de travail des volumes doivent être restreintes 3. Si l'utilisation du nœud est élevée, déplacez certains volumes de la machine virtuelle de stockage vers un autre nœud ou réduisez l'ensemble de la charge de travail du nœud
Limite stricte des fichiers de quota utilisateur	PRIMORDIAL	Le nombre de fichiers créés au sein du volume a atteint la limite critique et aucun fichier supplémentaire ne peut être créé. La surveillance du nombre de fichiers stockés permet à l'utilisateur de recevoir un service de données sans interruption.	Des actions immédiates sont requises pour minimiser les interruptions de service si le seuil critique est atteint.…envisager de prendre les actions 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 logicielle des fichiers de quota utilisateur	AVERTISSEMENT	Le nombre de fichiers créés au sein du volume a atteint la limite seuil du quota et se situe à proximité 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.	Prenez en compte les actions immédiates si le seuil d'avertissement est dépassé : 1. Augmenter le quota de nombre de fichiers pour le quota d'utilisateur spécifique 2. Supprimez les fichiers indésirables pour réduire la pression sur le quota de fichiers pour l'utilisateur spécifique

Taux de Miss. Du cache du volume	AVERTISSEMENT / CRITIQUE	Volume cache Miss ratio est le pourcentage de demandes de lecture des applications client renvoyées du disque au lieu d'être renvoyées à partir du cache. Cela signifie que le volume a atteint le seuil défini.	Si un seuil critique est atteint, des mesures immédiates doivent être prises pour limiter les interruptions de service : 1. Déplacez certaines charges de travail depuis le nœud du volume pour réduire la charge d'E/S 2. Si ce n'est pas déjà le cas sur le nœud du volume, augmentez le cache WAFL en achetant et en ajoutant un module Flash cache 3. Lorsque le seuil d'avertissement est dépassé, réduisez les besoins en charges de travail moins prioritaires sur le même nœud via les limites de QoS. Déplacez certaines charges de travail depuis le nœud du volume pour réduire la charge d'E/S 2. Si ce n'est pas déjà le cas sur le nœud du volume, augmentez le cache WAFL en achetant et en ajoutant un module Flash cache 3. Réduisez les besoins en charges de travail prioritaires sur le même nœud via la limitation de la qualité de service 4. Modifier les caractéristiques des charges de travail (taille de bloc, mise en cache des applications, etc.)

Surallocation du quota de qtree volume	AVERTISSEMENT / CRITIQUE	Volume qtree quota overcommit spécifie le pourcentage auquel un volume est considéré comme surallouant par les quotas qtree. Le seuil défini pour le quota qtree est atteint pour le volume. La surveillance du surengagement de quota qtree du volume permet à l'utilisateur de recevoir un service de données sans interruption.	Si un seuil critique est atteint, des mesures immédiates doivent être prises pour limiter les interruptions de service : 1. Augmenter l'espace du volume 2. Supprimez les données non souhaitées lorsque le seuil d'avertissement est atteint, puis envisagez d'augmenter l'espace du volume.

Haut de la page

Moniteurs de journaux

Nom du moniteur	Gravité	Description	Action corrective
Identifiants AWS non initialisés	INFO	Cet événement se produit lorsqu'un module tente d'accéder aux identifiants basés sur les rôles Amazon Web Services (AWS) et de gestion des identités et des accès à partir du thread d'informations d'identification cloud avant leur initialisation.	Attendez que le thread des informations d'identification du cloud, ainsi que le système, aient terminé l'initialisation.

Cloud Tier inaccessible	PRIMORDIAL	Un nœud de stockage ne peut pas se connecter à l'API de 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 fonctionnelle 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 nœud de destination LIF intercluster… Assurez-vous ce qui suit :…la configuration de votre magasin d'objets n'a pas changé.…les informations de connexion et de connectivité sont Toujours valide… 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 de 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 d'assainissement ou est entré dans le centre de maintenance.	Aucune.

Composant FlexGroup complet	PRIMORDIAL	Un composant d'un volume FlexGroup est saturé, 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 dans le composant ne peut être modifié. Par conséquent, des erreurs aléatoires liées au manque d'espace peuvent s'afficher lorsque vous tentez d'effectuer des opérations d'écriture sur le volume FlexGroup.	Il est recommandé d'ajouter de la capacité au volume FlexGroup à l'aide de la commande « volume modify -Files +X »….alternativement, supprimez des fichiers du volume FlexGroup. Toutefois, il est difficile de déterminer quels fichiers ont été débarqués sur le composant.
FlexGroup Constituent presque plein	AVERTISSEMENT	Un composant d'un volume FlexGroup est quasiment à court d'espace, ce qui peut entraîner une interruption potentielle du service. Vous pouvez créer et développer des fichiers. Cependant, si le composant est à court d'espace, il se peut que vous ne puissiez pas ajouter ou modifier les fichiers du composant.	Il est recommandé d'ajouter de la capacité au volume FlexGroup à l'aide de la commande « volume modify -Files +X »….alternativement, supprimez des fichiers du volume FlexGroup. Toutefois, il est difficile de déterminer quels fichiers ont été débarqués sur le composant.
FlexGroup Constituent quasiment hors des inodes	AVERTISSEMENT	Un composant d'un volume FlexGroup se trouve quasiment en dehors des inodes, à l'origine d'une interruption potentielle du service. Le composant reçoit des demandes de création moins élevées que la moyenne. Cela peut avoir un impact sur les performances globales du volume FlexGroup, car les demandes sont acheminées à des composants avec davantage d'inodes.	Il est recommandé d'ajouter de la capacité au volume FlexGroup à l'aide de la commande « volume modify -Files +X »….alternativement, supprimez des fichiers du volume FlexGroup. Toutefois, il est difficile de déterminer quels fichiers ont été débarqués sur le composant.

FlexGroup Constituent à partir d'inodes	PRIMORDIAL	Un composant d'un volume FlexGroup a des inodes, à un risque de perturbation potentielle du service. Vous ne pouvez pas créer de nouveaux fichiers sur ce composant. Cela peut conduire à une distribution du contenu globalement iméquilibrée sur l'ensemble du volume FlexGroup.	Il est recommandé d'ajouter de la capacité au volume FlexGroup à l'aide de la commande « volume modify -Files +X »….alternativement, supprimez des fichiers du volume FlexGroup. Toutefois, il est difficile de déterminer quels fichiers ont été débarqués sur le composant.
LUN hors ligne	INFO	Cet événement se produit lorsqu'une LUN est mise hors ligne manuellement.	Remettre la LUN en ligne.
Echec du ventilateur de l'unité principale	AVERTISSEMENT	Un ou plusieurs ventilateurs de l'unité principale sont défectueux. 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 en état d'avertissement.	Remplacer les ventilateurs indiqués pour éviter toute surchauffe.

Batterie NVRAM faible	AVERTISSEMENT	La capacité de la batterie NVRAM est extrêmement faible. Une perte de données peut se produire si la batterie devient hors tension.…votre système génère et transmet un message AutoSupport ou d'appel en cas d'incident au support technique NetApp et aux destinations configurées si elle est configurée pour le faire. La transmission réussie d'un message AutoSupport améliore considérablement la détermination et la résolution des problèmes.	Effectuez les actions correctives suivantes :…visualisez l'état actuel de la batterie, sa capacité et son état de charge à l'aide de la commande « System node Environment Sensors ».…si la batterie a été remplacée récemment ou si le système n'était pas opérationnel pendant une période prolongée, Surveillez la batterie pour vérifier qu'elle se charge correctement.…contactez le support technique de 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 une fois par semaine pour vous rappeler de configurer le processeur de service. Le processeur de service est un dispositif physique intégré à votre système pour fournir des fonctions d'accès à distance et de gestion à distance. Vous devez configurer le processeur de service pour qu'il utilise toutes ses fonctionnalités.	Effectuez les actions correctives suivantes :…configurez le SP à l'aide de la commande « system service-processor network modify ».…facultativement, Obtenir l'adresse MAC du processeur de service à l'aide de la commande « system service-processor network show ».…Vérifiez la configuration du réseau du processeur de service à l'aide de la commande « system service-processor network show ».…Vérifiez que le processeur de service peut envoyer un e-mail AutoSupport à l'aide de la commande « system service-processor AutoSupport Invoke ». REMARQUE : les hôtes de messagerie et les destinataires AutoSupport doivent être configurés dans ONTAP avant d'exécuter cette commande.

Processeur de service hors ligne	PRIMORDIAL	Le processeur de service ne reçoit plus de signaux émis par le processeur de service, même si toutes les actions de restauration du processeur de service ont été effectuées. ONTAP ONTAP ne peut pas surveiller l'état du matériel sans le SP.… le système s'arrêtera pour éviter des dommages matériels et des pertes de données. Configurez une alerte de panique pour être immédiatement avertie en cas de mise hors ligne du processeur de service.	Mettez le système hors tension puis sous tension en exécutant les actions suivantes :…retirez le contrôleur du châssis.…remettez le contrôleur sous tension.…si le problème persiste, remplacez le module de contrôleur.
Défaillance des ventilateurs du tiroir	PRIMORDIAL	Le module de ventilateur ou de ventilateur de refroidissement indiqué du shelf est défectueux. Les disques du tiroir peuvent ne pas recevoir suffisamment d'air de refroidissement, ce qui peut entraîner une panne du disque.	Effectuez les actions correctives suivantes :…Vérifiez que le module de ventilateur est bien en place et bien fixé. REMARQUE : le ventilateur est intégré au module d'alimentation dans certains tiroirs disques.… si le problème persiste, remplacez le module de ventilation.… 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	PRIMORDIAL	Un ou plusieurs ventilateurs de l'unité principale sont défectueux, ce qui interrompt le fonctionnement du système. Cela peut entraîner une perte potentielle de données.	Remplacez les ventilateurs défectueux.

Disques non assignés	INFO	Le système contient des disques non attribués. La capacité est alors gaspillée et votre système peut disposer de erreurs de configuration ou de modifications partielles de la configuration.	Effectuez les actions correctives suivantes :…déterminez quels disques sont non affectés en utilisant la commande « disk show -n »….affectez les disques à un système à l'aide de la commande « disk assigned ».
Serveur antivirus occupé	AVERTISSEMENT	Le serveur antivirus est trop occupé pour accepter toute nouvelle demande de scan.	Si ce message se produit fréquemment, assurez-vous qu'il y a suffisamment de serveurs antivirus pour gérer la charge d'analyse antivirus générée par la SVM.
Informations d'identification AWS pour le rôle IAM expirées	PRIMORDIAL	Cloud volumes ONTAP est devenu inaccessible. Les identifiants basés sur les rôles de gestion des identités et des accès ont expiré. Les identifiants sont acquis auprès du serveur de métadonnées Amazon Web Services (AWS) via le rôle IAM et signent des demandes d'API à Amazon simple Storage Service (Amazon S3).	Procédez comme suit :…Connectez-vous à la console de gestion EC2 AWS.…accédez à la page instances.…recherchez l'instance pour le déploiement Cloud Volumes ONTAP et vérifiez son intégrité.…Vérifiez que le rôle IAM AWS associé à l'instance est valide et a reçu les privilèges appropriés à l'instance.
Informations d'identification AWS pour le rôle IAM introuvables	PRIMORDIAL	Le thread d'identification cloud ne peut pas acquérir les identifiants basés sur les rôles Amazon Web Services (AWS) Identity and Access Management (IAM) à partir du serveur de métadonnées AWS. Ces identifiants sont utilisés pour signer des demandes d'API vers Amazon simple Storage Service (Amazon S3). Cloud volumes ONTAP est devenu inaccessible.…	Procédez comme suit :…Connectez-vous à la console de gestion EC2 AWS.…accédez à la page instances.…recherchez l'instance pour le déploiement Cloud Volumes ONTAP et vérifiez son intégrité.…Vérifiez que le rôle IAM AWS associé à l'instance est valide et a reçu les privilèges appropriés à l'instance.

Informations d'identification AWS pour le rôle IAM non valides	PRIMORDIAL	Les identifiants basés sur les rôles de gestion des identités et des accès ne sont pas valides. Les identifiants sont acquis auprès du serveur de métadonnées Amazon Web Services (AWS) via le rôle IAM et signent des demandes d'API à Amazon simple Storage Service (Amazon S3). Cloud volumes ONTAP est devenu inaccessible.	Procédez comme suit :…Connectez-vous à la console de gestion EC2 AWS.…accédez à la page instances.…recherchez l'instance pour le déploiement Cloud Volumes ONTAP et vérifiez son intégrité.…Vérifiez que le rôle IAM AWS associé à l'instance est valide et a reçu les privilèges appropriés à l'instance.
Rôle IAM AWS introuvable	PRIMORDIAL	Le thread des rôles de gestion des identités et des accès ne peut pas trouver de rôle IAM Amazon Web Services (AWS) sur le serveur de métadonnées AWS. Le rôle IAM est requis pour acquérir des identifiants basés sur des rôles afin de signer les demandes d'API vers Amazon simple Storage Service (Amazon S3). Cloud volumes ONTAP est devenu inaccessible.…	Procédez comme suit :…Connectez-vous à la console de gestion EC2 AWS.…accédez à la page instances.…recherchez l'instance pour le déploiement Cloud Volumes ONTAP et vérifiez son état.…Vérifiez que le rôle IAM AWS associé à l'instance est valide.
Rôle IAM AWS non valide	PRIMORDIAL	Le rôle de gestion des identités et des accès Amazon Web Services (AWS) sur le serveur de métadonnées AWS n'est pas valide. Cloud Volume ONTAP est devenu inaccessible.…	Procédez comme suit :…Connectez-vous à la console de gestion EC2 AWS.…accédez à la page instances.…recherchez l'instance pour le déploiement Cloud Volumes ONTAP et vérifiez son intégrité.…Vérifiez que le rôle IAM AWS associé à l'instance est valide et a reçu les privilèges appropriés à l'instance.

Échec de la connexion au serveur de métadonnées AWS	PRIMORDIAL	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). Il convient de établir une communication pour acquérir les identifiants basés sur les rôles AWS IAM nécessaires à la signature des demandes d'API à Amazon simple Storage Service (Amazon S3). Cloud volumes ONTAP est devenu inaccessible.…	Procédez comme suit :…Connectez-vous à la console de gestion EC2 AWS.…accédez à la page instances.…recherchez l'instance pour le déploiement Cloud Volumes ONTAP et vérifiez son état de santé.…
Limite d'utilisation de l'espace FabricPool presque atteinte	AVERTISSEMENT	L'utilisation de l'espace FabricPool total dans le cluster des magasins d'objets auprès de fournisseurs sous licence en termes de capacité a presque atteint la limite autorisée.	Exécutez les actions correctives suivantes :…Vérifiez le pourcentage de la capacité sous licence utilisée par chaque Tier de stockage FabricPool à l'aide de la commande « Storage Aggregate Object-store show-space ».…supprimez les copies Snapshot de volumes grâce à la règle de hiérarchisation « snapshot » ou « sauvegarde » à l'aide de la commande « volume snapshot delete » pour libérer de l'espace.…installez une nouvelle licence sur le cluster, vous pouvez augmenter la capacité sous licence.

Limite d’utilisation de l’espace FabricPool atteinte	PRIMORDIAL	L’utilisation totale de l’espace FabricPool sur l’ensemble du cluster des magasins d’objets auprès de fournisseurs sous licence en fonction de la capacité a atteint la limite de licence.	Exécutez les actions correctives suivantes :…Vérifiez le pourcentage de la capacité sous licence utilisée par chaque Tier de stockage FabricPool à l’aide de la commande « Storage Aggregate Object-store show-space »….supprimez les copies Snapshot de volumes grâce à la règle de hiérarchisation « snapshot » ou « sauvegarde » à l’aide de la commande « volume snapshot delete » pour libérer de l’espace.…installez une nouvelle licence sur le cluster, vous pouvez augmenter la capacité sous licence.

Échec du rétablissement de l'agrégat	PRIMORDIAL	Cet événement a lieu pendant la migration d'un agrégat dans le cadre d'un rétablissement de basculement du stockage (SFO), lorsque le nœud de destination ne peut pas atteindre les magasins d'objets.	Effectuer les actions correctives suivantes :…Vérifiez que votre LIF intercluster est en ligne et fonctionnelle 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 nœud de destination LIF intercluster. …Vérifiez que la configuration de votre magasin d'objets n'a pas changé et que les informations de connexion et de connectivité sont toujours précises à l'aide de la commande « Aggregate Object-store config show ».…alternativement, Vous pouvez ignorer l'erreur en spécifiant false pour le paramètre « exiger-Partner-waiting » de la commande giveback.…contactez le support technique de NetApp pour plus d'informations ou d'aide.

Interconnexion HAUTE DISPONIBILITÉ en panne	AVERTISSEMENT	L’interconnexion haute disponibilité est en panne. Le risque d’interruption de service lorsque le basculement n’est pas disponible.	Les actions correctives dépendent du nombre et du type de liaisons d’interconnexion haute disponibilité prises en charge par la plateforme, ainsi que de la raison pour laquelle l’interconnexion est en panne. …Si les liaisons sont en panne :…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 petits SFP (Form-factor plugables), 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 à l’aide de la commande "ic link on". …Si un poste n’est pas connecté, désactivez et réactivez les liens l’un après l’autre à l’aide des commandes « ic link off » et « ic link on ».…contactez le support technique de 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 terminez toutes celles qui ne fonctionnent pas correctement.…redémarrez le client.…Vérifiez si le problème est causé par une nouvelle application ou une application existante :… si l'application est nouvelle, définissez un seuil plus élevé pour le client en utilisant la commande "cifs option modify -max-ouvre -même-fichier-par -arborescence". Dans certains cas, les clients fonctionnent comme prévu, mais nécessitent un seuil plus élevé. Vous devez disposer d'un privilège avancé 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. Pour plus d'informations ou pour obtenir de l'aide, contactez le support technique NetApp.

Nombre max. D'heures d'ouverture par fichier 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 la fermeture de 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 ne pas fonctionner correctement en raison de l'exécution de l'application.…Reboot le client.…Vérifiez si le problème est causé par une nouvelle application ou une application existante :…si l'application est nouvelle, définissez un seuil plus élevé pour le client en utilisant la commande "option cifs modify -max-iouverture -même-fichier-par -arborescence". Dans certains cas, les clients fonctionnent comme prévu, mais nécessitent un seuil plus élevé. Vous devez disposer d'un privilège avancé 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. Pour plus d'informations ou pour obtenir de l'aide, contactez le support technique NetApp.

Conflit de nom NetBIOS	PRIMORDIAL	Le service de noms NetBIOS a reçu une réponse négative à une demande d'enregistrement de nom provenant d'un ordinateur distant. Ceci est généralement causé par un conflit dans le nom NetBIOS ou un alias. Par conséquent, les clients ne peuvent pas accéder aux données ou se connecter au nœud qui transmet les données approprié dans le cluster.	Effectuez l'une des actions correctives suivantes :…en cas de conflit dans le nom NetBIOS ou dans un alias, Effectuer l'une des opérations suivantes :…Supprimer l'alias NetBIOS en double en utilisant la commande « vserver cifs delete -alias -vserver vserver vserver »….Renommer un alias NetBIOS en supprimant le nom dupliqué et en ajoutant un alias avec un nouveau nom en utilisant la commande « vserver cifs create -alias -vserver ». …En l'absence d'alias configurés et en présence d'un conflit dans le nom NetBIOS, renommez le serveur CIFS en utilisant les commandes « vserver cifs delete -vserver 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 l'ordinateur distant.
Pool de magasins NFSv4 épuisé	PRIMORDIAL	Un pool de magasins 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 de lecture enregistré	PRIMORDIAL	L'antivirus Connector a notifié à ONTAP qu'il ne possède pas de moteur d'analyse enregistré. Cela peut entraîner une indisponibilité des données si l'option « Scan-mandatory » est activée.	Effectuez les actions correctives suivantes :…Assurez-vous que le logiciel du moteur de scan installé sur le serveur antivirus est compatible avec ONTAP.…Assurez-vous que le logiciel du moteur de scan est en cours d'exécution et configuré pour se connecter au connecteur antivirus sur la boucle locale.
Aucune connexion Vscan	PRIMORDIAL	ONTAP n'a pas de connexion Vscan pour les demandes de scan antivirus. Cela peut entraîner une indisponibilité des données si l'option « Scan-mandatory » est activée.	Assurez-vous que le pool de scanner est correctement configuré et que les serveurs antivirus sont actifs et connectés à ONTAP.
Espace de volume racine du nœud faible	PRIMORDIAL	Le système a détecté que le volume racine est dangereusement faible sur l'espace. Le nœud n'est pas entièrement opérationnel. Les LIF de données peuvent avoir basculé sur le cluster car l'accès NFS et CIFS est limité sur le nœud. La capacité administrative est limitée aux procédures de restauration locale pour que le nœud vide l'espace sur le volume racine.	Effectuez les actions correctives suivantes :…effacez 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 développant la capacité du volume racine.…redémarrez le contrôleur.…contactez le support technique NetApp pour obtenir plus d'informations ou d'assistance.
Partage Admin inexistant	PRIMORDIAL	Problème Vscan : un client a tenté de se connecter à un partage ONTAP_ADMIN$ inexistant.	S'assurer que le Vscan est activé pour l'ID SVM mentionné. L'activation du Vscan sur un SVM entraîne la création automatique du partage ONTAP_ADMIN$ pour la SVM.

Espace de nom NVMe insuffisant	PRIMORDIAL	Un namespace NVMe a été mis hors ligne pour cause d'une défaillance d'écriture provoquée par le manque d'espace.	Ajoutez de l'espace au volume, puis mettez le namespace NVMe en ligne en utilisant la commande « vserver nvme namespace modify ».
Délai de grâce NVMe-of actif	AVERTISSEMENT	Cet événement se produit tous les jours lorsque le protocole NVMe over Fabrics (NVMe-of) est en cours d'utilisation et que la période de grâce de la licence est active. La fonctionnalité NVMe-of requiert une licence après l'expiration de la période de grâce de la licence. La fonctionnalité NVMe-of est désactivée lorsque la période de grâce des licences est terminée.	Contactez votre ingénieur commercial pour obtenir une licence NVMe-of et l'ajouter au cluster, ou supprimer toutes les instances de la configuration NVMe-of du cluster.
Délai de grâce NVMe-of expiré	AVERTISSEMENT	La période de grâce de la licence NVMe-of (NVMe over Fabrics) est terminée et la fonctionnalité NVMe-of est désactivée.	Contactez votre ingénieur commercial pour obtenir une licence NVMe-of et l'ajouter au cluster.
Début du délai de grâce NVMe-of	AVERTISSEMENT	La configuration NVMe-of (NVMe over Fabrics) a été détectée lors de la mise à niveau du logiciel ONTAP 9.5. La fonctionnalité NVMe-of requiert une licence après l'expiration de la période de grâce de la licence.	Contactez votre ingénieur commercial pour obtenir une licence NVMe-of et l'ajouter au cluster.
L'hôte de magasin d'objets ne peut pas être résolu	PRIMORDIAL	Le nom d'hôte du serveur de stockage d'objets ne peut pas être résolu en adresse IP. Le client de magasin d'objets ne peut pas communiquer avec le serveur de 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 Object Store en panne	PRIMORDIAL	Le client Object-Store ne peut pas trouver une LIF opérationnelle qui communique avec le serveur de magasin d'objets. Le nœud n'autorise pas le trafic client de magasin d'objets tant que le LIF intercluster n'est pas opérationnel. Par conséquent, les données peuvent être inaccessibles.	Effectuer les actions correctives suivantes :…Vérifiez le statut de LIF intercluster en utilisant la commande « network interface show -role intercluster ».…Vérifiez que le LIF intercluster est configuré correctement et opérationnel.…si une LIF intercluster n'est pas configurée, ajoutez-la en utilisant la commande « network interface create -role intercluster ».
Incohérence de signature de magasin d'objets	PRIMORDIAL	La signature de demande envoyée au serveur de stockage 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 configurée correctement. Si elle est correctement configurée, contactez le support technique NetApp pour obtenir de l'aide.

Délai D’attente DU RÉADR	PRIMORDIAL	Une opération DE fichier DE REMADDIR a dépassé le délai d’exécution autorisé dans WAFL. Ceci peut être dû à des répertoires très grands ou épars. Une action corrective est recommandée.	Effectuez les actions correctives suivantes :…recherchez les informations spécifiques aux répertoires récents qui ont eu DES opérations DE fichier DE RÉADDIR expirant en utilisant la commande suivante 'diag' Privilege nodeshell CLI: WAFL readdir avis show.…Vérifiez si les répertoires sont indiqués comme sparse ou non:… si un répertoire est indiqué comme sparse, il est recommandé de copier le contenu du répertoire dans un nouveau répertoire pour supprimer l’sparseness du fichier de répertoire. …Si un répertoire n’est pas indiqué comme étant sparse 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.

Le transfert de l'agrégat a échoué	PRIMORDIAL	Cet événement a lieu pendant le transfert d'un agrégat, si le nœud de destination ne peut pas atteindre les magasins d'objets.	Effectuer les actions correctives suivantes :…Vérifiez que votre LIF intercluster est en ligne et fonctionnelle 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 nœud de destination LIF intercluster. …Vérifiez que la configuration de votre magasin d'objets n'a pas changé et que les informations de connexion et de connectivité sont toujours précises à l'aide de la commande « Aggregate Object-store config show ».…vous pouvez également ignorer l'erreur en utilisant le paramètre « override-destination-chvérifié » de la commande de transfert.…Contactez le support technique de NetApp pour plus d'informations ou d'assistance.
Échec de la copie en double	PRIMORDIAL	Une opération VSS (Volume Shadow Copy Service), un service de sauvegarde et de restauration Microsoft Server, a échoué.	Vérifiez ce qui suit à l'aide des informations fournies dans le message d'événement :…la configuration de copie en double est-elle activée?…les licences appropriées sont-elles installées? …Sur quels partages l'opération de copie en double est-elle effectuée?…le nom du partage est-il correct?…le chemin du partage existe-t-il?…Quels sont les États du jeu de copies en double et de ses copies en double ?

Échec des blocs d'alimentation du commutateur de stockage	AVERTISSEMENT	Il manque une alimentation dans le commutateur du cluster. La redondance est réduite, le risque de panne lié à d'autres pannes de courant.	Effectuez les actions correctives suivantes :…Assurez-vous que l'alimentation secteur, qui alimente le commutateur du cluster, est sous tension.…assurez-vous que le cordon d'alimentation est connecté à l'alimentation.…contactez le support technique NetApp si le problème persiste.
Authentification CIFS trop nombreuses	AVERTISSEMENT	De nombreuses négociations d'authentification ont eu lieu simultanément. Il y a 256 nouvelles demandes de session incomplètes de ce client.	Étudier les raisons pour lesquelles le client a créé au moins 256 nouvelles demandes de connexion. Vous devrez peut-être contacter le fournisseur du client ou de l'application pour déterminer la raison de l'erreur.
Accès utilisateur non autorisé au partage Admin	AVERTISSEMENT	Un client a tenté de se connecter au partage Privileged ONTAP_ADMIN$, même si l'utilisateur connecté n'est pas un utilisateur autorisé.	Effectuer les actions correctives suivantes :…Assurez-vous que le nom d'utilisateur et l'adresse IP mentionnés sont configurés dans l'un des pools de scanner Vscan actifs.…Vérifiez la configuration du pool de scanner actuellement active 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 causer 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.	Vérifier le journal du serveur Vscan signalé dans l'événement « syslog » pour voir s'il peut nettoyer, mettre en quarantaine ou supprimer le fichier infecté. S'il n'a pas pu le faire, un administrateur système peut avoir à supprimer manuellement le fichier.
Volume hors ligne	INFO	Ce message indique qu'un volume est mis hors ligne.	Remettre le volume en ligne.
Volume restreint	INFO	Cet événement indique qu'un volume flexible est réduit.	Remettre le volume en ligne.
L'arrêt de la VM de stockage a réussi	INFO	Ce message se produit lorsqu'une opération « arrêt vServer » réussit.	Utiliser la commande « vserver start » pour démarrer l'accès aux données sur une machine virtuelle de stockage.
Problème au niveau des nœuds	AVERTISSEMENT	Cet événement est émis en cas de panique	Contactez l'assistance client NetApp.

Haut de la page

Moniteurs de journal anti-ransomware

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

Surveillance anti-ransomwares du volume activée	INFO	La surveillance anti-ransomwares du volume est activée.	Aucune
Surveillance anti-ransomware du volume désactivée	AVERTISSEMENT	La surveillance anti-ransomware du volume est désactivée. Activation d'anti-ransomwares pour protéger le volume	Aucune
Surveillance anti-ransomware des volumes activée (mode apprentissage)	INFO	La surveillance anti-ransomwares du volume est activée en mode d'apprentissage.	Aucune
Mise en pause de la surveillance anti-ransomware des volumes (mode apprentissage)	AVERTISSEMENT	La surveillance anti-ransomware du volume est suspendue en mode d'apprentissage.	Aucune
Mise en pause de la surveillance anti-ransomware du volume	AVERTISSEMENT	La surveillance anti-ransomware du volume est suspendue.	Aucune
Surveillance anti-ransomwares du volume désactivation	AVERTISSEMENT	La surveillance anti-ransomwares du volume est désactivée.	Aucune
Activité de ransomware détectée	PRIMORDIAL	Pour protéger les données contre le ransomware détecté, une copie Snapshot peut être utilisée pour restaurer les données d'origine. Votre système génère et transmet un message AutoSupport ou d'appel en cas d'incident au support technique NetApp, ainsi qu'à toute destination configurée. Le message AutoSupport améliore l'identification et la résolution des problèmes.	Reportez-vous au « NOM DU DOCUMENT FINAL » pour prendre des mesures correctives concernant l'activité de ransomware.

Haut de la page

FSX pour moniteurs ONTAP NetApp

Nom du moniteur	Seuils	Description du moniteur	Action corrective

La capacité du volume FSX est pleine	Avertissement @ > 85 %…critique @ > 95 %	La capacité de stockage d'un volume est nécessaire pour stocker les données des applications et des clients. Plus le volume ONTAP est stocké, plus la disponibilité du stockage des données futures est faible. Si la capacité de stockage de données d'un volume atteint la capacité de stockage totale, cela peut conduire le client à ne pas pouvoir stocker les données en raison d'une capacité de stockage insuffisante. La surveillance du volume utilisé permet d'assurer la continuité des services de données.	Des actions immédiates sont requises pour minimiser les interruptions de service si le seuil critique est atteint :…1. Envisagez de supprimer les données qui ne sont plus nécessaires pour libérer de l'espace
Volume FSX latence élevée	Avertissement @ > 1000 µs…critique @ > 2000 µs	Les volumes sont des objets qui servent le trafic d'E/S souvent pilotées par des applications sensibles aux performances, notamment les applications DevOps, les répertoires locaux et les bases de données. Une latence élevée signifie que les applications elles-mêmes risquent de subir des conséquences et d'être dans l'impossibilité d'accomplir leurs tâches. Pour maintenir des performances prévisibles au niveau des applications, il est essentiel de contrôler les latences des volumes.	Des actions immédiates sont requises pour minimiser les interruptions de service si le seuil critique est atteint :…1. Si une règle de QoS lui est attribuée, évaluez ses seuils de limite au cas où la charge de travail du volume serait mise au ralenti…… planifier de prendre les actions suivantes rapidement si le seuil d'avertissement est dépassé :…1. Si une règle de QoS lui est attribuée, évaluez ses seuils de limite au cas où la charge de travail du volume serait mise au ralenti.…2. Si l'utilisation du nœud est également élevée, déplacez-le vers un autre nœud ou réduisez la charge de travail totale du nœud.

Limite des inodes de volume FSX	Avertissement @ > 85 %…critique @ > 95 %	Les volumes qui stockent des fichiers utilisent des nœuds d'index (inode) pour stocker les métadonnées de fichiers. Lorsqu'un volume épuise son allocation d'inode, aucun autre fichier ne peut lui être ajouté. Une alerte d'avertissement indique que l'action planifiée doit être prise pour augmenter le nombre d'inodes disponibles. Une alerte critique indique que la limite d'épuisement des fichiers est imminente et que des mesures d'urgence doivent être prises pour libérer les inodes afin d'assurer la continuité des services	Des actions immédiates sont requises pour minimiser les interruptions de service si le seuil critique est atteint :…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 les actions suivantes rapidement 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
Surallocation du quota qtree volume FSX	Avertissement @ > 95 %…critique @ > 100 %	Volume qtree quota overcommit spécifie le pourcentage auquel un volume est considéré comme surallouant par les quotas qtree. Le seuil défini pour le quota qtree est atteint pour le volume. La surveillance du surengagement de quota qtree du volume permet à l'utilisateur de recevoir un service de données sans interruption.	Si un seuil critique est atteint, des mesures immédiates doivent être prises pour limiter les interruptions de service : 1. Supprimez les données indésirables… lorsque le seuil d'avertissement est atteint, envisagez d'augmenter l'espace du volume.

Espace de réserve Snapshot FSX saturé	Avertissement @ > 90 %…critique @ > 95 %	La capacité de stockage d'un volume est nécessaire pour stocker les données des applications et des clients. Une partie de cet espace, appelée espace réservé pour les instantanés, est utilisée pour stocker des instantanés qui permettent de protéger les données localement. Plus les données stockées dans le volume ONTAP sont récentes, plus la capacité Snapshot est élevée et moins la capacité de stockage Snapshot sera disponible pour les données à venir (nouvelles ou mises à jour). Si la capacité des données snapshot d'un volume atteint l'espace total de réserve snapshot, il se peut que le client ne puisse pas stocker de nouvelles données snapshot et qu'il ne puisse pas réduire le niveau de protection des données du volume. La surveillance du volume utilisé permet la continuité des services de données.	Des actions immédiates sont requises pour minimiser les interruptions de service si le seuil critique est atteint :…1. Envisagez de configurer les instantanés pour utiliser l'espace de données dans le volume lorsque la réserve de snapshot est pleine… 2. Pensez à supprimer des instantanés plus anciens qui pourraient ne plus être nécessaires pour libérer de l'espace…… planifier pour prendre les actions suivantes bientôt si le seuil d'avertissement est dépassé:…1. Envisagez d'augmenter l'espace de réserve snapshot au sein du volume pour répondre à la croissance…2. Envisagez de configurer des instantanés pour utiliser l'espace de données dans le volume lorsque la réserve Snapshot est pleine

Taux de Miss. Du cache du volume FSX	Avertissement @ > 95 %…critique @ > 100 %	Volume cache Miss ratio est le pourcentage de demandes de lecture des applications client renvoyées du disque au lieu d'être renvoyées à partir du cache. Cela signifie que le volume a atteint le seuil défini.	Si un seuil critique est atteint, des mesures immédiates doivent être prises pour limiter les interruptions de service : 1. Déplacez certaines charges de travail depuis le nœud du volume pour réduire la charge d'E/S 2. Réduisez la demande de charges de travail moins prioritaires sur le même nœud via des limites de QoS… prenez des mesures immédiates en cas de dépassement du seuil d'avertissement : 1. Déplacez certaines charges de travail depuis le nœud du volume pour réduire la charge d'E/S 2. Réduisez les besoins en charges de travail prioritaires sur le même nœud via la limitation de la qualité de service 3. Modifier les caractéristiques des charges de travail (taille de bloc, mise en cache des applications, etc.)

Haut de la page

Contrôleurs K8s

Nom du moniteur	Description	Actions correctives	Gravité/seuil

Latence élevée du volume persistant	Avec des latences de volume persistantes élevées, les applications elles-mêmes risquent d'être affectées et ne peuvent pas accomplir leurs tâches. La surveillance de la latence des volumes persistants est essentielle pour maintenir la cohérence des performances des applications. Les latences suivantes sont attendues pour le type de support : SSD jusqu'à 1-2 millisecondes ; SAS jusqu'à 8-10 millisecondes et disques durs SATA 17-20 millisecondes.	**Actions immédiates** Si le seuil critique est dépassé, prenez des mesures immédiates pour minimiser l'interruption du service : Si une politique de QoS est attribuée au volume, évaluez ses seuils limités si celui-ci ralentit la charge de travail du volume. **Actions à faire bientôt** Si le seuil d'avertissement est dépassé, planifiez les actions immédiates suivantes : 1. Si le pool de stockage est également très utilisé, déplacez le volume vers un autre pool de stockage. 2. Si une règle de qualité de service lui est attribuée, évaluez ses seuils de limite au cas où il restreint la charge de travail du volume. 3. Si le contrôleur connaît également un taux d'utilisation élevé, 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 de la mémoire du cluster élevée	La saturation de la mémoire allouable du cluster est élevée. La saturation du CPU 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 K8s.	Ajouter des nœuds. Corrigez tous les nœuds non planifiés. Pods de taille adéquate pour libérer de la mémoire sur les nœuds.	Avertissement @ > 80 % Critique à > 90 %
Échec de la connexion DU POD	Cette alerte se produit en cas d'échec d'une pièce jointe à un volume avec POD.		Avertissement

Taux de retransmission élevé	Taux de retransmission TCP élevé	Vérifier l'encombrement du réseau : identifiez les charges de travail qui consomment beaucoup de bande passante réseau. Vérifiez si le taux d'utilisation du processeur du Pod est élevé. Vérifiez les performances du réseau matériel.	Avertissement @ > 10 % Critique à > 25 %
Capacité élevée du système de fichiers nœud	Capacité élevée du système de fichiers nœud	- Augmenter la taille des disques de nœud pour s'assurer qu'il y a suffisamment de place pour les fichiers d'application. - Diminuer l'utilisation du fichier d'application.	Avertissement @ > 80 % Critique à > 90 %
Charge de travail instabilité du réseau élevée	Puissance TCP élevée (variations de temps de réponse/latence élevées)	Vérifiez la présence d'une congestion du réseau. Identifiez les charges de travail qui consomment beaucoup de bande passante réseau. Vérifiez si le taux d'utilisation du processeur du Pod est élevé. Vérifiez les performances du réseau matériel	Avertissement à > 30 ms. Critique à > 50 ms.

Débit de volume persistant	Les seuils EN MBIT/S sur les volumes persistants peuvent être utilisés pour alerter l'administrateur lorsque les volumes persistants dépassent les attentes de performance prédéfinies, ce qui peut affecter d'autres volumes persistants. L'activation de ce moniteur génère des alertes adaptées au profil de débit type des volumes persistants sur les disques SSD. Ce contrôle couvre tous les volumes persistants de votre environnement. Les valeurs de seuil critique et d'avertissement peuvent être ajustées en fonction de vos objectifs de surveillance en dupliquant ce moniteur et en définissant des seuils appropriés à votre classe de stockage. Un moniteur dupliqué peut être davantage ciblé sur un sous-ensemble de volumes persistants de votre environnement.	**Actions immédiates** Si le seuil critique est dépassé, planifiez immédiatement des actions pour minimiser l'interruption du service : 1. Introduire des limites QoS EN MBIT/S pour le volume. 2. Examinez l'application pilotant le workload sur le volume pour voir s'il y a des anomalies. **Actions à faire bientôt** Si le seuil d'avertissement est dépassé, prévoyez de prendre les mesures immédiates suivantes : 1. Introduire des limites QoS EN MBIT/S pour le volume. 2. Examinez l'application pilotant le workload sur le volume pour voir s'il y a des anomalies.	Avertissement @ > 10,000 Mo/s. Critique @ > 15,000 Mo/s.
Conteneur à risque de tuer le MOO	Les limites de mémoire du conteneur sont trop basses. Le conteneur risque d'être expulsé (mémoire saturée).	Augmentez les limites de la mémoire du conteneur.	Avertissement @ > 95 %
Charge de travail réduite	La charge de travail ne comporte pas de pods sains.		Critique @ < 1
Échec de liaison de la demande de volume persistant	Cette alerte se produit en cas d'échec de liaison sur un volume persistant.		Avertissement
Resourcequota Mem limites sur le point de dépasser	Les limites de mémoire pour l'espace de noms vont dépasser Resourcequota		Avertissement @ > 80 % Critique à > 90 %
Resourcequota Mem requêtes sur le point de dépasser	Les demandes de mémoire pour l'espace de noms vont dépasser Resourcequota		Avertissement @ > 80 % Critique à > 90 %

La création du nœud a échoué	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 configuration.	Primordial
Échec de la récupération du volume persistant	La récupération automatique du volume a échoué.		Avertissement @ > 0 B.
Restriction du processeur du conteneur	Les limites de l'UC du conteneur sont trop basses. Les processus de conteneur sont ralentis.	Augmentez les limites du processeur du conteneur.	Avertissement @ > 95 % Critique à > 98 %
Échec de la suppression de Service Load Balancer			Avertissement
IOPS de volume persistant	Les seuils d'IOPS pour les volumes persistants peuvent être utilisés pour alerter l'administrateur lorsque les volumes persistants dépassent les attentes de performance prédéfinies. L'activation de ce moniteur génère des alertes appropriées pour le profil IOPS type des volumes de persistance. Ce contrôle couvre tous les volumes persistants de votre environnement. Les valeurs de seuil critique et d'avertissement 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 immédiatement des actions pour réduire au minimum les interruptions de service : 1. Introduire des limites IOPS de QoS pour le volume. 2. Examinez l'application pilotant le workload sur le volume pour voir s'il y a des anomalies. **Actions à faire bientôt** Si le seuil d'avertissement est dépassé, planifiez les actions immédiates suivantes : 1. Introduire des limites IOPS de QoS pour le volume. 2. Examinez l'application pilotant le workload sur le volume pour voir s'il y a des anomalies.	Avertissement @ > 20,000 IO/s. Critique à plus de 25,000 E/s.
Échec de la mise à jour de Service Load Balancer			Avertissement
Échec du montage DU POD	Cette alerte survient lorsqu'un montage est en panne sur un POD.		Avertissement

Nœud pression PID	Les identificateurs de processus disponibles sur le nœud (Linux) sont tombés en dessous d'un seuil d'exclusion.	Recherchez et corrigez les pods qui génèrent de nombreux processus et qui ne disposent plus des 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 d'image pod	Kubernetes n'a pas pu extraire l'image du conteneur du pod.	- Assurez-vous que l'image du pod est correctement orthographiée dans la configuration du pod. - Vérifiez que la balise 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'arrivez pas aux limites de taux imposées par les fournisseurs de registres publics.	Avertissement
Tâche en cours d'exécution trop longue	Le travail est en cours d'exécution trop longtemps		Avertissement @ > 1 heure Critique à > 5 h
Mémoire de nœud élevée	L'utilisation de la mémoire des nœuds est élevée	Ajouter des nœuds. Corrigez tous les nœuds non planifiés. Pods de taille adéquate pour libérer de la mémoire sur les nœuds.	Avertissement @ > 85 % Critique à > 90 %
Resourcequota CPU limites sur le point de dépasser	Les limites de CPU pour l'espace de noms vont dépasser Resourcequota		Avertissement @ > 80 % Critique à > 90 %
Boucle de collision du pod	Le pod s'est écrasé et a tenté de redémarrer plusieurs fois.		Critique @ > 3

CPU du nœud haut	L'utilisation du processeur du nœud est élevée.	Ajouter des nœuds. Corrigez tous les nœuds non planifiés. Pods de taille appropriée pour libérer le processeur sur les nœuds.	Avertissement @ > 80 % Critique à > 90 %
Temps de réponse de latence du réseau de la charge de travail élevé	Temps de latence TCP RTT (aller-retour) élevé	Vérifier la congestion du réseau ▒ identifier les charges de travail qui consomment beaucoup de bande passante du réseau. Vérifiez si le taux d'utilisation du processeur du Pod est élevé. Vérifiez les performances du réseau matériel.	Avertissement à > 150 ms. Critique à > 300 ms.
Echec du travail	La tâche ne s'est pas terminée correctement en raison d'une panne ou d'un redémarrage du nœud, d'un épuisement de la ressource, d'un délai d'attente de la tâche ou d'un échec de la planification du pod.	Recherchez les causes d'échec dans les journaux d'événements Kubernetes.	Avertissement @ > 1
Volume persistant plein en quelques jours	L'espace d'un volume persistant sera insuffisant dans quelques jours	-Augmentez la taille du volume pour vous assurer 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 mémoire du nœud	La mémoire du nœud est insuffisante. La mémoire disponible a atteint le seuil d'exclusion.	Ajouter des nœuds. Corrigez tous les nœuds non planifiés. Pods de taille adéquate 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, de mémoire et de disque. Vérifiez la connectivité réseau des nœuds. Recherchez les causes d'échec dans les journaux d'événements Kubernetes.	Critique @ < 1

Capacité élevée du volume persistant	La capacité utilisée par le back-end du volume persistant est élevée.	- Augmenter la taille du volume pour s'assurer qu'il y a suffisamment d'espace pour les fichiers d'application. - Réduire la quantité de données stockées dans les applications.	Avertissement @ > 80 % Critique à > 90 %
La création de Service Load Balancer a échoué	Échec de la création de Service Load Balancer		Primordial
Incompatibilité du réplica de la charge de travail	Certains modules ne sont actuellement pas disponibles pour un déploiement ou un jeu de démonstration.		Avertissement @ > 1
Resourcequota demandes CPU sur le point de dépasser	Les demandes de processeur pour l'espace de noms vont dépasser Resourcequota		Avertissement @ > 80 % Critique à > 90 %
Taux de retransmission élevé	Taux de retransmission TCP élevé	Vérifier l'encombrement du réseau : identifiez les charges de travail qui consomment beaucoup de bande passante réseau. Vérifiez si le taux d'utilisation du processeur du Pod est élevé. Vérifiez les performances du réseau matériel.	Avertissement @ > 10 % Critique à > 25 %
Pression du disque du nœud	L'espace disque disponible et les inodes sur le système de fichiers racine du nœud ou sur le système de fichiers image ont satisfait un seuil d'exclusion.	- Augmenter la taille des disques de nœud pour s'assurer qu'il y a suffisamment de place pour les fichiers d'application. - Diminuer l'utilisation du fichier d'application.	Critique @ > 0
Saturation élevée de l'UC du cluster	La saturation CPU pouvant être localisée par le cluster est élevée. La saturation des processeurs du cluster est calculée comme la somme de l'utilisation des processeurs divisée par la somme des CPU allouables sur tous les nœuds K8s.	Ajouter des nœuds. Corrigez tous les nœuds non planifiés. Pods de taille appropriée pour libérer le processeur sur les nœuds.	Avertissement @ > 80 % Critique à > 90 %

Haut de la page

Changer les moniteurs de journal

Nom du moniteur	Gravité	Description du moniteur
Volume interne détecté	Informatif	Ce message s'affiche lorsqu'un volume interne est détecté.
Volume interne modifié	Informatif	Ce message s'affiche lorsqu'un volume interne est modifié.
Nœud de stockage détecté	Informatif	Ce message s'affiche lorsqu'un nœud de stockage est détecté.
Nœud de stockage supprimé	Informatif	Ce message apparaît lorsqu'un nœud de stockage est supprimé.
Pool de stockage détecté	Informatif	Ce message s'affiche lorsqu'un pool de stockage est découvert.
Storage Virtual machine découvert	Informatif	Ce message s'affiche lorsqu'un Storage Virtual machine est détecté.
Machine virtuelle de stockage modifiée	Informatif	Ce message apparaît lorsqu'un Storage Virtual machine est modifié.

Haut de la page

Moniteurs de collecte de données

Nom du moniteur	Description	Action corrective
Arrêt de l'unité d'acquisition	Les unités d'acquisition Cloud Insights redémarrent régulièrement dans le cadre des mises à niveau pour introduire de nouvelles fonctionnalités. Cela se produit une fois par mois ou moins dans un environnement standard. Un avertissement indiquant qu'une unité d'acquisition est arrêtée doit être suivi peu après par une résolution indiquant que l'unité d'acquisition nouvellement redémarrée a terminé un enregistrement auprès de Cloud Insights. En général, ce cycle de fermeture à enregistrement prend de 5 à 15 minutes.	Si l'alerte survient fréquemment ou dure plus de 15 minutes, vérifiez le fonctionnement du système hébergeant l'unité d'acquisition, le réseau et tout proxy connectant l'UA à Internet.
Echec du collecteur	Le sondage d'un collecteur de données a rencontré une défaillance inattendue.	Visitez la page Data Collector de Cloud Insights pour en savoir plus sur la situation.

Avertissement du collecteur	Cette alerte peut généralement survenir en raison d'une configuration erronée du collecteur de données ou du système cible. Revoir les configurations pour éviter les alertes futures. Cela peut également être dû à la récupération de données moins complètes où le collecteur de données a rassemblé toutes les données qu'il pourrait. Cela peut se produire lorsque des situations changent pendant la collecte de données (par exemple, une machine virtuelle présente au début de la collecte de données est supprimée lors de la collecte et avant la capture de ces données).	Vérifier la configuration du collecteur de données ou du système cible. Notez que le moniteur pour l'avertissement du collecteur peut envoyer plus d'alertes que d'autres types de moniteur. Il est donc recommandé de ne définir aucun destinataire d'alerte à moins que vous ne soyez en mesure de résoudre les problèmes.

Haut de la page

Moniteurs de sécurité

Nom du moniteur	Seuil	Description du moniteur	Action corrective
Transport AutoSupport HTTPS désactivé	Avertissement @ < 1	AutoSupport prend en charge les protocoles de transport HTTPS, HTTP et SMTP. En raison des nature sensibles des messages AutoSupport, NetApp recommande fortement d'utiliser HTTPS comme protocole de transport par défaut pour l'envoi des 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
Chiffrement de cluster non sécurisé pour SSH	Avertissement @ < 1	Indique que SSH utilise des chiffrements non sécurisés, par exemple les chiffrements commençant par *cbc.	Pour supprimer le chiffrement CBC, exécutez la commande ONTAP suivante :…Security ssh remove -vserver <admin vserver> -chiffrements 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 qui accèdent 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 pour un cluster, exécutez la commande ONTAP suivante :…Security login banner modify -vserver <admin svm> -message « Access restreint to Authorized Users autorisés »
Communication entre les pairs de cluster non chiffrée	Avertissement @ < 1	Lors de la réplication de données pour la reprise sur incident, la mise en cache ou la sauvegarde, vous devez protéger ces données lors du transport sur le réseau entre un cluster ONTAP et un autre. Le chiffrement doit être configuré sur les clusters source et de destination.	Pour activer le cryptage sur des relations entre clusters qui ont été créées avant ONTAP 9.6, le cluster source et le cluster de destination doivent être mis à niveau vers la version 9.6. Utilisez ensuite la commande « cluster peer modify » afin de modifier les pairs de cluster source et de destination et utiliser le cryptage de peering de cluster.…consultez le guide NetApp sur le renforcement de la sécurité pour ONTAP 9 pour en savoir plus.
Utilisateur Admin local par défaut activé	Avertissement @ > 0	NetApp recommande de verrouiller (désactiver) tous les comptes administrateur utilisateur (intégrés) inutiles à l'aide de 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 les modèles 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 Advanced Privilege :…Security config modify -interface SSL -is-fips -Enabled true

Transfert de journal non crypté	Avertissement @ < 1	Le délestage des données des syslog est nécessaire pour limiter l'impact d'une faille à un seul système ou une seule solution. Par conséquent, NetApp recommande de décharger des informations syslog en toute sécurité vers un emplacement de stockage ou de conservation sécurisé.	Une fois qu'une destination de transfert de journaux est créée, son protocole ne peut pas être modifié. Pour passer à un protocole crypté, supprimez et recréez la destination du transfert du journal à l'aide de la commande ONTAP suivante :…cluster log-forwarding create -destination <destination ip> -protocole TCP chiffré
Mot de passe MD5 hachée	Avertissement @ > 0	NetApp recommande fortement d'utiliser la fonction de hachage SHA-512 plus sécurisée pour les mots de passe des comptes utilisateur ONTAP. Les comptes utilisant la fonction de hachage MD5 moins sécurisée doivent migrer vers la fonction de hachage SHA-512.	NetApp recommande fortement aux utilisateurs de migrer vers la solution SHA-512 plus sécurisée en leur laissant changer de mot de passe… pour verrouiller des 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 ne dispose d'aucun serveur NTP configuré. 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 serveur ntp create -Server <nom d'hôte du serveur ntp ou adresse ip>
Le nombre de serveurs NTP est faible	Avertissement @ < 3	Indique que le cluster comporte 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 serveur ntp create -Server <nom d'hôte du serveur ntp ou adresse ip>

Shell distant activé	Avertissement @ > 0	Le shell distant 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 sécuriser l'accès à distance.	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 VM de stockage désactivé	Avertissement @ < 1	Indique que la journalisation d'audit est désactivée pour SVM.	Pour configurer le journal d'audit d'un vserver, exécutez la commande ONTAP suivante :…vserver audit enable -vserver <svm>
Chiffrement non sécurisé des machines virtuelles de stockage pour SSH	Avertissement @ < 1	Indique que SSH utilise des chiffrements non sécurisés, par exemple les chiffrements commençant par *cbc.	Pour supprimer le chiffrement CBC, exécutez la commande ONTAP suivante :…Security ssh remove -vserver <vserver> -chiffrements aes256-cbc,aes192-cbc,aes128-cbc,3des-cbc
Bannière connexion VM de stockage désactivée	Avertissement @ < 1	Indique que la bannière de connexion est désactivée pour les utilisateurs qui accèdent 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 pour un cluster, exécutez la commande ONTAP suivante :…Security login banner modify -vserver <svm> -message « Access restreint to Authorized Users autorisés »
Protocole Telnet activé	Avertissement @ > 0	Telnet n'est pas une méthode sécurisée pour établir l'accès par ligne de commande à la solution ONTAP. Pour sécuriser l'accès à distance, Telnet doit être désactivé.	NetApp recommande un accès sécurisé à distance (SSH). Pour désactiver Telnet sur un cluster, exécutez la commande ONTAP suivante en mode Advanced Privilege :…Security Protocol modify -application telnet -Enabled false

Haut de la page

Moniteurs de protection des données

Nom du moniteur	Seuils	Description du moniteur	Action corrective
Espace insuffisant pour la copie Snapshot de la LUN	(Filtre contient_lun = Oui) Avertissement @ > 95 %…critique @ > 100 %	La capacité de stockage d'un volume est nécessaire pour stocker les données des applications et des clients. Une partie de cet espace, appelée espace réservé pour les instantanés, est utilisée pour stocker des instantanés qui permettent de protéger les données localement. Plus les données stockées dans le volume ONTAP sont récentes, plus la capacité Snapshot est élevée et moins la capacité de stockage Snapshot sera disponible pour les données à venir (nouvelles ou mises à jour). Si la capacité des données snapshot d'un volume atteint l'espace total de réserve snapshot, il se peut que le client ne puisse pas stocker de nouvelles données snapshot et qu'il réduit le niveau de protection des données des LUN du volume. La surveillance du volume utilisé permet la continuité des services de données.	**Actions immédiates** si le seuil critique est dépassé, prenez en considération des mesures immédiates pour minimiser les interruptions de service : 1. Configurez les instantanés pour utiliser l'espace de données dans le volume lorsque la réserve Snapshot est pleine. 2. Supprimez d'anciens snapshots indésirables pour libérer de l'espace. **Actions à faire bientôt** si le seuil d'avertissement est dépassé, prévoir de prendre les mesures suivantes immédiatement : 1. Augmentez l'espace de réserve Snapshot au sein du volume pour faire face à la croissance. 2. Configurez les instantanés pour utiliser l'espace de données dans le volume lorsque la réserve d'instantanés est pleine.

Décalage de la relation SnapMirror	Avertissement @ > 150 %…critique @ > 300 %	Le décalage de la relation SnapMirror est la différence entre l'horodatage de l'instantané et l'heure sur le système de destination. Le décalage_temps_pourcentage correspond au rapport entre le temps de décalage et l'intervalle de planification de la règle SnapMirror. Si le temps de décalage est égal à l'intervalle de planification, le décalage_temps_percent sera de 100 %. Si la politique SnapMirror n'a pas de planification, lag_time_percent ne sera pas calculé.	Surveiller 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 »

Haut de la page

Contrôleurs de Cloud volumes (CVO)

Nom du moniteur	Gravité de l'EC	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 d'assainissement ou est entré dans le centre de maintenance.	Aucune

Échec de la reprise de CVO du pool de stockage	PRIMORDIAL	Cet événement a lieu pendant la migration d'un agrégat dans le cadre d'un rétablissement de basculement du stockage (SFO), lorsque le nœud de destination ne peut pas atteindre les magasins d'objets.	Effectuer les actions correctives suivantes : vérifier que votre LIF intercluster est en ligne et fonctionnelle via la commande « network interface show ». Vérifier la connectivité réseau au serveur de magasin d'objets à l'aide de la commande « ping » sur le nœud de destination LIF intercluster. Vérifiez que la configuration de votre magasin d'objets n'a pas changé et que les informations de connexion et de connectivité sont toujours précises à l'aide de la commande « agrégat Object-store config show ». Vous pouvez également annuler l'erreur en spécifiant false pour le paramètre « exiger-Partner-waiting » de la commande giveback. Pour plus d'informations ou pour obtenir de l'aide, contactez le support technique NetApp.

Panne de l’interconnexion haute disponibilité de CVO	AVERTISSEMENT	L’interconnexion haute disponibilité est en panne. Le risque d’interruption de service lorsque le basculement n’est pas disponible.	Les actions correctives dépendent du nombre et du type de liaisons d’interconnexion haute disponibilité prises en charge par la plateforme, ainsi que de la raison pour laquelle l’interconnexion est en panne. Si les liaisons sont arrêtées : vérifiez que les deux contrôleurs de la paire haute disponibilité sont opérationnels. Pour les liaisons externes, assurez-vous que les câbles d’interconnexion sont correctement connectés et que les SFP (Small form-factor pluggables), 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 liens à l’aide de 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.

Sessions CVO max par utilisateur dépassées	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 exécutées sur le client et arrêtez toutes 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 à l'aide de la commande « cifs option modify -max -iouverture-same-file-per -Tree ». Dans certains cas, les clients fonctionnent comme prévu, mais nécessitent un seuil plus élevé. Vous devez disposer d'un privilège avancé 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. Pour plus d'informations ou pour obtenir de l'aide, contactez le support technique NetApp.

Conflit de nom NetBIOS CVO	PRIMORDIAL	Le service de noms NetBIOS a reçu une réponse négative à une demande d'enregistrement de nom provenant d'un ordinateur distant. Ceci est généralement causé par un conflit dans le nom NetBIOS ou un alias. Par conséquent, les clients ne peuvent pas accéder aux données ou se connecter au nœud qui transmet les données approprié dans le cluster.	Effectuer l'une des actions correctives suivantes : en cas de conflit dans le nom NetBIOS ou avec un alias, effectuer l'une des actions suivantes : supprimer l'alias NetBIOS en double à l'aide de la commande « vserver cifs delete -alias -vserver vserver vserver vserver vserver vserver ». Renommez un alias NetBIOS en supprimant le nom dupliqué et en ajoutant un alias avec un nouveau nom à l'aide de la commande « vserver cifs create -alias -vserver ». Si aucun alias n'est configuré et qu'il existe un conflit dans le nom NetBIOS, renommez le serveur CIFS en utilisant les commandes « vserver cifs delete -vserver 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 l'ordinateur distant.
CVO pour le pool de magasins NFSv4 épuisé	PRIMORDIAL	Un pool de magasins NFSv4 a été épuisé.	Si le serveur NFS ne répond pas pendant plus de 10 minutes après cet événement, contactez le support technique NetApp.
Incident de nœud CVO	AVERTISSEMENT	Cet événement est émis en cas de panique	Contactez l'assistance client NetApp.

Espace de volume racine du nœud CVO faible	PRIMORDIAL	Le système a détecté que le volume racine est dangereusement faible sur l'espace. Le nœud n'est pas entièrement opérationnel. Les LIF de données peuvent avoir basculé sur le cluster car l'accès NFS et CIFS est limité sur le nœud. La capacité administrative est limitée aux procédures de restauration locale pour que le nœud vide l'espace sur le volume racine.	Effectuez les actions correctives suivantes : supprimez 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 étendant la capacité du volume racine. Redémarre le contrôleur. Pour plus d'informations ou pour obtenir de l'aide, contactez le support technique NetApp.
CVO n'a pas de partage d'administration	PRIMORDIAL	Problème Vscan : un client a tenté de se connecter à un partage ONTAP_ADMIN$ inexistant.	S'assurer que le Vscan est activé pour l'ID SVM mentionné. L'activation du Vscan sur un SVM entraîne la création automatique du partage ONTAP_ADMIN$ pour la SVM.
L'hôte du magasin d'objets CVO ne peut pas être résolu	PRIMORDIAL	Le nom d'hôte du serveur de stockage d'objets ne peut pas être résolu en adresse IP. Le client de magasin d'objets ne peut pas communiquer avec le serveur de 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 arrêté	PRIMORDIAL	Le client Object-Store ne peut pas trouver une LIF opérationnelle qui communique avec le serveur de magasin d'objets. Le nœud n'autorise pas le trafic client de magasin d'objets tant que le LIF intercluster n'est pas opérationnel. Par conséquent, les données peuvent être inaccessibles.	Effectuer les actions correctives suivantes : vérifier le statut du LIF intercluster en utilisant la commande « network interface show -role intercluster ». Vérifier que le LIF intercluster est correctement configuré et opérationnel. Si un LIF intercluster n'est pas configuré, ajoutez-le en utilisant la commande « network interface create -role intercluster ».

Discordance de la signature du magasin d'objets CVO	PRIMORDIAL	La signature de demande envoyée au serveur de stockage 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 configurée correctement. Si elle est correctement configurée, contactez le support technique NetApp pour obtenir de l'aide.
QoS de CVO pour surveiller la mémoire insuffisante	PRIMORDIAL	La mémoire dynamique du sous-système QoS a atteint sa limite pour le matériel de la plate-forme actuelle. Certaines fonctionnalités de QoS peuvent fonctionner à une capacité limitée.	Supprimez des charges de travail ou des flux actifs pour libérer de la mémoire. Utilisez la commande "statistics show -object workload -Counter OPS" pour déterminer les charges de travail actives. Les workloads actifs montrent des opérations non nulles. Utilisez ensuite plusieurs fois la commande « workload delete <nom_charge de travail> » pour supprimer des charges de travail spécifiques. Vous pouvez également utiliser la commande « stream delete -workload <nom de charge de travail> * » pour supprimer les flux associés de la charge de travail active.

CVO - temporisation	PRIMORDIAL	Une opération DE fichier DE REMADDIR a dépassé le délai d'exécution autorisé dans WAFL. Ceci peut être dû à des répertoires très grands ou épars. Une action corrective est recommandée.	Effectuez les actions correctives suivantes : recherchez les informations spécifiques aux répertoires récents qui ont eu UNE NOUVELLE ADDIR opérations sur les fichiers expire à l'aide de la commande 'diag' privilege nodeshell CLI: WAFL remaddir notice show. Vérifiez si les répertoires sont indiqués comme sparse ou non : si un répertoire est indiqué comme sparse, il est recommandé de copier le contenu du répertoire dans un nouveau répertoire pour supprimer l'sparseness du fichier de répertoire. Si un répertoire n'est pas indiqué comme étant sparse et que le répertoire est grand, il est recommandé de réduire la taille du fichier de répertoire en réduisant le nombre d'entrées de fichier dans le répertoire.

Échec du transfert de CVO du pool de stockage	PRIMORDIAL	Cet événement a lieu pendant le transfert d'un agrégat, si le nœud de destination ne peut pas atteindre les magasins d'objets.	Effectuer les actions correctives suivantes : vérifier que votre LIF intercluster est en ligne et fonctionnelle via la commande « network interface show ». Vérifier la connectivité réseau au serveur de magasin d'objets à l'aide de la commande « ping » sur le nœud de destination LIF intercluster. Vérifiez que la configuration de votre magasin d'objets n'a pas changé et que les informations de connexion et de connectivité sont toujours précises à l'aide de la commande « agrégat Object-store config show ». Vous pouvez également annuler l'erreur en utilisant le paramètre "override-destination-chèques" de la commande de déplacement. Pour plus d'informations ou pour obtenir de l'aide, contactez le support technique NetApp.
Échec de la copie Shadow CVO	PRIMORDIAL	Une opération VSS (Volume Shadow Copy Service), un service de sauvegarde et de restauration Microsoft Server, a échoué.	Vérifiez les éléments suivants à l'aide des informations fournies dans le message d'événement : la configuration de la copie en double est-elle activée ? Les licences appropriées sont-elles installées ? Sur quels partages l'opération de copie en double est-elle effectuée ? Le nom du partage est-il correct ? Le chemin du partage existe-t-il ? Quels sont les États du jeu de clichés instantanés et de ses clichés instantanés ?

L'arrêt de la VM de CVO Storage a réussi	INFO	Ce message se produit lorsqu'une opération « arrêt vServer » réussit.	Utiliser la commande « vserver start » pour démarrer l'accès aux données sur une machine virtuelle de stockage.
CVO trop nombreuses authentification CIFS	AVERTISSEMENT	De nombreuses négociations d'authentification ont eu lieu simultanément. Il y a 256 nouvelles demandes de session incomplètes de ce client.	Étudier les raisons pour lesquelles le client a créé au moins 256 nouvelles demandes de connexion. Vous devrez peut-être contacter le fournisseur du client ou de l'application pour déterminer la raison de l'erreur.
Disques non affectés par CVO	INFO	Le système contient des disques non attribués. La capacité est alors gaspillée et votre système peut disposer de erreurs de configuration ou de modifications partielles de la configuration.	Effectuez les actions correctives suivantes : identifiez les disques non affectés à l'aide de la commande « disque show -n ». Assigner les disques à un système en utilisant la commande « Disk assignez ».
Accès utilisateur non autorisé de CVO au partage Admin	AVERTISSEMENT	Un client a tenté de se connecter au partage Privileged ONTAP_ADMIN$, même si l'utilisateur connecté n'est pas un utilisateur autorisé.	Effectuer les actions correctives suivantes : assurez-vous que le nom d'utilisateur et l'adresse IP mentionnés sont configurés dans l'un des pools de scanner Vscan actifs. Vérifier la configuration du scanner pool qui est 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 entraîner 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.	Vérifier le journal du serveur Vscan signalé dans l'événement « syslog » pour voir s'il peut nettoyer, mettre en quarantaine ou supprimer le fichier infecté. S'il n'a pas pu le faire, un administrateur système peut avoir à supprimer manuellement le fichier.
Volume CVO hors ligne	INFO	Ce message indique qu'un volume est mis hors ligne.	Remettre le volume en ligne.
Volume CVO restreint	INFO	Cet événement indique qu'un volume flexible est réduit.	Remettre le volume en ligne.

Haut de la page

SnapMirror pour les moniteurs de journaux de l'utilitaire de continuité de l'activité (SMBC)

Nom du moniteur	Gravité	Description du moniteur	Action corrective
ONTAP Mediator ajouté	INFO	Ce message s'affiche lorsque le médiateur ONTAP est correctement ajouté à un cluster.	Aucune
ONTAP Mediator non accessible	PRIMORDIAL	Ce message s'affiche lorsque le médiateur ONTAP est reconverti ou que le progiciel du médiateur n'est plus installé sur le serveur du médiateur. Le basculement de SnapMirror n'est donc pas possible.	Supprimez la configuration du médiateur ONTAP actuel à l'aide de la commande « snapmirror médiateur remove ». Reconfigurez l'accès au médiateur ONTAP à l'aide de la commande SnapMirror médiateur add.
Mediator ONTAP supprimé	INFO	Ce message s'affiche lorsque le médiateur ONTAP a été supprimé avec succès d'un cluster.	Aucune

ONTAP Médiateur inaccessible	AVERTISSEMENT	Ce message apparaît lorsque le médiateur ONTAP est inaccessible sur un cluster. Le basculement de SnapMirror n'est donc pas possible.	Vérifiez la connectivité réseau du médiateur ONTAP à l'aide des commandes "ping réseau" et "traceroute réseau". Si le problème persiste, supprimez la configuration du médiateur ONTAP actuel à l'aide de la commande « snapmirror médiateur remove ». Reconfigurez l'accès au médiateur ONTAP à l'aide de la commande SnapMirror médiateur add.
Certificat CA SMBC expiré	PRIMORDIAL	Ce message s'affiche lorsque le certificat de l'autorité de certification du médiateur ONTAP (CA) a expiré. Par conséquent, toute autre communication avec le médiateur ONTAP ne sera pas possible.	Supprimez la configuration du médiateur ONTAP actuel à l'aide de la commande « snapmirror médiateur remove ». Mettez à jour un nouveau certificat d'autorité de certification sur le serveur du médiateur ONTAP. Reconfigurez l'accès au médiateur ONTAP à l'aide de la commande SnapMirror médiateur add.
Expiration du certificat de l'AC SMBC	AVERTISSEMENT	Ce message survient lorsque le certificat de l'autorité de certification du médiateur (CA) de ONTAP expire 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 médiateur remove ». Mettez à jour un nouveau certificat d'autorité de certification sur le serveur du médiateur ONTAP. Reconfigurez l'accès au médiateur ONTAP à l'aide de la commande SnapMirror médiateur add.

Certificat client SMBC expiré	PRIMORDIAL	Ce message s'affiche lorsque le certificat client du médiateur ONTAP a expiré. Par conséquent, toute autre communication avec le médiateur ONTAP ne sera pas possible.	Supprimez la configuration du médiateur ONTAP actuel à l'aide de la commande « snapmirror médiateur remove ». Reconfigurez l'accès au médiateur ONTAP à l'aide de la commande SnapMirror médiateur add.
Expiration du certificat client SMBC	AVERTISSEMENT	Ce message s'affiche lorsque le certificat du client du médiateur ONTAP 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 médiateur remove ». Reconfigurez l'accès au médiateur ONTAP à l'aide de la commande SnapMirror médiateur add.
Relation SMBC hors synchronisation Remarque : L'UM n'a pas cette relation	PRIMORDIAL	Ce message survient lorsqu'une relation SnapMirror pour la continuité de l'activité (SMBC) passe du statut « In-sync » à « Out-of-sync ». La protection des données RPO=0 sera interrompue.	Vérifiez la connexion réseau entre les volumes source et de destination. Surveillez l'état de la relation SMBC à l'aide de la commande « snapmirror show » sur la destination et en utilisant la commande « snapmirror list-destinations » sur la source. La resynchronisation automatique essaiera de ramener la relation à l'état « in-sync ». Si la resynchronisation échoue, vérifiez que tous les nœuds du cluster se trouvent au quorum et sont en bon état.

Certificat de serveur SMBC expiré	PRIMORDIAL	Ce message s'affiche lorsque le certificat du serveur du médiateur ONTAP a expiré. Par conséquent, toute autre communication avec le médiateur ONTAP ne sera pas possible.	Supprimez la configuration du médiateur ONTAP actuel à l'aide de la commande « snapmirror médiateur remove ». Mettez 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 médiateur add.
Expiration du certificat du serveur SMBC	AVERTISSEMENT	Ce message s'affiche lorsque le certificat du serveur du médiateur ONTAP 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 médiateur remove ». Mettez 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 médiateur add.

Haut de la page

Moniteurs d'alimentation, de fréquence cardiaque et divers systèmes supplémentaires

Nom du moniteur	Gravité	Description du moniteur	Action corrective
Alimentation du tiroir disque détectée	INFORMATIF	Ce message survient lors de l'ajout d'une unité d'alimentation au tiroir disque.	AUCUNE
Blocs d'alimentation des tiroirs disques supprimés	INFORMATIF	Ce message survient lorsqu'une unité d'alimentation est retirée du tiroir disque.	AUCUNE
MetroCluster basculement automatique non planifié désactivé	PRIMORDIAL	Ce message survient lorsque la fonctionnalité de basculement automatique non planifié est désactivée.	Exécutez la commande « MetroCluster modify -node -name <nodename> -Automatic-switchover -onfailure true » pour chaque nœud du cluster afin d'activer le basculement automatique.

Nom du moniteur	Gravité	Description du moniteur	Action corrective
Pont de stockage MetroCluster inaccessible	PRIMORDIAL	Le pont de stockage est inaccessible sur le réseau de gestion	1) si le pont est surveillé par SNMP, vérifier que le LIF de node management fonctionne à l'aide de la commande « network interface show ». Vérifiez que le pont est actif à l'aide de la commande « ping réseau ». 2) si le pont est surveillé en bande, vérifiez le câblage de la structure du pont, puis vérifiez que le pont est sous tension.
Température du pont MetroCluster anormale - inférieure à la valeur critique	PRIMORDIAL	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) vérifier que le pont fonctionne dans des conditions de température recommandées.
Température du pont MetroCluster anormale - supérieure à critique	PRIMORDIAL	Le capteur sur le pont Fibre Channel signale une température supérieure au seuil critique.	1) vérifier l'état de fonctionnement du capteur de température du châssis sur le pont de stockage à l'aide de la commande « Storage Bridge show -Cooly ». 2) Vérifiez que le pont de stockage fonctionne dans des conditions de température recommandées.
Agrégat MetroCluster restant derrière	AVERTISSEMENT	L'agrégat a été laissé derrière lors du rétablissement.	1) Vérifiez l'état de l'agrégat à l'aide de la commande « aggr show ». 2) si l'agrégat est en ligne, retournez-le à son propriétaire initial en utilisant la commande « MetroCluster rétablissement ».

Nom du moniteur	Gravité	Description du moniteur	Action corrective
Tous les liens entre les partenaires MetroCluster sont en panne	PRIMORDIAL	Les adaptateurs d'interconnexion RDMA et les LIF intercluster ont des connexions rompues au cluster de peering ou le cluster de peering est en panne.	1) s'assurer que les LIFs intercluster sont opérationnels. Réparer les LIFs intercluster si elles sont en panne. 2) Vérifiez que le cluster peering est opérationnel en utilisant la commande « cluster peer ping ». Reportez-vous au Guide de reprise sur incident de MetroCluster si le cluster de peering est arrêté. 3) pour la structure MetroCluster, vérifiez que les liens ISL de la structure back-end sont opérationnels. Corrigez les liens ISL de la structure back-end s'ils ne sont pas affectés. 4) pour les configurations MetroCluster sans structure, vérifier que le câblage est correct entre les adaptateurs d'interconnexion RDMA. Reconfigurez le câblage si les liaisons sont en panne.
Les partenaires MetroCluster ne sont pas accessibles sur le réseau de peering	PRIMORDIAL	La connectivité au cluster homologue est interrompue.	1) Assurez-vous que le port est connecté au réseau/commutateur approprié. 2) s'assurer que le LIF intercluster est connecté au cluster peering. 3) Assurez-vous que le cluster peering est opérationnel en utilisant la commande « cluster peer ping ». Reportez-vous au Guide de reprise sur incident de MetroCluster si le cluster de peering est hors service.

Nom du moniteur	Gravité	Description du moniteur	Action corrective
MetroCluster inter basculer toutes les liaisons vers le bas	PRIMORDIAL	Toutes les liaisons ISL (Inter-Switch Link) du commutateur de stockage sont en panne.	1) réparer les liens ISL de la structure interne sur le commutateur de stockage. 2) Assurez-vous que le commutateur partenaire est opérationnel et que ses liens ISL sont opérationnels. 3) s'assurer que l'équipement intermédiaire, tel que les appareils xWDM, est opérationnel.
Liaison SAS du nœud MetroCluster vers la pile de stockage	AVERTISSEMENT	L'adaptateur SAS ou son câble connecté peut être défectueux.	1. Vérifiez que l'adaptateur SAS est en ligne et exécuté. 2. Vérifiez que la connexion du câble physique est sécurisée et opérationnelle, et remplacez le câble si nécessaire. 3. Si l'adaptateur SAS est connecté aux tiroirs disques, assurez-vous que les modules d'E/S et les disques sont correctement installés.
Initiateurs MetroClusterFC en panne	PRIMORDIAL	L'adaptateur FC initiateur est en panne.	1. Assurez-vous que la liaison de l'initiateur FC n'a pas été altérée. 2. Vérifiez le statut opérationnel de l'adaptateur FC initiator à l'aide de la commande « system node run -node local -command Storage show adapter ».
Panne de la liaison de l'interconnexion FC-VI	PRIMORDIAL	La liaison physique du port FC-VI est hors ligne.	1. S'assurer que la liaison FC-VI n'a pas été altérée. 2. Vérifiez que le statut physique de l'adaptateur FC-VI est « Marche » à l'aide de la commande « MetroCluster Interconnect adapter show ». 3. Si la configuration inclut des commutateurs de structure, assurez-vous qu'ils sont correctement câblés et configurés.

Nom du moniteur	Gravité	Description du moniteur	Action corrective
Les disques de secours MetroCluster se sont laissés derrière	AVERTISSEMENT	Le disque de spare a été laissé au retard lors du rétablissement.	Si le disque n'est pas en panne, retournez-le à son propriétaire initial en utilisant la commande « MetroCluster rétablissement ».
Port de la passerelle de stockage MetroCluster arrêté	PRIMORDIAL	Le port du Bridge de stockage est hors ligne.	1) Vérifiez le statut opérationnel des ports sur le pont de stockage à l'aide de la commande « Storage Bridge show -ports ». 2) Vérifiez la connectivité logique et physique au port.
Panne des ventilateurs du commutateur de stockage MetroCluster	PRIMORDIAL	Le ventilateur du commutateur de stockage est défectueux.	1) s'assurer que les ventilateurs du commutateur fonctionnent correctement à l'aide de la commande « Storage Switch show -Coolant ». 2) s'assurer que les FRU de ventilateur sont correctement insérées et opérationnelles.
Commutateur de stockage MetroCluster inaccessible	PRIMORDIAL	Le commutateur de stockage est inaccessible sur le réseau de gestion.	1) Assurez-vous que la LIF node management est active à l'aide de la commande « network interface show ». 2) s'assurer que l'interrupteur est actif à l'aide de la commande "ping réseau". 3) Assurez-vous que le commutateur est accessible via SNMP en vérifiant ses paramètres SNMP après avoir ouvert une session sur le commutateur.

Nom du moniteur	Gravité	Description du moniteur	Action corrective
Échec des blocs d'alimentation du commutateur MetroCluster	PRIMORDIAL	Une unité d'alimentation sur le commutateur de stockage n'est pas opérationnelle.	1) Vérifiez les détails d'erreur à l'aide de la commande « Storage Switch show -error -switch -name <swtich name> ». 2) identifier l'unité d'alimentation défectueuse à l'aide de 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	PRIMORDIAL	Le capteur du commutateur Fibre Channel est défectueux.	1) vérifier l'état de fonctionnement des capteurs de température sur le commutateur de stockage à l'aide de la commande « Storage Switch show -Coolant ». 2) vérifier que le contacteur fonctionne dans des conditions de température recommandées.
Température du commutateur MetroCluster anormale	PRIMORDIAL	Le capteur de température sur le commutateur Fibre Channel a signalé une température anormale.	1) vérifier l'état de fonctionnement des capteurs de température sur le commutateur de stockage à l'aide de la commande « Storage Switch show -Coolant ». 2) vérifier que le contacteur fonctionne dans des conditions de température recommandées.

Nom du moniteur	Gravité	Description du moniteur	Action corrective
Absence de signal de détection du processeur de service	INFORMATIF	Ce message apparaît lorsque ONTAP ne reçoit pas de signal de « pulsation » attendu du processeur de service. En plus de ce message, les fichiers journaux du SP sont envoyés pour débogage. ONTAP réinitialise le processeur de service pour tenter de restaurer la communication. Le processeur de service est indisponible pendant deux minutes maximum lorsqu'il redémarre.	Contactez le support technique NetApp.

Nom du moniteur	Gravité	Description du moniteur	Action corrective
Signal de détection du processeur de service arrêté	AVERTISSEMENT	Ce message survient lorsque ONTAP ne reçoit plus les pulsations de l'ensemble du processeur de service. Selon la conception matérielle, le système peut continuer à transmettre des données ou décider de s'arrêter afin d'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 concernant les dispositifs en panne, les erreurs de démarrage ou les erreurs D'autotest de mise sous tension (POST) d'Open Firmware (OFW). Si votre système est configuré pour ce faire, il génère et transmet un message AutoSupport (ou « appel en cas d'incident ») au support technique NetApp et aux destinations configurées. La transmission réussie d'un message AutoSupport améliore considérablement la détermination et la résolution des problèmes.	Si le système s'est arrêté, essayez de mettre hors tension puis sous tension le système : retirez le contrôleur du châssis, poussez-le de nouveau, puis mettez le système sous tension. Si le problème persiste après la mise hors/sous tension ou pour tout autre condition susceptible de justifier votre intervention, contactez le support technique NetApp.

Haut de la page

Plus d'informations

- "Affichage et rejet des alertes"

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site http://www.netapp.com/TM sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.