Corriger les alertes

NetApp Console local deployment

NetApp
August 10, 2026

Sommaire

Corriger les alertes

Découvrez les alertes dans le déploiement local de la NetApp Console

NetApp Console local déploiement génère des alertes qui identifient les problèmes de santé sur vos clusters ONTAP sur site et pour les opérations NetApp Backup and Recovery.

Le déploiement local de la Console consolide les alertes des clusters ONTAP et des opérations de Backup and Recovery dans une vue unique. La page Alertes comprend un tableau de bord, une liste d'alertes et une vue des systèmes afin que vous puissiez consulter les alertes à l'échelle de l'ensemble de l'organisation ou les limiter à une flotte ou un système spécifique. Chaque alerte identifie le système concerné, son niveau de gravité et sa zone d'impact.

Utilisez les alertes dans le déploiement local de NetApp Console pour :

- Détectez les problèmes de capacité, de connectivité, de protection des données, de performance et de sécurité.
- Priorisez les alertes en fonction de leur gravité et de leur zone d'impact.
- Ouvrez une alerte dans System Manager ou Workload Analyzer, puis exécutez une action Fix-It guidée ou automatisée lorsque la page en propose une.
- Acheminer les notifications par e-mail vers les utilisateurs disposant de rôles d'accès spécifiques, ou envoyer les données d'alerte à un système externe via un webhook.
- Exportez la liste des alertes dans un fichier CSV pour une analyse hors ligne.

Niveau de gravité de l'alerte et zones d'impact

Chaque alerte comprend un niveau de gravité et une zone d'impact :

- **Gravité** indique le degré d'urgence, du plus élevé au plus faible : Critique, Majeur, Mineur, Avertissement et Information.
- **Zone d'impact** identifie le domaine affecté : capacité, connectivité, protection des données, performance et sécurité.

Sources et étendue des alertes

- **Les alertes ONTAP** proviennent du système de gestion des événements ONTAP (EMS) sur les clusters sur site que le déploiement local de NetApp Console a découverts."En savoir plus sur le ONTAP EMS et les alertes disponibles."
- **NetApp Backup and Recovery** les alertes proviennent des actions de sauvegarde et de restauration. "En savoir plus sur les alertes NetApp Backup and Recovery."
- Vos autorisations déterminent les flottes que vous pouvez consulter. Limitez la vue à l'ensemble de l'organisation, à une flotte spécifique ou à un système individuel. L'onglet **Systems health** affiche l'état de chaque système et l'onglet **Alerts** affiche la liste actuelle des alertes pour la zone sélectionnée.
- L'exportation CSV reflète la portée actuelle, le texte de recherche et les filtres.

Règles de notification d'alerte

Créez des règles de notification pour déterminer quelles alertes génèrent des notifications et qui les reçoit. Une règle de notification possède les caractéristiques suivantes :

- Il fait correspondre les alertes au service (comme la gestion ONTAP ou NetApp Backup and Recovery), à la gravité, à la zone d'impact et au système cible.
- Pour l'envoi d'e-mails, il envoie des notifications aux utilisateurs disposant des rôles d'accès spécifiés. Pour l'envoi par webhook, il envoie les données d'alerte au point de terminaison configuré ; l'accès à ces données est contrôlé par l'application destinataire, et non par le déploiement local de Console.
- Cela s'applique à des systèmes spécifiques, pas à des flottes.
- Il est possible de la désactiver pendant une fenêtre de maintenance planifiée afin de supprimer les alertes attendues.

Le déploiement local de la Console inclut une règle de notification par défaut qui est active immédiatement après l'installation. La règle par défaut surveille tous les services et systèmes pour les alertes de gravité critique et délivre les notifications uniquement au Centre de notifications de la Console—aucun envoi par e-mail ou webhook n'est configuré tant que vous ne l'avez pas mis en place. Vous pouvez consulter et ajuster cette règle, et créer des règles personnalisées adaptées à votre environnement.

Les alertes de niveau Info sont visibles sur la page Alertes, mais ne sont pas envoyées par notification à moins que vous ne créiez explicitement une règle incluant le niveau de gravité Info.

Informations connexes

- "Surveiller et analyser les alertes"
- "Créer et gérer des règles de notification d'alerte"
- "Découvrez les alertes ONTAP dans le déploiement local de NetApp Console"

Surveillez et analysez les alertes dans le déploiement local de la NetApp Console

Surveillez et analysez les alertes dans le déploiement local de NetApp Console afin de garantir le bon fonctionnement de votre stockage et de minimiser les interruptions.

Consultez les alertes actives pour l'ensemble de votre organisation ou une flotte spécifique, hiérarchisez-les par niveau de gravité et zone d'impact, et identifiez leurs causes profondes afin de résoudre les problèmes avant qu'ils ne s'aggravent. Lorsqu'une alerte propose une action recommandée ou une option Fix It, vous pouvez passer directement de l'investigation à la correction.

Rôle d'accès requis

Tous les rôles, à l'exception d'administrateur de fédération et de lecteur de fédération. Les utilisateurs disposant du rôle d'administrateur de fédération ou de lecteur de fédération ne peuvent pas consulter les alertes. "Découvrez les rôles d'accès".

Pour les alertes ONTAP, vous pouvez accéder à des outils tels que System Manager et Workload Analyzer directement depuis la page Alertes pour examiner et résoudre les problèmes.

Pour les rapports externes, vous pouvez exporter la liste des alertes dans un fichier CSV pour une analyse hors ligne.

Vous pouvez également configurer des règles de notification pour recevoir des alertes par e-mail ou par webhook. "Apprenez à configurer les notifications d'alerte".

Alertes disponibles

NetApp Console local prend en charge les alertes pour ONTAP et NetApp Backup and Recovery.

- "Découvrez les alertes ONTAP dans le déploiement local de NetApp Console"
- "En savoir plus sur les alertes NetApp Backup and Recovery."

Consultez le tableau de bord des alertes

Utilisez le tableau de bord des alertes pour obtenir un aperçu rapide de l'activité d'alertes en cours pour le périmètre que vous avez sélectionné. Le tableau de bord récapitule les alertes actives par gravité et zone d'impact, et inclut un graphique montrant la répartition des alertes au cours des 24 dernières heures afin que vous puissiez repérer rapidement les tendances.

Vous pouvez filtrer le tableau de bord pour vous concentrer sur les alertes critiques ou les alertes concernant une zone d'impact spécifique.

Étapes

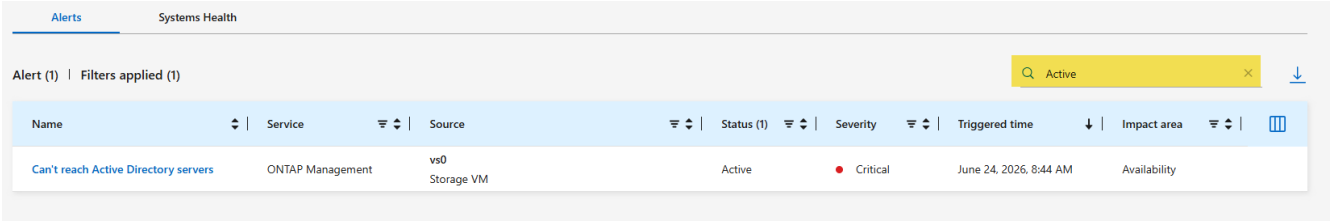
1. Sélectionnez **Santé > Alertes > Vue d'ensemble**.
2. Dans le sélecteur de portée, choisissez l'une des options suivantes :
   - **Toutes** (par défaut) pour afficher les alertes concernant toutes les flottes auxquelles vous avez accès
   - Une flotte spécifique pour voir les alertes uniquement pour cette flotte
3. Filtrez le tableau de bord en fonction des alertes que vous souhaitez consulter, notamment :
   - Gravité (Critique, Avertissement ou Information)
   - Alertes critiques regroupées par zone d'impact
   - Domaine d'impact (Sécurité, Protection, Disponibilité, Performance, Capacité ou Configuration)

Afficher toutes les alertes

Utilisez l'onglet Alertes pour consulter la liste complète des alertes actives pour le périmètre que vous avez sélectionné. La liste est mise à jour pour refléter l'organisation ou le périmètre de flotte actuel, et vous pouvez rechercher des alertes spécifiques par nom ou description.

Étapes

1. Sélectionnez **Santé > Alertes > Vue d'ensemble**.
2. Dans le sélecteur de portée, choisissez l'une des options suivantes :
   - **Toutes** (par défaut) pour afficher les alertes concernant toutes les flottes auxquelles vous avez accès
   - Une flotte spécifique pour voir les alertes uniquement pour cette flotte
3. Sélectionnez l'onglet **Alertes** pour afficher la liste complète des alertes actives pour le périmètre sélectionné.
4. Vous pouvez également rechercher une alerte spécifique dans la liste par nom ou description.



Afficher les alertes par système

Vous pouvez consulter les alertes relatives à un système spécifique au sein d'une flotte ou de votre organisation.

Étapes

1. Sélectionnez **Santé > Alertes > Vue d'ensemble**.
2. Dans le sélecteur de portée, choisissez l'une des options suivantes :
   - **Toutes** (par défaut) pour afficher les alertes concernant toutes les flottes auxquelles vous avez accès
   - Une flotte spécifique pour voir les alertes uniquement pour cette flotte
3. Sélectionnez l'onglet **État des systèmes** pour afficher un résumé des alertes associées aux systèmes inclus dans le périmètre que vous avez sélectionné.
4. Sélectionnez **Afficher les alertes** sur la ligne du système concerné pour afficher la liste complète des alertes actives associées à ce système.

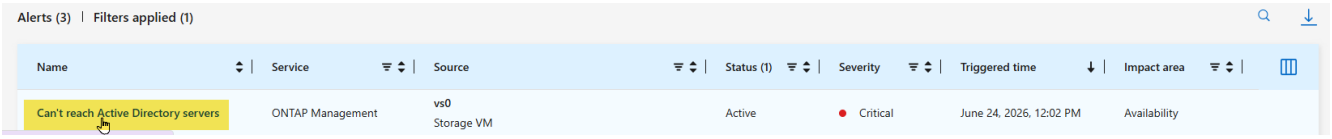
Enquêter sur une alerte

Vous pouvez examiner une alerte pour voir ce qui l'a déclenchée et qui a reçu la notification.

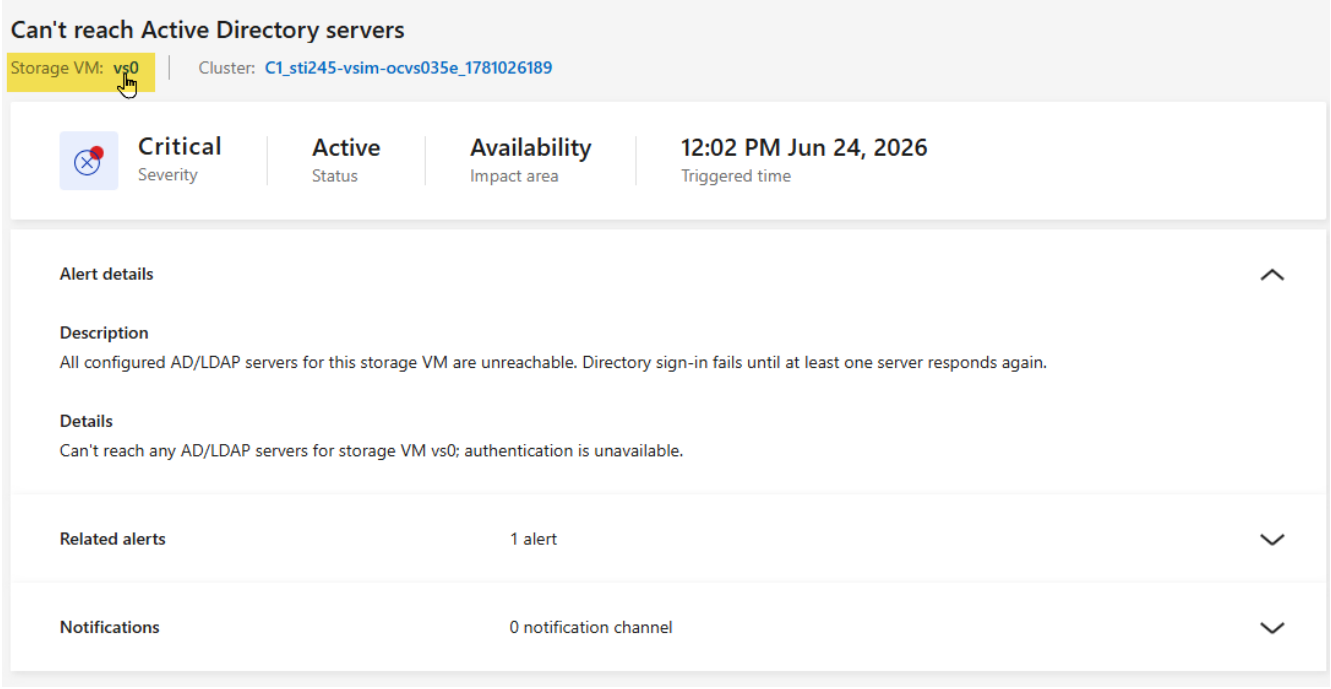
Lors de l'investigation d'une alerte ONTAP, vous pouvez également accéder directement à l'interface System Manager du système qui a généré l'alerte pour consulter des détails supplémentaires et prendre des mesures.

Étapes

1. Sélectionnez **Santé > Alertes > Vue d'ensemble**.
2. Dans le sélecteur de portée, choisissez l'une des options suivantes :
   - **Toutes** (par défaut) pour afficher les alertes concernant toutes les flottes auxquelles vous avez accès
   - Une flotte spécifique pour voir les alertes uniquement pour cette flotte
3. Dans l'un ou l'autre onglet, sélectionnez le nom de l'alerte que vous souhaitez examiner pour afficher ses détails.



4. Le cas échéant, sélectionnez le nom de la machine virtuelle ou du cluster pour ouvrir l'interface du System Manager du système qui a généré l'alerte.



Corriger une alerte

Lorsqu'une alerte comprend une action recommandée ou une option Fix It, utilisez-la pour passer de l'investigation à la remédiation sans quitter les détails de l'alerte.

Étapes

1. Sélectionnez **Santé > Alertes > Vue d'ensemble**.
2. Dans le sélecteur de portée, choisissez l'une des options suivantes :
   - **Toutes** (par défaut) pour afficher les alertes concernant toutes les flottes auxquelles vous avez accès
   - Une flotte spécifique pour voir les alertes uniquement pour cette flotte
3. Sélectionnez l'alerte que vous souhaitez corriger.
4. Consultez les détails de l'alerte, puis sélectionnez l'action recommandée ou l'option **Corriger** si elle est disponible.
5. Suivez les étapes guidées pour appliquer la correction, puis retournez aux détails de l'alerte pour confirmer l'état de l'alerte.

Si l'action résout le problème, l'alerte n'apparaît plus comme active pour ce périmètre. Si l'alerte reste active, consultez à nouveau les détails de l'alerte et poursuivez l'investigation.

Analyser une alerte

Vous pouvez analyser une alerte ONTAP dans Workload Analyzer pour comprendre ce qui l'a déclenchée.

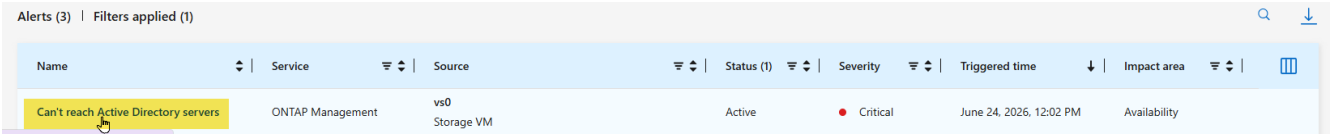
Lors de l'investigation d'une alerte ONTAP, vous pouvez également accéder directement à l'interface System Manager du système qui a généré l'alerte pour consulter des détails supplémentaires et prendre des mesures.

Étapes

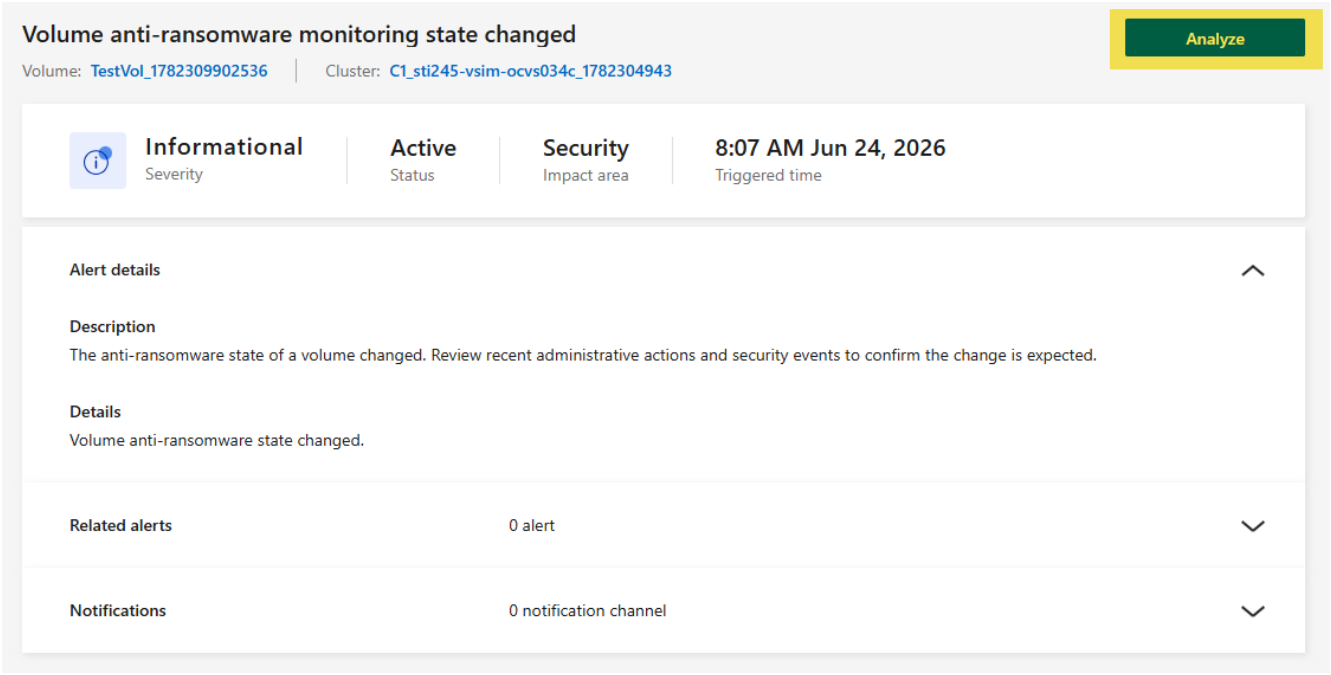
1. Sélectionnez **Santé > Alertes > Vue d'ensemble**.
2. Dans le sélecteur de portée, choisissez l'une des options suivantes :

- **Toutes** (par défaut) pour afficher les alertes concernant toutes les flottes auxquelles vous avez accès
- Une flotte spécifique pour voir les alertes uniquement pour cette flotte

3. Sélectionnez l'onglet **Systems health** pour afficher la liste complète des alertes actives pour le périmètre sélectionné.
4. Dans l'un ou l'autre onglet, sélectionnez le nom de l'alerte que vous souhaitez examiner pour afficher ses détails.



5. Le cas échéant, sélectionnez **Analyser** pour ouvrir l'interface Workload Analyzer pour le système qui a généré l'alerte.



6. Saisissez la plage horaire correspondant à la période pendant laquelle l'alerte a été déclenchée, puis sélectionnez **Analyser** pour afficher les résultats de l'analyse. "Découvrez Workload Analyzer."

Exporter les alertes au format CSV

Exportez la liste des alertes dans le déploiement local de la NetApp Console vers un fichier CSV pour une analyse ou un reporting hors ligne. L'export reflète le périmètre actuel (organisation ou flotte), le texte de recherche et les filtres.

Étapes

1. Sélectionnez **Santé > Alertes**, puis sélectionnez l'onglet **Alertes**.
2. Définissez la portée (organisation ou flotte) et appliquez tous les filtres ou le texte de recherche que vous souhaitez inclure dans l'export.
3. Sélectionnez l'icône de téléchargement pour exporter la liste des alertes vers un fichier CSV.

Configurez les règles de notification pour les alertes dans le déploiement local de la NetApp Console

Configurez les règles de notification dans le déploiement local de NetApp Console pour contrôler quelles alertes déclenchent des notifications, qui les reçoit et comment elles sont distribuées.

Rôles d'accès requis

Super administrateur, administrateur d'organisation, administrateur de stockage, analyste de support opérationnel ou tout autre rôle d'administrateur pour NetApp Backup and Recovery. "Découvrez les rôles d'accès".

Utilisez les règles de notification pour acheminer les alertes pertinentes aux bonnes personnes via les canaux adaptés à votre environnement, tout en réduisant le bruit des alertes qui ne vous concernent pas. Les règles de notification complètent la page Alerts : vous examinez ou résolvez l'alerte dans le workflow Alerts, puis vous utilisez les règles pour contrôler la façon dont les alertes similaires seront transmises à l'avenir.

Une règle de notification associe les alertes à des conditions que vous définissez, telles que le service, la gravité et la zone d'impact, puis délivre une notification via les canaux que vous sélectionnez. Le déploiement local de la Console inclut des règles de notification par défaut que vous pouvez consulter et ajuster, et vous pouvez créer vos propres règles personnalisées. Vous pouvez également mettre en sourdine des règles pour supprimer temporairement les notifications lors d'événements planifiés, comme les fenêtres de maintenance.

- "En savoir plus sur le ONTAP EMS et les alertes disponibles."

Avant de commencer

- Pour envoyer des notifications par e-mail, l'administrateur de votre organisation doit configurer un serveur de messagerie dans le déploiement local de la Console. Pour envoyer des notifications à un système externe, l'administrateur de votre organisation doit configurer un webhook. Pour connaître la procédure, consultez "Configurer la diffusion des notifications".
- Le centre de notifications du déploiement local de la Console affiche les notifications par défaut, aucune configuration supplémentaire n'est donc requise pour les notifications dans la Console.

Consulter les règles de notification

La page des règles de notification centralise la consultation et la gestion de toutes les règles applicables à votre organisation. Chaque règle présente ses attributs principaux, ce qui vous permet d'évaluer et d'ajuster rapidement le comportement de vos alertes.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Santé > Alertes**.
2. Sélectionnez **Paramètres de notification**.
3. Consultez les règles de la liste. Chaque règle indique son statut actif, son nom, les services et niveaux de gravité qu'elle surveille, les rôles autorisés à recevoir des notifications, les canaux de diffusion activés, la date de sa dernière modification et toute période de mise en sourdine programmée.
4. Pour trouver une règle spécifique, utilisez les commandes de filtre et de recherche pour filtrer par statut actif, service, gravité, rôle, canal ou statut de mise en sourdine.

Créer une règle de notification

Créez une règle de notification pour définir les conditions qui déclenchent une notification et la manière dont cette notification est diffusée.

> Vous ne pouvez pas définir de règles de notification pour les flottes. Vous pouvez les définir uniquement pour des systèmes spécifiques. Dans les environnements de grande taille comportant de nombreux systèmes, envisagez de créer des règles plus larges par niveau de gravité plutôt que de dupliquer les règles pour chaque système. Par exemple, une règle Critique unique couvrant tous les systèmes agit comme une règle générale, avec des règles supplémentaires ciblées pour les systèmes nécessitant un routage ou des destinataires différents.

Exemple de règle de notification pour les alertes critiques dans tous les systèmes

Supposons que vous souhaitiez éviter qu'une alerte critique ne passe inaperçue, quel que soit le système d'origine. Vous pouvez créer une règle générale qui achemine toutes les alertes critiques vers le Console Notification Center pour les administrateurs de stockage.

Dans cet exemple, vous créez une règle avec les paramètres suivants :

- **Services** : Tous
- **Gravité** : Critique
- **Rôle IAM** : Administrateur de stockage
- **Système** : (Laisser vide pour appliquer à tous les systèmes)
- **Méthode de distribution** : Centre de notifications de la console

Grâce à cette règle, les administrateurs de stockage voient une notification dans la Console pour chaque alerte critique sur l'ensemble des systèmes. Cette règle sert de base que vous pouvez compléter par des règles plus ciblées.

Exemple de règle de notification ciblée pour les alertes de capacité d'administration du stockage

Supposons que vos administrateurs de stockage doivent intervenir immédiatement en cas de problème critique de capacité sur un système de production spécifique, mais que vous ne souhaitez pas encombrer leurs boîtes de réception d'alertes de moindre gravité. Vous pouvez créer une règle ciblée qui envoie un e-mail aux administrateurs de stockage uniquement lorsqu'une alerte critique de capacité est déclenchée sur ce système.

Dans cet exemple, vous créez une règle avec les paramètres suivants :

- **Services** : gestion ONTAP
- **Gravité** : Critique
- **Zone d'impact** : Capacité
- **Rôle IAM** : Administrateur de stockage
- **Système** : <system_name>
- **Mode de livraison** : Email

Grâce à cette règle, le déploiement local de Console envoie un e-mail à tous les administrateurs de stockage du système spécifié lorsqu'une alerte de capacité critique survient. Les alertes de moindre gravité, telles que les avertissements ou les messages d'information, ne génèrent pas d'e-mail, de sorte que l'équipe puisse se concentrer sur les problèmes nécessitant une attention urgente.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Santé > Alertes**.
2. Sélectionnez **Paramètres de notification**, puis sélectionnez **Ajouter une règle**.
3. Définissez les conditions auxquelles la règle correspond :
   - **Nom de la règle** : saisissez un nom concis et descriptif. Ce champ est obligatoire.
   - **Description de la règle** : saisissez éventuellement un contexte supplémentaire concernant l'objectif de la règle.
   - **Services** : sélectionnez un ou plusieurs services ONTAP ou de plateforme auxquels la règle s'applique.
   - **Rôles** : sélectionnez les rôles d'accès que les utilisateurs doivent posséder pour recevoir des notifications lorsque la règle est déclenchée.
   - **Niveaux de gravité** : sélectionnez les niveaux de gravité que la règle surveille, tels que Critique, Avertissement, Erreur ou Information.
   - **Domaine d'impact** : sélectionnez les domaines opérationnels à faire correspondre, tels que la capacité ou la performance.
   - **Nom de l'alerte** : sélectionnez les types d'alerte spécifiques qui déclenchent la règle.
   - **Système** : sélectionnez le contexte système auquel la règle s'applique.
4. Sélectionnez les canaux de diffusion de la notification :
   - **Courriel** : envoie des courriels d'alerte aux utilisateurs qui ont les rôles sélectionnés. Nécessite un serveur de messagerie configuré.
   - **Webhook** : envoie des données d'alerte à un système externe. Nécessite la sélection d'une intégration webhook configurée.
   - **Centre de notifications de la console** : affiche des alertes en temps réel pour les utilisateurs qui ont les rôles sélectionnés.
5. Pour désactiver les notifications de cette règle pendant une période planifiée, comme une fenêtre de maintenance, définissez une planification **Désactiver les notifications** et choisissez une récurrence si vous souhaitez que la période de désactivation se répète. Vous pouvez ajouter plusieurs périodes de désactivation par règle, ce qui est utile pour les cycles de maintenance récurrents, comme les mises à jour hebdomadaires.
6. Sélectionnez **Créer**.

Activer ou désactiver une règle de notification

Activez ou désactivez les règles de notification individuelles pour contrôler les conditions qui déclenchent des notifications. Désactivez les règles qui ne sont pas pertinentes pour votre environnement afin de réduire les notifications superflues, et activez les règles pour recommencer à recevoir leurs notifications.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Santé > Alertes**.
2. Sélectionnez **Paramètres de notification**.
3. Repérez la règle que vous souhaitez modifier.
4. Activez ou désactivez le commutateur **Actif** de la règle. La modification prend effet immédiatement.

Mettre en sourdine une règle de notification

Mettez en sourdine une règle de notification pour suspendre la livraison des alertes pendant un événement planifié, tel qu'une fenêtre de maintenance, sans désactiver la règle. Les alertes continuent d'apparaître dans la page Alertes pendant la période de mise en sourdine — seules les notifications par e-mail, webhook et dans la console sont supprimées. Lorsque la période de mise en sourdine expire, les notifications reprennent automatiquement.

Vous pouvez ajouter plusieurs fenêtres de mise en sourdine à une seule règle et configurer chacune d'elles pour qu'elle se répète selon une planification.

Exemples de fenêtres muettes

- **Fenêtre de maintenance ponctuelle** : Vous effectuez une mise à jour du firmware d'un système de stockage samedi soir et souhaitez désactiver les alertes pendant cette période. Définissez une fenêtre de désactivation des notifications du samedi 22h00 au dimanche 2h00, sans récurrence. À l'expiration de cette fenêtre, les notifications reprennent automatiquement.
- **Fenêtre de mise à jour hebdomadaire récurrente** : Votre équipe effectue des mises à jour des systèmes tous les dimanches de minuit à 4 h du matin. Ajoutez une fenêtre de mise en sourdine avec récurrence hebdomadaire afin que les notifications soient automatiquement désactivées chaque semaine sans intervention manuelle. Si un deuxième système a son propre calendrier de mise à jour à un autre moment, ajoutez une deuxième fenêtre de mise en sourdine à la même règle, avec sa propre heure de début et sa propre récurrence.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Santé > Alertes**.
2. Sélectionnez **Règles de notification**.
3. Dans la liste des règles, repérez la règle que vous souhaitez désactiver et sélectionnez le menu d'actions correspondant.
4. Sélectionnez **Modifier**.
5. Dans la section **Désactiver les notifications**, définissez la date et l'heure de début et de fin de la période de désactivation.
6. Vous pouvez également sélectionner une récurrence pour répéter la fenêtre selon un calendrier.
7. Pour ajouter des fenêtres muettes supplémentaires, sélectionnez **Ajouter une fenêtre muette** et répétez les étapes précédentes.
8. Sélectionnez **Enregistrer**.

Supprimer une règle de notification

Supprimez une règle de notification si vous n'en avez plus besoin. La suppression d'une règle est définitive, vous ne pourrez donc pas la récupérer.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Santé > Alertes**.
2. Sélectionnez **Paramètres de notification**.
3. Dans la liste des règles, repérez la règle que vous souhaitez supprimer et sélectionnez le menu d'actions correspondant.
4. Sélectionnez **Supprimer** dans le menu d'actions.

Informations connexes

- "Configurer la diffusion des notifications"
- "Découvrez les alertes de la Console"
- "Afficher les alertes"

Corriger la dérive des classes de stockage dans le déploiement local de la NetApp Console

Dans le déploiement local de la NetApp Console, recherchez les alertes liées aux dérives, analysez les résultats de ces dérives et corrigez les charges de travail qui ne correspondent plus à leur classe de stockage prévue.

Rôles requis

Administrateur de stockage

> Vous pouvez uniquement consulter et corriger les charges de travail dans les flottes pour lesquelles vous avez l'autorisation.

Remédier à la dérive

Lorsqu'une charge de travail ne correspond plus à son intention de classe de stockage, le déploiement local de la NetApp Console génère une alerte. Utilisez cette alerte pour analyser l'écart et appliquer la correction recommandée.

Vous pouvez appliquer certaines corrections directement depuis l'alerte. Pour d'autres problèmes, mettez à jour la configuration de la charge de travail ou attribuez une autre classe de stockage pour rétablir la conformité. Le processus de correction affiche l'impact prévu avant que vous n'appliquiez les modifications.

Étapes

1. Sélectionnez **Stockage > Classes de stockage**.

   Un résumé des variations de classe de stockage figure dans la section **Variations par classe de stockage**. La liste complète figure dans le tableau.

2. Dans la colonne **Drifts**, sélectionnez **View** pour la classe de stockage concernée.

   La page **Alertes > Vue d'ensemble** s'ouvre avec les filtres appliqués.

3. Sélectionnez une alerte pour ouvrir la page de détails de l'alerte.
4. Sélectionnez **Analyze**.
5. Examinez les résultats dans **Workload analyzer**.

   Pour les dérives de configuration, comparez les paramètres prévus et réels afin de déterminer ce qui a changé.

6. Sélectionnez l'action corrective recommandée, telle que **Fix it**.
7. Examinez les modifications proposées et appliquez les mesures correctives.
8. Retournez dans **Stockage > Classes de stockage** et vérifiez que la charge de travail n'apparaît plus

comme ayant dérivé.

L'évaluation de la conformité peut prendre plusieurs minutes pour prendre en compte les modifications de configuration récentes. Si la charge de travail est toujours signalée comme ayant dérivé, retournez à la page des détails de l'alerte et sélectionnez **Analyser** pour examiner les résultats restants.

Informations connexes

- "Découvrez la dérive des classes de stockage et la conformité dans le déploiement local de la NetApp Console"
- "Découvrez les alertes de stockage"
- "Afficher les alertes"

Actions de correction des alertes dans le déploiement local de la NetApp Console

Utilisez cette référence pour comprendre les actions correctives disponibles via **Fix it** dans le déploiement local de NetApp Console. Pour chaque action, le tableau décrit ce que fait l'action et l'alerte associée. Examinez les détails de l'action dans la boîte de dialogue de confirmation avant de l'exécuter.

Mesures correctives

Action de remédiation	Nom de l'alerte	Description de l'alerte	Zone d'impact	Résumé des mesures correctives
Activer la croissance automatique du volume	Volume plein	Le volume dispose de peu d'espace et approche de sa capacité maximale.	Capacité	Augmente automatiquement la taille d'un volume (jusqu'à une limite configurée) afin de réduire le risque de manque d'espace.
Redimensionner le volume	Volume plein	Le volume dispose de peu d'espace et approche de sa capacité maximale.	Capacité	Augmente la taille d'un volume pour fournir immédiatement plus d'espace.
Mettre le volume en ligne	Volume hors ligne	Le volume est hors ligne et ne sert pas de données.	Disponibilité	Remet en ligne un volume hors ligne afin qu'il puisse reprendre la diffusion de données.
Mettre l'agrégat en ligne	Agrégat hors ligne	L'agrégat n'est pas en ligne et les volumes qui y sont hébergés peuvent être indisponibles.	Disponibilité	Remet en ligne un agrégat hors ligne pour rétablir l'accès aux volumes qu'il héberge.

Action de remédiation	Nom de l'alerte	Description de l'alerte	Zone d'impact	Résumé des mesures correctives
Mettre LUN en ligne	LUN hors ligne	Le LUN est hors ligne et l'accès à l'hôte est indisponible.	Disponibilité	Permet de remettre en ligne un LUN hors ligne afin que les hôtes puissent reprendre l'accès et les E/S.
Volume non restreint	Volume limité	Le volume est dans un état restreint et peut ne pas assurer un fonctionnement normal des E/S.	Disponibilité	Permet de remettre en ligne un volume restreint afin que les clients puissent y accéder à nouveau.
Mettre en ligne l'espace de noms NVMe	L'espace de noms NVMe est hors ligne	L'espace de noms NVMe est hors ligne et l'accès à l'hôte est indisponible.	Disponibilité	Permet de remettre en ligne un espace de noms NVMe hors ligne afin de rétablir l'accès à l'hôte.
Activer le LIF intercluster	Intercluster LIF en panne	Une interface LIF intercluster est hors service et la communication entre clusters peut être affectée.	Connectivité	Active une interface LIF intercluster pour rétablir la connectivité cluster-à-cluster utilisée pour la réplication.
Réactiver MetroCluster AUSO	MetroCluster basculement automatique non planifié désactivé	La commutation automatique non planifiée est désactivée sur ce cluster.	Disponibilité	Réactive la commutation automatique non planifiée (AUSO) afin que la protection MetroCluster fonctionne comme prévu.
Configurer le réseau du Service Processor	Le processeur de service n'est pas configuré	Le réseau du Service Processor (SP) n'est pas configuré.	Gestion	Configure les paramètres réseau du Service Processor (SP) pour activer l'accès à la gestion hors bande.
Attribuer les disques non attribués	Disques non attribués détectés	Des disques non attribués sont présents et leur capacité disponible peut être inutilisée. Attribuez ces disques à un nœud afin qu'ils puissent être utilisés pour le stockage.	Disponibilité	Attribue à un nœud les disques actuellement non attribués afin qu'ils puissent être utilisés pour le stockage.
Récupération de l'espace du volume racine	Espace faible sur le volume racine du nœud	L'espace disponible sur le volume racine du nœud est faible et peut affecter le fonctionnement normal du système.	Santé du système	Libère de l'espace sur le volume racine du nœud en supprimant le plus grand instantané ou le plus grand fichier de vidage mémoire. Les suppressions sont définitives.

Informations sur le copyright

Informations sur les marques commerciales