Présentation des événements de performances et des alertes

Active IQ Unified Manager 9.9

NetApp
April 05, 2024

Sommaire

Présentation des événements de performances et des alertes

Les événements de performance sont des notifications qu'Unified Manager génère automatiquement lorsqu'une condition prédéfinie se produit ou lorsqu'une valeur de compteur de performances franchit un seuil. Les événements vous aident à identifier les problèmes de performance dans les clusters surveillés.

Vous pouvez configurer des alertes pour envoyer automatiquement une notification par e-mail lorsque des événements de performance de certains types de gravité se produisent.

Sources des événements de performance

Les événements de performance sont des problèmes liés aux performances des charges de travail sur un cluster. Ils vous aident à identifier les objets de stockage avec des temps de réponse lents, également appelés « latence élevée ». Avec d'autres événements de santé qui se sont produits en même temps, vous pouvez déterminer les problèmes qui pourraient avoir causé, ou contribué à, les délais de réponse lents.

Unified Manager reçoit des événements de performance des sources suivantes :

- **Événements de politique de seuil de performances définis par l'utilisateur**

  Problèmes de performances basés sur des valeurs de seuil personnalisées que vous avez définies. Vous configurez des règles de seuil de performances pour les objets de stockage, par exemple des agrégats et des volumes, de sorte que les événements soient générés lorsqu'une valeur de seuil pour un compteur de performances a été atteinte.

  Vous devez définir une règle de seuil de performances et l'affecter à un objet de stockage pour recevoir ces événements.

- **Événements de politique de seuil de performances définis par le système**

  Problèmes de performances basés sur des valeurs seuils définies par le système. Ces règles de seuil sont incluses dans l'installation de Unified Manager afin de couvrir les problèmes de performance les plus courants.

  Ces règles de seuil sont activées par défaut et vous pouvez afficher des événements peu après l'ajout d'un cluster.

- **Événements seuil de performances dynamiques**

  Problèmes de performance dus à des défaillances ou à des erreurs dans une infrastructure IT, ou à la sur-utilisation des ressources du cluster par les charges de travail. La cause de ces événements peut être un simple problème qui se corrige au cours d'un certain temps ou qui peut être résolu par une réparation ou un changement de configuration. Un événement à seuil dynamique indique que les workloads d'un système ONTAP sont lents en raison d'autres workloads dont l'utilisation des composants du cluster partagé est élevée.

  Ces seuils sont activés par défaut et vous pouvez afficher des événements après trois jours de collecte des données d'un nouveau cluster.

Types de sévérité des événements de performance

Chaque événement de performance est associé à un type de gravité pour vous aider à hiérarchiser les événements nécessitant une action corrective immédiate.

- **Critique**

  Un événement sur les performances peut entraîner une interruption des services si des actions correctives ne sont pas prises immédiatement.

  Les événements critiques sont envoyés à partir de seuils définis par l'utilisateur uniquement.

- **Avertissement**

  Un compteur de performances pour un objet de cluster est hors de la plage normale et doit être surveillé pour vérifier qu'il n'atteint pas la gravité critique. Les événements de ce niveau de gravité n'entraînent pas d'interruption des services, mais une action corrective immédiate peut ne pas être nécessaire.

  Les événements d'avertissement sont envoyés à partir de seuils définis par l'utilisateur, définis par le système ou dynamiques.

- **Information**

  L'événement se produit lorsqu'un nouvel objet est découvert ou lorsqu'une action utilisateur est exécutée. Par exemple, lorsqu'un objet de stockage est supprimé ou en cas de modification de la configuration, l'événement contenant des informations de type de gravité est généré.

  Les événements d'informations sont envoyés directement depuis ONTAP lorsqu'il détecte une modification de configuration.

Modifications de configuration détectées par Unified Manager

Unified Manager surveille vos clusters pour modifier la configuration, ce qui vous permet de déterminer si une modification a pu être causée ou contribué à un événement de performances. Les pages de l'Explorateur de performances affichent une icône d'événement de changement (●) pour indiquer la date et l'heure de détection de la modification.

Vous pouvez consulter les graphiques de performances dans les pages de l'explorateur de performances et dans la page analyse de la charge de travail pour voir si l'événement de modification a affecté les performances de l'objet de cluster sélectionné. Si la modification a été détectée en même temps qu'un événement de performance ou à peu près, la modification peut avoir contribué au problème, qui a déclenché l'alerte d'événement.

Unified Manager peut détecter les événements de modification suivants, classés dans la catégorie « événements d'information » :

- Un volume est déplacé entre agrégats.

  Unified Manager peut détecter lorsque le déplacement est en cours, terminé ou échoué. Lorsqu'Unified Manager est inactif pendant le déplacement d'un volume, lors de sa sauvegarde, il détecte le déplacement

de volume et affiche un événement de modification pour celui-ci.

- Le débit (Mbit/s ou IOPS) d'un groupe de règles de QoS contenant un ou plusieurs changements de charge de travail surveillés.

  La modification de la limite d'un groupe de règles peut entraîner des pics intermittents de latence (temps de réponse), qui peuvent également déclencher des événements pour le groupe de règles. La latence revient progressivement à la normale et tous les événements provoqués par les pics deviennent obsolètes.

- Un nœud d'une paire haute disponibilité prend le relais ou renvoie le stockage de son nœud partenaire.

  Unified Manager peut détecter la fin de l'opération de basculement, de basculement partiel ou de rétablissement. Si le basculement est causé par un nœud paniqué, Unified Manager ne détecte pas l'événement.

- Une opération de mise à niveau ou de restauration de ONTAP a été effectuée correctement.

  La version précédente et la nouvelle version sont affichées.

Que se passe-t-il lorsqu'un événement est reçu

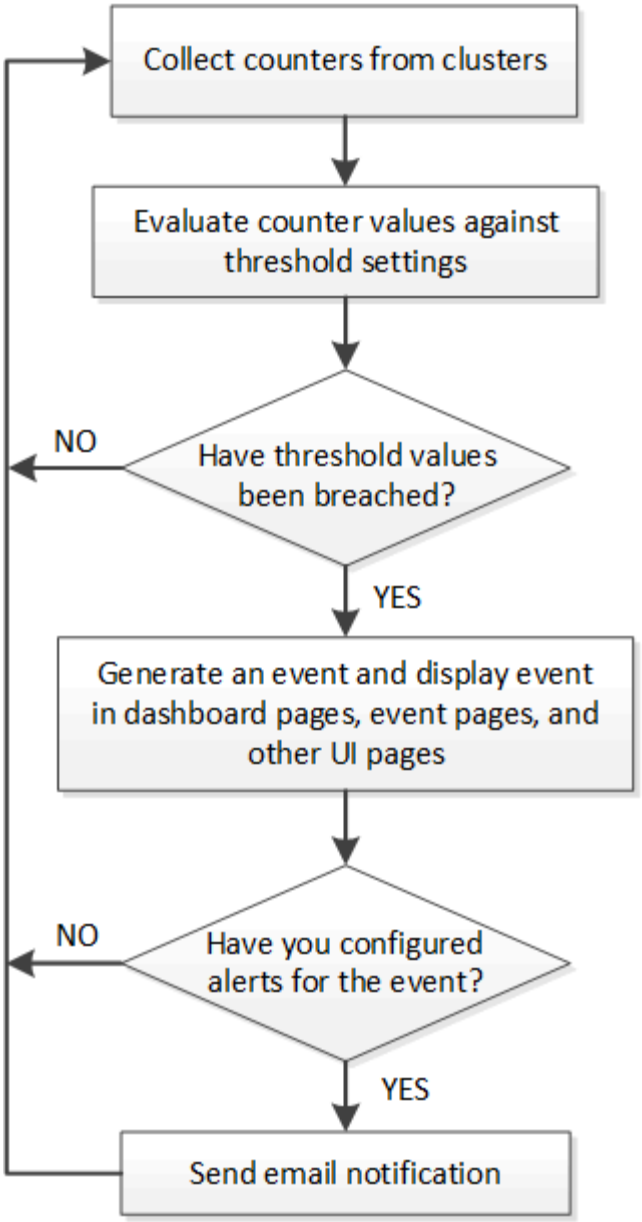
Lorsqu'Unified Manager reçoit un événement, celui-ci s'affiche sur la page Tableau de bord, dans la page d'inventaire de la gestion des événements, dans les onglets Summary et Explorer de la page Cluster/Performance, ainsi que dans la page d'inventaire spécifique à chaque objet (par exemple, la page d'inventaire volumes/Health).

Lorsque Unified Manager détecte plusieurs occurrences continues de la même condition d'événement pour le même composant de cluster, il traite toutes les occurrences comme un événement unique et non comme des événements distincts. La durée de l'événement est incrémentée pour indiquer que l'événement est toujours actif.

En fonction de la configuration des paramètres dans la page Configuration des alertes, vous pouvez avertir d'autres utilisateurs de ces événements. L'alerte entraîne le lancement des actions suivantes :

- Un e-mail sur l'événement peut être envoyé à tous les utilisateurs d'Unified Manager Administrator.
- L'événement peut être envoyé à d'autres destinataires de courrier électronique.
- Une interruption SNMP peut être envoyée au récepteur d'interruption.
- Un script personnalisé peut être exécuté pour exécuter une action.

Ce flux de travail est présenté dans le schéma suivant.



Les informations contenues dans un e-mail d'alerte

Dans les e-mails d'alerte Unified Manager, vous indiquez le type d'événement, la gravité de l'événement, le nom de la règle ou le seuil non respecté pour provoquer l'événement et la description de l'événement. L'e-mail fournit également un lien hypertexte pour chaque événement qui vous permet d'afficher la page de détails de l'événement dans l'interface utilisateur.

Les e-mails d'alerte sont envoyés à tous les utilisateurs qui se sont abonnés pour recevoir des alertes.

Si un compteur de performances ou une valeur de capacité a un changement important pendant une période de collecte, cela peut provoquer le déclenchement d'un événement critique et d'un événement d'avertissement en même temps pour la même stratégie de seuil. Dans ce cas, vous pouvez recevoir un e-mail pour l'événement d'avertissement et un autre pour l'événement critique. En effet, Unified Manager vous permet de vous abonner séparément pour recevoir des alertes en cas d'avertissement ou de franchissement de seuils critiques.

Voici un exemple d'e-mail d'alerte :

```
From: 10.11.12.13@company.com
Sent: Tuesday, May 1, 2018 7:45 PM
To: sclaus@company.com; user1@company.com
Subject: Alert from Active IQ Unified Manager: Thin-Provisioned Volume Space at Risk (State: New)

A risk was generated by 10.11.12.13 that requires your attention.

Risk            - Thin-Provisioned Volume Space At Risk
Impact Area     - Capacity
Severity        - Warning
State           - New
Source          - svm_n1:/sm_vol_23
Cluster Name    - fas3250-39-33-37
Cluster FQDN    - fas3250-39-33-37-cm.company.com
Trigger Condition - The thinly provisioned capacity of the volume is 45.73% of the available space on the
host aggregate. The capacity of the volume is at risk because of aggregate capacity issues.

Event details:
https://10.11.12.13:443/events/94

Source details:
https://10.11.12.13:443/health/volumes/106

Alert details:
https://10.11.12.13:443/alerting/1
```

Ajout d'alertes

Vous pouvez configurer des alertes pour vous avertir lorsqu'un événement particulier est généré. Vous pouvez configurer les alertes pour une seule ressource, pour un groupe de ressources ou pour les événements d'un type de sévérité particulier. Vous pouvez spécifier la fréquence à laquelle vous souhaitez être averti et associer un script à l'alerte.

Avant de commencer

- Vous devez avoir configuré des paramètres de notification tels que l'adresse e-mail de l'utilisateur, le serveur SMTP et l'hôte d'interruption SNMP pour permettre au serveur Active IQ Unified Manager d'utiliser ces paramètres pour envoyer des notifications aux utilisateurs lorsqu'un événement est généré.
- Vous devez connaître les ressources et les événements pour lesquels vous souhaitez déclencher l'alerte, ainsi que les noms d'utilisateur ou adresses e-mail des utilisateurs que vous souhaitez notifier.
- Si vous souhaitez que le script soit exécuté en fonction de l'événement, vous devez l'avoir ajouté à Unified Manager à l'aide de la page scripts.
- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Description de la tâche

Vous pouvez créer une alerte directement à partir de la page Détails de l'événement après avoir reçu un

événement en plus de créer une alerte à partir de la page Configuration de l'alerte, comme décrit ici.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Alert Setup**.
2. Dans la page **Configuration des alertes**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter une alerte**, cliquez sur **Nom**, puis entrez un nom et une description pour l'alerte.
4. Cliquez sur **Ressources**, puis sélectionnez les ressources à inclure ou à exclure de l'alerte.

   Vous pouvez définir un filtre en spécifiant une chaîne de texte dans le champ **Nom contient** pour sélectionner un groupe de ressources. En fonction de la chaîne de texte que vous spécifiez, la liste des ressources disponibles n'affiche que les ressources qui correspondent à la règle de filtre. La chaîne de texte que vous spécifiez est sensible à la casse.

   Si une ressource est conforme à la fois aux règles inclure et exclure que vous avez spécifiées, la règle d'exclusion est prioritaire sur la règle inclure et l'alerte n'est pas générée pour les événements liés à la ressource exclue.

5. Cliquez sur **Evénements**, puis sélectionnez les événements en fonction du nom de l'événement ou du type de gravité de l'événement pour lequel vous souhaitez déclencher une alerte.

   Pour sélectionner plusieurs événements, appuyez sur la touche Ctrl pendant que vous effectuez vos sélections.

6. Cliquez sur **actions** et sélectionnez les utilisateurs que vous souhaitez notifier, choisissez la fréquence de notification, choisissez si une interruption SNMP sera envoyée au récepteur d'interruption et affectez un script à exécuter lorsqu'une alerte est générée.

   Si vous modifiez l'adresse e-mail spécifiée pour l'utilisateur et rouvrez l'alerte pour modification, le champ Nom apparaît vide car l'adresse e-mail modifiée n'est plus mappée à l'utilisateur qui a été précédemment sélectionné. En outre, si vous avez modifié l'adresse e-mail de l'utilisateur sélectionné à partir de la page utilisateurs, l'adresse e-mail modifiée n'est pas mise à jour pour l'utilisateur sélectionné.

   Vous pouvez également choisir de notifier les utilisateurs via les interruptions SNMP.

7. Cliquez sur **Enregistrer**.

Exemple d'ajout d'une alerte

Dans cet exemple, vous apprendrez à créer une alerte conforme aux exigences suivantes :

- Nom de l'alerte : HealthTest
- Ressources : inclut tous les volumes dont le nom contient « abc » et exclut tous les volumes dont le nom contient « xyz ».
- Événements : inclut tous les événements de santé critiques
- Actions : inclut «ample@domain.com», un script «Test», et l'utilisateur doit être averti toutes les 15 minutes

Effectuez les opérations suivantes dans la boîte de dialogue Ajouter une alerte :

1. Cliquez sur **Nom** et saisissez `HealthTest` Dans le champ **Nom d'alerte**.
2. Cliquez sur **Ressources** et, dans l'onglet inclure, sélectionnez **volumes** dans la liste déroulante.
   a. Entrez `abc` Dans le champ **Name contient** pour afficher les volumes dont le nom contient « abc ».
   b. Sélectionnez **<<All Volumes whose name contains 'abc'>>** dans la zone Ressources disponibles, puis déplacez-le dans la zone Ressources sélectionnées.
   c. Cliquez sur **exclure**, puis saisissez `xyz` Dans le champ **Name contient**, puis cliquez sur **Add**.
3. Cliquez sur **Evénements**, puis sélectionnez **critique** dans le champ gravité de l'événement.
4. Sélectionnez **tous les événements critiques** dans la zone événements de correspondance et déplacez-le dans la zone événements sélectionnés.
5. Cliquez sur **actions**, puis saisissez `sample@domain.com` Dans le champ Alert ces utilisateurs.
6. Sélectionnez **rappeler toutes les 15 minutes** pour avertir l'utilisateur toutes les 15 minutes.

   Vous pouvez configurer une alerte pour qu'elle envoie régulièrement des notifications aux destinataires pendant une heure donnée. Vous devez déterminer l'heure à laquelle la notification d'événement est active pour l'alerte.

7. Dans le menu Select script to Execute, sélectionnez **Test** script.
8. Cliquez sur **Enregistrer**.

Ajout d'alertes en cas d'événements de performances

Vous pouvez configurer les alertes en cas d'événements de performance individuels comme n'importe quel autre événement reçu par Unified Manager. Par ailleurs, si vous souhaitez traiter tous les événements de performance comme si un e-mail est envoyé à la même personne, vous pouvez créer une seule alerte pour vous informer en cas de déclenchement d'événements de performance critiques ou d'avertissement.

Avant de commencer

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Description de la tâche

L'exemple ci-dessous montre comment créer un événement pour toutes les latence critique, les IOPS et les Mo/sec. Vous pouvez utiliser cette même méthodologie pour sélectionner des événements à partir de tous les compteurs de performances et pour tous les événements d'avertissement.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Alert Setup**.
2. Dans la page **Configuration des alertes**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter une alerte**, cliquez sur **Nom**, puis entrez un nom et une description pour l'alerte.
4. Ne sélectionnez aucune ressource sur la page **Ressources**.

   Aucune ressource n'est sélectionnée, l'alerte est appliquée à tous les clusters, agrégats, volumes, etc.

Pour lesquels ces événements sont reçus.

5. Cliquez sur **Evénements** et effectuez les opérations suivantes :
   a. Dans la liste gravité de l'événement, sélectionnez **critique**.
   b. Dans le champ Nom de l'événement contient, entrez `latency` puis cliquez sur la flèche pour sélectionner tous les événements correspondants.
   c. Dans le champ Nom de l'événement contient, entrez `iops` puis cliquez sur la flèche pour sélectionner tous les événements correspondants.
   d. Dans le champ Nom de l'événement contient, entrez `mbps` puis cliquez sur la flèche pour sélectionner tous les événements correspondants.
6. Cliquez sur **actions**, puis sélectionnez le nom de l'utilisateur qui recevra l'e-mail d'alerte dans le champ **Alert thavent Users**.
7. Configurez toutes les autres options de cette page pour l'émission de taps SNMP et l'exécution d'un script.
8. Cliquez sur **Enregistrer**.

Types de règles de seuils de performance définies par le système

Unified Manager fournit des règles de seuil standard qui contrôlent les performances du cluster et génèrent automatiquement des événements. Ces règles sont activées par défaut et génèrent des événements d'avertissement ou d'information lorsque les seuils de performances surveillés sont enfreintes.

> Les règles de seuil de performance définies par le système ne sont pas activées sur les systèmes Cloud Volumes ONTAP, ONTAP Edge ou ONTAP Select.

Si vous recevez des événements inutiles provenant de règles de seuils de performance définies par le système, vous pouvez désactiver les événements de règles individuelles à partir de la page de configuration des événements.

Règles de seuil du cluster

Les règles de seuil des performances du cluster définies par le système sont attribuées, par défaut, à chaque cluster contrôlé par Unified Manager :

- **Déséquilibre de charge du groupe**

  Identifie les situations où un nœud fonctionne à une charge bien plus élevée que les autres nœuds du cluster et peut donc affecter les latences des charges de travail.

  Pour ce faire, il compare la valeur en termes de capacité des performances utilisée par tous les nœuds du cluster afin de voir si la charge est différente de 30 % entre tous les nœuds. Il s'agit d'un incident d'avertissement.

- **Déséquilibre de capacité du groupe**

  Identifie les situations où la capacité utilisée d'un agrégat est bien plus élevée que celle des autres agrégats du cluster et affecte donc potentiellement l'espace requis pour les opérations.

Pour ce faire, elle compare la valeur de capacité utilisée de tous les agrégats du cluster afin de voir si la différence entre 70 % d'un agrégat. Il s'agit d'un incident d'avertissement.

Règles de seuil des nœuds

Les règles de seuil de performance des nœuds définies par le système sont attribuées par défaut à chaque nœud des clusters contrôlé par Unified Manager :

- **Seuil de capacité utilisée de performances dépassé**

  Identifie les situations dans lesquelles un nœud fonctionne au-delà des limites de son efficacité opérationnelle et risque par conséquent d'affecter la latence des charges de travail.

  Pour ce faire, il recherche des nœuds qui utilisent plus de 100 % de leur capacité en performance pendant plus de 12 heures. Il s'agit d'un incident d'avertissement.

- **Surutilisation de la paire HA de nœuds**

  Identifie les situations dans lesquelles les nœuds d'une paire haute disponibilité fonctionnent au-dessus des limites de l'efficacité opérationnelle de la paire haute disponibilité.

  Pour ce faire, le système étudie la valeur de la capacité en termes de performances utilisée pour les deux nœuds de la paire haute disponibilité. Si la capacité de performance combinée des deux nœuds dépasse 200 % pendant plus de 12 heures, un basculement de contrôleur affecte les latences des charges de travail. Il s'agit d'un événement informatif.

- **Fragmentation de disque de nœud**

  Identifie les situations où un ou plusieurs disques d'un agrégat sont fragmentés, ralentissant les principaux services système et potentiellement affecter les latences des charges de travail sur un nœud.

  Pour ce faire, il s'agit de certains ratios d'opération de lecture et d'écriture sur tous les agrégats d'un nœud. Cette règle peut également être déclenchée lors de la resynchronisation SyncMirror ou lorsque des erreurs sont détectées lors des opérations de nettoyage du disque. Il s'agit d'un incident d'avertissement.

  > La règle de « fragmentation des disques des nœuds » analyse les agrégats uniquement composés de disques durs ; les agrégats Flash Pool, SSD et FabricPool ne sont pas analysés.

Règles de seuil agrégées

La règle de seuil de performance des agrégats définis par le système est attribuée par défaut à chaque agrégat des clusters contrôlé par Unified Manager :

- **Disques agrégés sur-utilisés**

  Identifie les situations dans lesquelles un agrégat fonctionne au-delà des limites de son efficacité opérationnelle et peut ainsi affecter le latence des charges de travail. Ce cas est identifié par la recherche d'agrégats où les disques de l'agrégat sont utilisés à plus de 95 % pendant plus de 30 minutes. Cette règle multicondition effectue alors l'analyse suivante pour déterminer la cause du problème :

  - Un disque de l'agrégat est-il actuellement en cours d'opération de maintenance en arrière-plan ?

    Certaines activités de maintenance en arrière-plan qu'un disque peut être en cours de reconstruction

sont : disque, nettoyage de disque, resynchronisation SyncMirror et reparité.

- Existe-t-il un goulet d'étranglement au niveau des communications dans l'interconnexion Fibre Channel du tiroir disque ?
- L'agrégat dispose-t-il trop peu d'espace libre ? Un événement d'avertissement est émis pour cette politique uniquement si une ou plusieurs des trois politiques subordonnées sont également considérées comme enfreintes. Un événement de performances n'est pas déclenché si seuls les disques de l'agrégat sont utilisés à plus de 95 %.

> La politique « d'agrégation de disques sur-utilisés » analyse les agrégats de disques durs uniquement et les agrégats Flash Pool (hybrides) ; les agrégats SSD et FabricPool ne sont pas analysés.

Règles de seuil de latence des workloads

Les règles de seuil de latence de la charge de travail définies par le système sont attribuées à toute charge de travail dont la règle de niveau de service de performance est configurée et dont la valeur de « latence attendue » est définie :

- **Seuil de latence de volume de charge de travail/LUN dépassé tel que défini par le niveau de service de performances**

  Identifie les volumes (partages de fichiers) et les LUN qui ont dépassé leur limite de « latence attendue » et qui ont un impact sur les performances des charges de travail. Il s'agit d'un incident d'avertissement.

  Pour ce faire, il recherche des charges de travail qui ont dépassé la valeur de latence prévue pour 30 % de l'heure précédente.

Règles de seuil de QoS

Les règles de seuil de performances de QoS définies par le système sont attribuées à toute charge de travail dont la règle de débit maximal est la QoS ONTAP configurée (IOPS, IOPS/To ou Mo/s). Unified Manager déclenche un événement lorsque la valeur du débit des workloads est inférieure de 15 % à la valeur de la QoS configurée :

- **QoS Max IOPS ou seuil MB/s**

  Identifie les volumes et les LUN qui ont dépassé leur limite maximale en termes d'IOPS ou de débit en Mo/s de qualité de service, et qui affectent la latence des charges de travail. Il s'agit d'un incident d'avertissement.

  Lorsqu'une seule charge de travail est attribuée à un groupe de règles, elle recherche les charges de travail qui ont dépassé le seuil de débit maximal défini dans le groupe de règles QoS attribué au cours de chaque période de collecte pendant l'heure précédente.

  Lorsque plusieurs charges de travail partagent une seule règle de QoS, celle-ci est ajoutée en ajoutant les IOPS ou les Mo/s de tous les workloads de la règle et en vérifiant le total dans la limite.

- **QoS Peak IOPS/To ou IOPS/To avec seuil de taille de bloc**

  Identifie les volumes qui ont dépassé la limite de débit en IOPS/To adaptative pour la qualité de service (ou IOPS/To avec limite de taille de bloc), tout en affectant la latence de la charge de travail. Il s'agit d'un incident d'avertissement.

Pour ce faire, la conversion du seuil maximal d'IOPS/To défini dans la règle de QoS adaptative en une valeur maximale d'IOPS basée sur la taille de chaque volume. Elle recherche les volumes qui ont dépassé la limite d'IOPS maximale de QoS au cours de chaque période de collecte de performances pendant l'heure précédente.

> Cette règle s'applique aux volumes uniquement lorsque le cluster est installé avec ONTAP 9.3 et les versions ultérieures.

Lorsque l'élément « taille de bloc » a été défini dans la règle de QoS adaptative, le seuil est converti en valeur MB/s maximale basée sur la taille de chaque volume. Ensuite, il recherche les volumes qui ont dépassé la limite de qualité de service en Mo/s au cours de chaque période de collecte des performances pour l'heure précédente.

> Cette règle s'applique aux volumes uniquement lorsque le cluster est installé avec ONTAP 9.5 et les versions ultérieures.