Comprendre les événements et alertes de performance

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/fr-fr/active-iq-unified-manager-918/performance-checker/concept_understand_performance_events_and_alerts.html on November 13, 2026. Always check docs.netapp.com for the latest.

Sommaire

Comprendre les événements et alertes de performance . . . 1
- Comprendre les événements et alertes de performance dans Active IQ Unified Manager . . . 1
- Identifier les sources des événements de performance dans Active IQ Unified Manager . . . 1
- Priorisez les événements de performance par niveau de gravité dans Active IQ Unified Manager . . . 2
- Surveillez les modifications de configuration détectées par Active IQ Unified Manager . . . 3
- Comprendre les politiques de seuil de performance définies par le système dans Active IQ Unified Manager . . . 3
  - Politiques de seuil du cluster . . . 4
  - Politiques de seuil de nœud . . . 4
  - Politiques de seuil d'agrégat . . . 5
  - Politiques de seuil de latence du workload . . . 5
  - Politiques de seuil de QoS . . . 6
- Analysez les événements et notifications de performance dans Active IQ Unified Manager . . . 6
  - Analyse d'événements . . . 7
  - État de l'événement . . . 7
  - Notification d'événement . . . 8
  - Interaction avec l'événement . . . 8
- Comprendre comment Active IQ Unified Manager détermine l'impact sur les performances d'un événement . . . 8
- Comprendre les composants du cluster et la contention dans Active IQ Unified Manager . . . 9
- Identifier les rôles de la charge de travail dans les événements de performance dans Active IQ Unified Manager . . . 11

Comprendre les événements et alertes de performance

Comprendre les événements et alertes de performance dans Active IQ Unified Manager

Les événements de performance sont des incidents liés aux performances des workloads sur un cluster. Ils vous aident à identifier les workloads dont les temps de réponse sont lents. Associés aux événements de santé survenus au même moment, ils vous permettent de déterminer les problèmes qui ont pu causer ces temps de réponse lents ou y contribuer.

Lorsque Unified Manager détecte plusieurs occurrences de la même condition d'événement pour le même composant du cluster, il traite toutes les occurrences comme un seul événement, et non comme des événements distincts.

Vous pouvez configurer des alertes pour envoyer automatiquement des notifications par e-mail lorsque des événements de performance d'un certain niveau de gravité se produisent.

Identifier les sources des événements de performance dans Active IQ Unified Manager

Les événements de performance sont des problèmes liés aux performances des workloads sur un cluster. Ils vous aident à identifier les objets de stockage présentant des temps de réponse lents, également appelés latence élevée. Associés à d'autres événements d'intégrité survenus au même moment, ils vous permettent de déterminer les problèmes susceptibles d'avoir causé, ou contribué à, les temps de réponse lents.

Unified Manager reçoit les événements de performance des sources suivantes :

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

  Problèmes de performance liés aux valeurs de seuil personnalisées que vous avez définies. Vous configurez des politiques de seuil de performance pour les objets de stockage, par exemple les agrégats et les volumes, afin que des événements soient générés lorsqu'une valeur de seuil d'un compteur de performance est dépassée.

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

- **Événements liés à la politique de seuil de performance définie par le système**

  Les problèmes de performance sont basés sur des valeurs seuils définies par le système. Ces politiques de seuil sont incluses dans l'installation d'Unified Manager afin de couvrir les problèmes de performance courants.

  Ces politiques de seuil sont activées par défaut, et vous pourriez voir des événements peu de temps après l'ajout d'un cluster.

- **Événements de seuil de performance dynamique**

  Les problèmes de performance résultent de défaillances ou d'erreurs dans l'infrastructure informatique, ou de workloads qui surutilisent les ressources du cluster. La cause de ces événements peut être un simple problème qui se corrige de lui-même avec le temps ou auquel il peut être remédié par une réparation ou une modification de la configuration. Un événement de seuil dynamique indique que les workloads sur un système ONTAP sont lents en raison d'autres workloads qui utilisent fortement les composants partagés du cluster.

  Ces seuils sont activés par défaut, et vous pourriez observer des événements après trois jours de collecte de données à partir d'un nouveau cluster.

Priorisez les événements de performance par niveau de gravité dans Active IQ Unified Manager

Chaque événement de performance est associé à un niveau de gravité afin de vous aider à prioriser les événements qui nécessitent une action corrective immédiate.

- **Critique**

  Un incident de performance s'est produit et pourrait entraîner une interruption de service si des mesures correctives ne sont pas prises immédiatement.

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

- **Avertissement**

  Un compteur de performance d'un objet de cluster présente une valeur anormale et doit être surveillé afin d'éviter qu'il n'atteigne le seuil critique. Les événements de cette gravité n'entraînent pas d'interruption de service et ne nécessitent généralement pas d'intervention immédiate.

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

- **Informations**

  Cet événement se produit lorsqu'un nouvel objet est découvert ou lorsqu'une action utilisateur est effectuée. Par exemple, lorsqu'un objet de stockage est supprimé ou que des modifications de configuration sont apportées, un événement de type de gravité Information est généré.

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

Pour plus d'informations, consultez les liens suivants :

- "Que se passe-t-il lorsqu'un événement est reçu"
- "Quelles informations contient un courriel d'alerte"
- "Ajout d'alertes"
- "Ajout d'alertes pour les événements de performance"

Surveillez les modifications de configuration détectées par Active IQ Unified Manager

Unified Manager surveille vos clusters pour détecter les modifications de configuration afin de vous aider à déterminer si une modification a pu provoquer ou contribuer à un événement de performances. Les pages de l'Explorateur de performances affichent une icône d'événement de modification (●) pour indiquer la date et l'heure à laquelle la modification a été détectée.

Vous pouvez consulter les graphiques de performance dans les pages de l'Explorateur de performances et dans la page Analyse de la charge de travail pour déterminer si l'événement de modification a eu un impact sur les performances de l'objet de cluster sélectionné. Si la modification a été détectée simultanément ou presque à un événement de performance, elle a pu contribuer au problème et déclencher l'alerte d'événement.

Unified Manager peut détecter les événements de changement suivants, qui sont catégorisés comme événements d'information :

- Un volume se déplace entre les agrégats.

  Unified Manager peut détecter l'état d'avancement, la fin ou l'échec d'un déplacement de volume. En cas d'indisponibilité d'Unified Manager pendant un déplacement de volume, une fois remis en service, il détecte le déplacement et affiche un événement de modification.

- La limite de débit (Mo/s ou IOPS) d'un groupe de stratégies QoS contenant une ou plusieurs charges de travail surveillées change.

  La modification d'une limite de groupe de règles peut entraîner des pics intermittents de latence (temps de réponse), susceptibles de déclencher des événements pour ce groupe. La latence revient progressivement à la normale et les événements provoqués par ces pics deviennent caducs.

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

  Unified Manager peut détecter la fin d'une prise de contrôle, d'une prise de contrôle partielle ou d'une restitution. En revanche, si la prise de contrôle est due à un nœud défaillant, Unified Manager ne détecte pas l'événement.

- Une opération de mise à niveau ou de rétablissement d'ONTAP s'est terminée avec succès.

  La version précédente et la nouvelle version sont affichées.

Comprendre les politiques de seuil de performance définies par le système dans Active IQ Unified Manager

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

Les politiques 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 politiques de seuil de performance définies par le système, vous pouvez désactiver les événements pour chaque politique individuellement à partir de la page Configuration des événements.

Politiques de seuil du cluster

Les politiques de seuil de performance de cluster définies par le système sont attribuées, par défaut, à chaque cluster surveillé par Unified Manager :

- **Déséquilibre de charge du cluster**

  Identifie les situations dans lesquelles un nœud fonctionne avec une charge bien plus élevée que les autres nœuds du cluster et peut donc potentiellement affecter les latences du workload.

  Pour ce faire, il compare la valeur de capacité de performance utilisée pour tous les nœuds d'un cluster afin de déterminer si l'un d'eux a dépassé le seuil de 30 % pendant plus de 24 heures. Il s'agit d'un événement d'alerte.

- **Déséquilibre de capacité du cluster**

  Identifie les situations dans lesquelles un agrégat a une capacité utilisée beaucoup plus élevée que les autres agrégats du cluster et peut donc potentiellement affecter l'espace requis pour les opérations.

  Il procède en comparant la capacité utilisée de tous les agrégats du cluster afin de détecter une éventuelle différence de 70 % entre eux. Il s'agit d'un événement d'alerte.

Politiques de seuil de nœud

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

- **Seuil de capacité de performance utilisée dépassé**

  Identifie les situations dans lesquelles un seul nœud fonctionne au-delà des limites de son efficacité opérationnelle et peut donc potentiellement affecter les latences des workloads.

  Il détecte les nœuds qui utilisent plus de 100 % de leur capacité de performance pendant plus de 12 heures. Il s'agit d'un événement d'alerte.

- **Paire haute disponibilité de nœuds surutilisée**

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

  Le système effectue cela en examinant la valeur de capacité de performance utilisée pour les deux nœuds de la paire haute disponibilité. Si la capacité de performance utilisée combinée des deux nœuds dépasse 200 % pendant plus de 12 heures, un basculement du contrôleur aura un impact sur la latence des workloads. Cet événement est informatif.

- **Fragmentation du disque du nœud**

  Identifie les situations dans lesquelles un ou plusieurs disques d'un agrégat sont fragmentés, ce qui ralentit les services système essentiels et peut potentiellement affecter les latences des workload sur un nœud.

Il le fait en examinant certains ratios d'opérations de lecture et d'écriture sur l'ensemble des agrégats d'un nœud. Cette politique peut également être déclenchée lors d'une resynchronisation SyncMirror ou lorsque des erreurs sont détectées lors d'opérations de nettoyage de disque. Il s'agit d'un événement d'avertissement.

La politique « Fragmentation du disque du nœud » analyse uniquement les agrégats HDD ; les agrégats Flash Pool, SSD et FabricPool ne sont pas analysés.

Politiques de seuil d'agrégat

La politique de seuil de performance d'agrégat définie par le système est attribuée par défaut à chaque agrégat des clusters surveillés par Unified Manager :

- **Disques d'agrégat surutilisés**

  Ce système identifie les situations dans lesquelles un agrégat fonctionne au-delà des limites de son efficacité opérationnelle, ce qui peut affecter les latences de workload. Il repère ces situations en recherchant les agrégats dont les disques sont utilisés à plus de 95 % pendant plus de 30 minutes. Cette politique multiconditionnelle effectue ensuite l'analyse suivante pour aider à déterminer la cause du problème :

  - Un disque de l'agrégat fait-il actuellement l'objet d'une activité de maintenance en arrière-plan ?

    Parmi les activités de maintenance en arrière-plan qu'un disque peut subir figurent la reconstruction du disque, le nettoyage du disque, la resynchronisation de SyncMirror et la réparation de la parité.

  - Existe-t-il un goulot d'étranglement des communications au niveau de l'interconnexion Fibre Channel du tiroir disque ?
  - L'espace libre est-il insuffisant dans l'agrégat ? Un événement d'avertissement est émis pour cette stratégie uniquement si une (ou plusieurs) des trois stratégies subordonnées est également considérée comme non respectée. Aucun événement de performance n'est déclenché si seuls les disques de l'agrégat sont utilisés à plus de 95 %.

La politique « Surutilisation des disques d'agrégat » analyse les agrégats composés uniquement de HDD et les agrégats Flash Pool (hybrides) ; les agrégats SSD et FabricPool ne sont pas analysés.

Politiques de seuil de latence du workload

Les politiques de seuil de latence de workload définies par le système sont attribuées à tout workload disposant d'une politique de niveau de service de performance configurée avec une valeur « latence attendue » définie :

- **Seuil de latence du volume/de la LUN du workload dépassé, conformément au niveau de service de performances**

  Identifie les volumes (partages de fichiers) et les LUN qui ont dépassé leur limite de "latence attendue" et qui affectent les performances du workload. Il s'agit d'un événement d'avertissement.

  Pour ce faire, il recherche les workloads qui ont dépassé la valeur de latence attendue pendant 30 % du temps au cours de l'heure précédente.

Politiques de seuil de QoS

Les politiques de seuil de performance QoS définies par le système sont attribuées à tout workload disposant d'une politique ONTAP QoS de débit maximal configurée (IOPS, IOPS/TB ou Mo/s). Unified Manager déclenche un événement lorsque la valeur de débit du workload est inférieure de 15 % à la valeur QoS configurée :

- **Seuil QoS max. en IOPS ou Mo/s**

  Identifie les volumes et les LUN qui ont dépassé leur limite maximale de QoS en IOPS ou en débit (Mo/s) et qui affectent la latence des workloads. Il s'agit d'un événement d'avertissement.

  Lorsqu'une seule workload est affectée à un groupe de stratégies, cela consiste à rechercher les workloads qui ont dépassé le seuil de débit maximal défini dans le groupe de stratégies QoS affecté au cours de chaque période de collecte de l'heure précédente.

  Lorsque plusieurs workloads partagent une seule politique QoS, celle-ci procède en additionnant les IOPS ou les MB/s de tous les workloads de la politique et en comparant ce total au seuil.

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

  Identifie les volumes ayant dépassé leur limite de débit de pointe IOPS/TB de la QoS adaptative (ou leur limite IOPS/TB avec taille de bloc) et qui affectent la latence du workload. Il s'agit d'un événement d'avertissement.

  Il le fait en convertissant le seuil maximal d'IOPS/TB défini dans la politique de QoS adaptative en une valeur maximale d'IOPS QoS basée sur la taille de chaque volume, puis en recherchant les volumes qui ont dépassé le nombre maximal d'IOPS QoS au cours de chaque période de collecte des performances pendant l'heure précédente.

  > Cette politique s'applique aux volumes uniquement lorsque le cluster est installé avec le logiciel ONTAP 9.3 ou une version ultérieure.

  Lorsque l'élément "block size" a été défini dans la politique QoS adaptative, le seuil est converti en une valeur QoS maximale en Mo/s en fonction de la taille de chaque volume. Ensuite, le système recherche les volumes qui ont dépassé la valeur QoS maximale en Mo/s pendant chaque période de collecte des performances de l'heure précédente.

  > Cette politique s'applique aux volumes uniquement lorsque le cluster est installé avec le logiciel ONTAP 9.5 ou une version ultérieure.

Analysez les événements et notifications de performance dans Active IQ Unified Manager

Les événements de performance vous informent des problèmes de performances d'E/S sur un workload causés par une contention sur un composant du cluster. Unified Manager analyse l'événement pour identifier tous les workloads concernés, le composant en contention et déterminer si le problème persiste et nécessite une intervention.

Unified Manager surveille la latence d'E/S (temps de réponse) et les IOPS (opérations) des volumes sur un cluster. Lorsque d'autres workloads sollicitent excessivement un composant du cluster, par exemple, le composant est en contention et ne peut pas fonctionner à un niveau optimal pour répondre aux exigences du

workload. Les performances des autres workloads qui utilisent le même composant peuvent être affectées, ce qui entraîne une augmentation de leur latence. Si la latence dépasse le seuil de performance dynamique, Unified Manager déclenche un événement de performance pour vous en informer.

Analyse d'événements

Unified Manager effectue les analyses suivantes, en utilisant les statistiques de performance des 15 derniers jours, afin d'identifier les workloads victimes, les workloads agresseurs et le composant du cluster impliqué dans un événement :

- Identifie les workloads victimes dont la latence a dépassé le seuil de performance dynamique, qui correspond à la limite supérieure de la prévision de latence :
  - Pour les volumes sur des agrégats hybrides HDD ou Flash Pool (niveau local), les événements ne sont déclenchés que lorsque la latence est supérieure à 5 millisecondes (ms) et que les IOPS sont supérieures à 10 opérations par seconde (ops/sec).
  - Pour les volumes sur des agrégats entièrement SSD ou des agrégats FabricPool (niveau cloud), les événements ne sont déclenchés que lorsque la latence est supérieure à 1 ms et que les IOPS sont supérieures à 100 ops/sec.
- Identifie le composant du cluster en contention.

  Si la latence des workloads victimes au niveau de l'interconnexion de cluster est supérieure à 1 ms, Unified Manager considère cela comme significatif et déclenche un événement pour l'interconnexion de cluster.

- Identifie les workloads perturbateurs qui surutilisent le composant du cluster et provoquent un état de contention.
- Classe les workloads concernés, en fonction de leur écart d'utilisation ou d'activité d'un composant du cluster, afin de déterminer quels bullies présentent la plus forte variation d'utilisation du composant du cluster et quelles victims sont les plus impactées.

Un événement peut ne se produire que pendant un bref instant, puis se corriger de lui-même une fois que le composant qu'il utilise n'est plus en situation de contention. Un événement continu est un événement qui se reproduit pour le même composant du cluster dans un intervalle de cinq minutes et reste à l'état actif. Pour les événements continus, Unified Manager déclenche une alerte après avoir détecté le même événement pendant deux intervalles d'analyse consécutifs.

Lorsqu'un événement est résolu, il reste disponible dans Unified Manager dans l'historique des problèmes de performance passés d'un volume. Chaque événement possède un identifiant unique qui précise son type, ainsi que les volumes, le cluster et les composants du cluster concernés.

Un seul volume peut être impliqué dans plusieurs événements simultanément.

État de l'événement

Les événements peuvent se trouver dans l'un des états suivants :

- **Actif**

  Indique que l'événement de performance est actuellement actif (nouveau ou confirmé). Le problème à l'origine de l'événement ne s'est pas corrigé ou n'a pas été résolu. Le compteur de performance de l'objet de stockage reste supérieur au seuil de performance.

- **Obsolète**

  Indique que l'événement n'est plus actif. Le problème à l'origine de l'événement s'est résolu de lui-même ou a été résolu. Le compteur de performances de l'objet de stockage ne dépasse plus le seuil de performance.

Notification d'événement

Les événements sont affichés sur la page Dashboard et sur de nombreuses autres pages de l'interface utilisateur, et des alertes pour ces événements sont envoyées aux adresses e-mail spécifiées. Vous pouvez consulter des informations d'analyse détaillées sur un événement et obtenir des suggestions pour le résoudre sur la page Event details et sur la page Workload Analysis.

Interaction avec l'événement

Sur la page Détails de l'événement et sur la page Analyse du workload, vous pouvez interagir avec les événements des manières suivantes :

- En déplaçant la souris sur un événement, un message s'affiche indiquant la date et l'heure de sa détection.

  S'il y a plusieurs événements pour la même période, le message affiche le nombre d'événements.

- Lorsque vous cliquez sur un seul événement, une boîte de dialogue s'affiche et présente des informations plus détaillées sur cet événement, notamment les composants du cluster impliqués.

  Le composant en cause est encerclé et surligné en rouge. Cliquez sur **Afficher l'analyse complète** pour consulter l'analyse complète sur la page Détails de l'événement. Si plusieurs événements se produisent pour la même période, la boîte de dialogue affiche les détails des trois événements les plus récents. Cliquez sur un événement pour afficher son analyse sur la page Détails de l'événement.

Comprendre comment Active IQ Unified Manager détermine l'impact sur les performances d'un événement

Unified Manager utilise les variations d'activité, d'utilisation, de débit d'écriture, d'utilisation des composants du cluster ou de latence d'E/S (temps de réponse) d'un workload pour déterminer le niveau d'impact sur les performances du workload. Ces informations déterminent le rôle de chaque workload dans l'événement et leur classement sur la page de détails de l'événement.

Unified Manager compare les dernières valeurs analysées pour un workload à la plage de valeurs attendue (prévision de latence). L'écart entre les dernières valeurs analysées et la plage de valeurs attendue permet d'identifier les workloads dont les performances ont été les plus affectées par l'événement.

Par exemple, supposons qu'un cluster contienne deux charges de travail : la charge de travail A et la charge de travail B. La latence prévue pour la charge de travail A est de 5 à 10 millisecondes par opération (ms/op) et sa latence réelle est généralement d'environ 7 ms/op. La latence prévue pour la charge de travail B est de 10 à 20 ms/op et sa latence réelle est généralement d'environ 15 ms/op. Les deux charges de travail respectent leurs prévisions de latence. En raison d'une contention sur le cluster, la latence des deux charges de travail augmente à 40 ms/op, dépassant ainsi le seuil de performance dynamique, qui correspond à la limite supérieure des prévisions de latence, et déclenchant des événements. L'écart de latence entre les valeurs attendues et les valeurs supérieures au seuil de performance est d'environ 33 ms/op pour la charge de travail A et d'environ 25 ms/op pour la charge de travail B. La latence des deux charges de travail atteint un pic de

40 ms/op, mais la charge de travail A a eu l'impact le plus important sur les performances, car elle présentait l'écart de latence le plus élevé, à 33 ms/op.

Sur la page Détails de l'événement, dans la section Diagnostic système, vous pouvez trier les workloads selon leur écart d'activité, d'utilisation ou de débit pour un composant du cluster. Vous pouvez également trier les workloads par latence. Lorsque vous sélectionnez une option de tri, Unified Manager analyse l'écart d'activité, d'utilisation, de débit ou de latence depuis la détection de l'événement par rapport aux valeurs attendues afin de déterminer l'ordre de tri des workloads. Pour la latence, les points rouges (🔴) indiquent le franchissement d'un seuil de performance par un workload victime, ainsi que l'impact qui en résulte sur la latence. Chaque point rouge indique un niveau d'écart de latence plus élevé, ce qui vous aide à identifier les workloads victimes dont la latence a été la plus affectée par un événement.

Comprendre les composants du cluster et la contention dans Active IQ Unified Manager

Vous pouvez identifier les problèmes de performance du cluster lorsqu'un composant du cluster est en contention. Les performances des workloads qui utilisent ce composant ralentissent et leur temps de réponse (latence) aux requêtes client augmente, ce qui déclenche un événement dans Unified Manager.

Un composant en situation de contention ne peut pas fonctionner à un niveau optimal. Ses performances ont diminué, et les performances des autres composants du cluster et des workloads, appelés « victimes », peuvent présenter une latence accrue. Pour sortir un composant de la contention, vous devez réduire son workload ou augmenter sa capacité à traiter davantage de travail, afin que les performances puissent revenir à des niveaux normaux. Comme Unified Manager collecte et analyse les performances des workloads à intervalles de cinq minutes, il détecte uniquement lorsqu'un composant du cluster est constamment surutilisé. Les pics transitoires de surutilisation qui ne durent qu'une courte période pendant l'intervalle de cinq minutes ne sont pas détectés.

Par exemple, un agrégat de stockage peut être en situation de contention parce qu'une ou plusieurs workloads qu'il contient se disputent le traitement de leurs requêtes d'E/S. D'autres workloads sur l'agrégat peuvent être affectés, ce qui entraîne une baisse de leurs performances. Pour réduire le niveau d'activité sur l'agrégat, vous pouvez prendre différentes mesures, par exemple déplacer une ou plusieurs workloads vers un agrégat ou un nœud moins sollicité, afin de réduire la demande globale de workload sur l'agrégat actuel. Pour un groupe de stratégies QoS, vous pouvez ajuster la limite de débit ou déplacer des workloads vers un autre groupe de stratégies, afin que les workloads ne soient plus limités.

Unified Manager surveille les composants de cluster suivants pour vous alerter lorsqu'ils sont en contention :

- **Réseau**

  Représente le temps d'attente des requêtes d'E/S par les protocoles réseau externes du cluster. Ce temps d'attente correspond au temps nécessaire pour que les transactions « transfer ready » soient terminées avant que le cluster puisse répondre à une requête d'E/S. Si le composant réseau est en contention, cela signifie qu'un temps d'attente élevé au niveau du protocole impacte la latence d'une ou plusieurs charges de travail.

- **Traitement réseau**

  Représente le composant logiciel du cluster impliqué dans le traitement des E/S entre la couche protocolaire et le cluster. Le nœud gérant le traitement réseau a peut-être changé depuis la détection de l'événement. Si le composant de traitement réseau est en contention, cela signifie qu'une utilisation élevée du nœud de traitement réseau impacte la latence d'un ou de plusieurs workloads.

Lors de l'utilisation d'un cluster All SAN Array en configuration active-active, la valeur de latence de traitement réseau est affichée pour les deux nœuds afin que vous puissiez vérifier que la charge est répartie équitablement entre eux.

- **Limite QoS maximale**

  Représente le paramètre de débit maximal (de pointe) du groupe de règles de qualité de service (QoS) du stockage attribué au workload. Si le composant du groupe de règles est en conflit, cela signifie que tous les workloads du groupe de règles sont limités par la limite de débit définie, ce qui affecte la latence d'un ou de plusieurs de ces workloads.

- **Limite minimale de QoS**

  Représente la latence d'un workload causée par le paramètre minimal de débit QoS (attendu) attribué à d'autres workloads. Si le minimum QoS défini sur certains workloads utilise la majeure partie de la bande passante pour garantir le débit promis, les autres workloads seront limités et présenteront une latence plus élevée.

- **Interconnexion de cluster**

  Représente les câbles et adaptateurs auxquels les nœuds du cluster sont physiquement connectés. Si le composant d'interconnexion de cluster est saturé, cela signifie qu'un temps d'attente élevé pour les requêtes d'E/S au niveau de l'interconnexion de cluster affecte la latence d'un ou de plusieurs workloads.

- **Data Processing**

  Représente le composant logiciel du cluster impliqué dans le traitement des E/S entre le cluster et l'agrégat de stockage qui contient le workload. Le nœud gérant le traitement des données a peut-être changé depuis la détection de l'événement. Si le composant de traitement des données est en contention, cela signifie qu'une utilisation élevée au niveau du nœud de traitement des données affecte la latence d'un ou de plusieurs workloads.

- **Activation du volume**

  Représente le processus qui suit l'utilisation de tous les volumes actifs. Dans les environnements de grande taille où plus de 1 000 volumes sont actifs, ce processus suit le nombre de volumes critiques qui doivent accéder simultanément aux ressources via le nœud. Lorsque le nombre de volumes actifs simultanés dépasse le seuil maximal recommandé, certains volumes non critiques présentent une latence, comme indiqué ici.

- **MetroCluster Ressources**

  Représente les ressources MetroCluster, notamment NVRAM et les liaisons inter-commutateurs (ISL), utilisées pour mettre en miroir les données entre les clusters dans une configuration MetroCluster. Si le composant MetroCluster est en conflit, cela signifie qu'un débit d'écriture élevé provenant des workloads sur le cluster local ou un problème d'état de la liaison affecte la latence d'un ou de plusieurs workloads sur le cluster local. Si le cluster n'est pas dans une configuration MetroCluster, cette icône n'est pas affichée.

- **Opérations sur des agrégats ou des agrégats SSD**

  Représente l'agrégat de stockage sur lequel les workloads s'exécutent. Si le composant d'agrégat est en contention, cela signifie qu'une utilisation élevée de l'agrégat affecte la latence d'un ou de plusieurs workloads. Un agrégat se compose uniquement de HDD, ou d'un mélange de HDD et de SSD (un agrégat Flash Pool), ou d'un mélange de HDD et d'un niveau cloud (un agrégat FabricPool). Un « `SSD Aggregate` » se compose uniquement de SSD (un agrégat 100 % Flash), ou d'un mélange de SSD et

d’un niveau cloud (un agrégat FabricPool).

- **Latence du cloud**

  Ce composant logiciel du cluster gère les entrées/sorties entre le cluster et le niveau cloud où sont stockées les données utilisateur. Si le composant de latence cloud est saturé, cela signifie qu’un grand nombre de lectures sur des volumes hébergés sur le niveau cloud impactent la latence d’un ou plusieurs workloads.

- **Synchronisation SnapMirror**

  Représente le composant logiciel du cluster impliqué dans la réplication des données utilisateur du volume principal vers le volume secondaire dans une relation synchrone SnapMirror. Si le composant de synchronisation SnapMirror est en contention, cela signifie que l’activité des opérations synchrones SnapMirror affecte la latence d’un ou de plusieurs workloads.

Identifier les rôles de la charge de travail dans les événements de performance dans Active IQ Unified Manager

Unified Manager utilise des rôles pour identifier l’implication d’un workload dans un événement de performance. Ces rôles incluent les victimes, les agresseurs et les prédateurs. Un workload défini par l’utilisateur peut être à la fois victime, agresseur et prédateur.

Rôle	Description
Victime	Un workload défini par l’utilisateur dont les performances ont diminué en raison d’autres workloads, appelés « agresseurs », qui surutilisent un composant du cluster. Seuls les workloads définis par l’utilisateur sont identifiés comme victimes. Unified Manager identifie les workloads victimes en fonction de leur écart de latence : la latence réelle, lors d’un événement, a considérablement augmenté par rapport à la latence prévue (plage attendue).
Brute	Un workload défini par l’utilisateur ou par le système, dont la surutilisation d’un composant du cluster a entraîné une baisse des performances d’autres workloads, appelés victimes. Unified Manager identifie les workloads accapareurs en fonction de leur écart d’utilisation d’un composant du cluster, lorsque l’utilisation réelle, lors d’un événement, a largement augmenté par rapport à la plage d’utilisation prévue.
Requin	Un workload défini par l’utilisateur présentant l’utilisation la plus élevée d’un composant du cluster par rapport à tous les workloads impliqués dans un événement. Unified Manager identifie les workloads shark en fonction de leur utilisation d’un composant du cluster pendant un événement.

Les workloads sur un cluster peuvent partager de nombreux composants du cluster, tels que les agrégats et le processeur pour le réseau et le traitement des données. Lorsqu'un workload, tel qu'un volume, augmente son utilisation d'un composant du cluster au point que ce composant ne puisse pas répondre efficacement aux demandes du workload, le composant est en contention. Le workload qui surutilise un composant du cluster est un agresseur. Les autres workloads qui partagent ces composants et dont les performances sont affectées par l'agresseur sont les victimes. L'activité de workloads définis par le système, tels que la déduplication ou les copies Snapshot, peut également dégénérer en « bullying ».

Lorsque Unified Manager détecte un événement, il identifie tous les workloads et composants du cluster impliqués, y compris les workloads agressifs qui ont provoqué l'événement, le composant du cluster en conflit et les workloads victimes dont les performances ont diminué en raison de l'activité accrue des workloads agressifs.

Si Unified Manager ne parvient pas à identifier les workloads perturbateurs, il génère uniquement des alertes concernant les workloads victimes et le composant du cluster concerné.

Unified Manager peut identifier les workloads victimes de workloads agressifs, et également identifier quand ces mêmes workloads deviennent des workloads agressifs. Un workload peut être agressif envers lui-même. Par exemple, un workload très performant dont les performances sont limitées par une limite de groupe de règles entraîne la limitation des performances de tous les workloads du groupe de règles, y compris le sien. Un workload qui est agressif ou victime dans un incident de performance en cours peut changer de rôle ou ne plus être un participant à l'incident.

Informations sur le copyright

Copyright © 2026 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.