



# **Contrôlez et gérez les performances du cluster à l'aide de l'interface de ligne de commandes**

**ONTAP 9**

NetApp  
April 24, 2024

# Sommaire

- Contrôlez et gérez les performances du cluster à l'aide de l'interface de ligne de commandes ..... 1
  - Contrôle des performances et présentation de la gestion ..... 1
  - Contrôle des performances ..... 1
  - Utilisez le conseiller numérique Active IQ pour consulter les performances du système ..... 12
  - Gérez les problèmes de performance ..... 12

# Contrôlez et gérez les performances du cluster à l'aide de l'interface de ligne de commandes

## Contrôle des performances et présentation de la gestion

Vous pouvez également définir des tâches de base de contrôle et de gestion des performances, et identifier et résoudre des problèmes courants de performance.

Vous pouvez utiliser ces procédures pour contrôler et gérer les performances du cluster si les hypothèses suivantes s'appliquent à votre situation :

- Vous voulez appliquer les bonnes pratiques, pas explorer toutes les options disponibles.
- Vous pouvez afficher l'état du système et les alertes, surveiller les performances du cluster et effectuer une analyse de la source des problèmes à l'aide de Active IQ Unified Manager (anciennement OnCommand Unified Manager) en plus de l'interface de ligne de commandes de ONTAP.
- Vous utilisez l'interface de ligne de commandes ONTAP pour configurer la qualité de service (QoS) du stockage.

La QoS est également disponible dans System Manager, NSLM, WFA, VSC (plug-in VMware) et les API.

- Vous souhaitez installer Unified Manager à l'aide d'une appliance virtuelle au lieu d'une installation Linux ou Windows.
- Vous êtes prêt à utiliser une configuration statique plutôt que DHCP pour installer le logiciel.
- Vous pouvez accéder aux commandes ONTAP au niveau de privilège avancé.
- Vous êtes un administrateur de cluster ayant le rôle « admin ».

### Informations associées

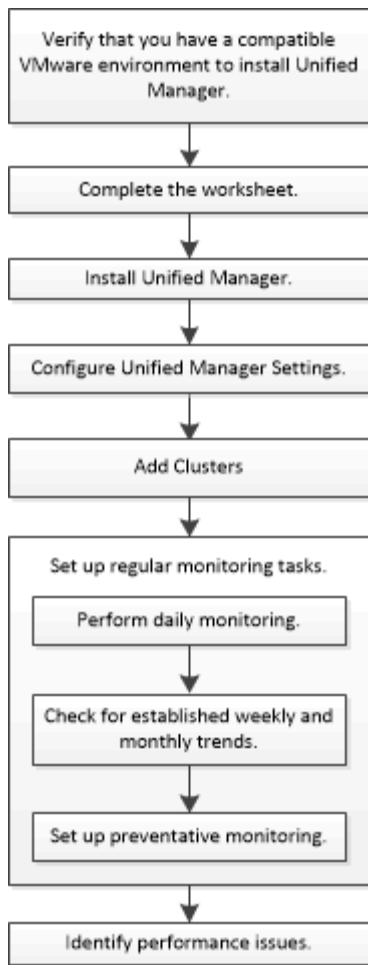
Si ces hypothèses ne sont pas correctes pour votre situation, vous devez consulter les ressources suivantes :

- ["Installation de Active IQ Unified Manager 9.8"](#)
- ["Administration du système"](#)

## Contrôle des performances

### Présentation du workflow de surveillance des performances et de maintenance

Le contrôle et la maintenance des performances du cluster impliquent l'installation du logiciel Active IQ Unified Manager, la configuration des tâches de surveillance de base, l'identification des problèmes de performances et les ajustements nécessaires.



## Vérifiez que votre environnement VMware est pris en charge

Pour installer correctement Active IQ Unified Manager, vous devez vérifier que votre environnement VMware répond aux exigences requises.

### Étapes

1. Vérifiez que votre infrastructure VMware répond aux exigences de dimensionnement pour l'installation de Unified Manager.
2. Accédez au ["Matrice d'interopérabilité"](#) pour vérifier que vous disposez d'une combinaison prise en charge des composants suivants :
  - Version ONTAP
  - Version du système d'exploitation ESXi
  - Version de VMware vCenter Server
  - Version des outils VMware
  - Type et version du navigateur



Le ["Matrice d'interopérabilité"](#) Le répertorie les configurations prises en charge pour Unified Manager.

3. Cliquez sur le nom de la configuration sélectionnée.

Les détails de cette configuration s'affichent dans la fenêtre Détails de la configuration.

4. Vérifiez les informations dans les onglets suivants :

- Remarques

Le répertoire les alertes et informations importantes spécifiques à votre configuration.

- Politiques et lignes directrices

Présente des recommandations d'ordre général pour toutes les configurations.

## Fiche technique Active IQ Unified Manager

Avant d'installer, de configurer et de connecter Active IQ Unified Manager, vous devez disposer facilement d'informations spécifiques sur votre environnement. Vous pouvez enregistrer les informations dans la fiche.

### Informations sur l'installation de Unified Manager

Machine virtuelle sur laquelle le logiciel est déployé	Votre valeur
Adresse IP du serveur ESXi	
Nom de domaine complet de l'hôte	
Adresse IP de l'hôte	
Masque de réseau	
Adresse IP de la passerelle	
Adresse DNS principale	
Adresse DNS secondaire	
Domaines de recherche	
Nom d'utilisateur de maintenance	
Mot de passe utilisateur de maintenance	


### Informations sur la configuration de Unified Manager

Réglage	Votre valeur
Adresse e-mail de l'utilisateur de maintenance	

Serveur NTP	
Nom d'hôte ou adresse IP du serveur SMTP	
Nom d'utilisateur SMTP	
Mot de passe SMTP	
Port SMTP par défaut	25 (valeur par défaut)
E-mail à partir duquel les notifications d'alerte sont envoyées	
Nom distinctif de la liaison LDAP	
Mot de passe de liaison LDAP	
Nom d'administrateur Active Directory	
Mot de passe Active Directory	
Nom distinctif de la base du serveur d'authentification	
Nom d'hôte ou adresse IP du serveur d'authentification	

### Informations sur le cluster

Capturer les informations suivantes pour chaque cluster sur Unified Manager.

Cluster 1 de N	Votre valeur
Nom d'hôte ou adresse IP de gestion du cluster	
<div>  <p>L'administrateur doit avoir reçu le rôle « admin ».</p> </div>	
Mot de passe administrateur ONTAP	
Protocole (HTTP ou HTTPS)	

### Informations associées

["Authentification de l'administrateur et RBAC"](#)

## Installez Active IQ Unified Manager

### Téléchargez et déployez Active IQ Unified Manager

Pour installer le logiciel, vous devez télécharger le fichier d'installation de l'appliance virtuelle (va), puis utiliser un client VMware vSphere pour déployer le fichier sur un serveur VMware ESXi. Le va est disponible dans un fichier OVA.

#### Étapes

1. Accédez à la page **NetApp support site Software Download** (Téléchargement de logiciels) et recherchez Active IQ Unified Manager.

<https://mysupport.netapp.com/products/index.html>

2. Sélectionnez **VMware vSphere** dans le menu déroulant **Select Platform** et cliquez sur **Go!**
3. Enregistrez le fichier « OVA » dans un emplacement local ou réseau accessible à votre client VMware vSphere.
4. Dans VMware vSphere client, cliquez sur **fichier > déployer le modèle OVF**.
5. Localisez le fichier « OVA » et utilisez l'assistant pour déployer l'appliance virtuelle sur le serveur ESXi.

Vous pouvez utiliser l'onglet **Propriétés** de l'assistant pour saisir vos informations de configuration statique.

6. Mise sous tension de la machine virtuelle
7. Cliquez sur l'onglet **Console** pour afficher le processus de démarrage initial.
8. Suivez l'invite pour installer VMware Tools sur la machine virtuelle.
9. Configurer le fuseau horaire.
10. Entrez un nom d'utilisateur et un mot de passe de maintenance.
11. Accédez à l'URL affichée par la console de la machine virtuelle.

### Configurez les paramètres Active IQ Unified Manager initiaux

La boîte de dialogue Configuration initiale du Active IQ Unified Manager s'affiche lorsque vous accédez pour la première fois à l'interface utilisateur Web, qui vous permet de configurer certains paramètres initiaux et d'ajouter des clusters.

#### Étapes

1. Acceptez le paramètre AutoSupport activé par défaut.
2. Entrez les détails du serveur NTP, l'adresse e-mail de l'utilisateur de maintenance, le nom d'hôte du serveur SMTP et les options SMTP supplémentaires, puis cliquez sur **Enregistrer**.

#### Une fois que vous avez terminé

Une fois la configuration initiale terminée, la page sources de données du cluster s'affiche, dans laquelle vous pouvez ajouter les détails du cluster.

### Spécifiez les clusters à surveiller

Vous devez ajouter un cluster à un serveur Active IQ Unified Manager pour surveiller le

cluster, afficher l'état de détection du cluster et contrôler ses performances.

### Ce dont vous avez besoin

- Vous devez disposer des informations suivantes :

- Nom d'hôte ou adresse IP de gestion du cluster

Le nom d'hôte est le nom de domaine complet (FQDN) ou le nom court que Unified Manager utilise pour se connecter au cluster. Ce nom d'hôte doit être résolu sur l'adresse IP de gestion du cluster.

L'adresse IP de gestion du cluster doit être la LIF de gestion du cluster du serveur virtuel de stockage administratif (SVM). Si vous utilisez une LIF node-management, l'opération échoue.

- Nom d'utilisateur et mot de passe de l'administrateur ONTAP
  - Type de protocole (HTTP ou HTTPS) pouvant être configuré sur le cluster et le numéro de port du cluster
- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
  - L'administrateur ONTAP doit disposer des rôles d'administrateur ONTAPI et SSH.
  - Le FQDN de Unified Manager doit pouvoir exécuter ONTAP.

Vous pouvez le vérifier à l'aide de la commande ONTAP `ping -node node_name -destination Unified_Manager_FQDN`.

### Description de la tâche

Dans le cas d'une configuration MetroCluster, vous devez ajouter les clusters locaux et distants, et les clusters doivent être configurés correctement.

### Étapes

1. Cliquez sur **Configuration > sources de données de cluster**.
2. Sur la page clusters, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter un cluster**, spécifiez les valeurs requises, telles que le nom d'hôte ou l'adresse IP (IPv4 ou IPv6) du cluster, le nom d'utilisateur, le mot de passe, le protocole de communication et le numéro de port.

Par défaut, le protocole HTTPS est sélectionné.

Vous pouvez modifier l'adresse IP de gestion du cluster d'IPv6 au format IPv4 ou d'IPv4 à IPv6. La nouvelle adresse IP est reflétée dans la grille du cluster et la page de configuration du cluster, une fois le cycle de surveillance suivant terminé.

4. Cliquez sur **Ajouter**.
5. Si HTTPS est sélectionné, effectuez les opérations suivantes :
  - a. Dans la boîte de dialogue **Authorise Host**, cliquez sur **View Certificate** pour afficher les informations de certificat relatives au cluster.
  - b. Cliquez sur **Oui**.

Unified Manager vérifie le certificat uniquement lors de l'ajout initial du cluster, mais ne le vérifie pas pour chaque appel d'API à ONTAP.



Si le certificat a expiré, vous ne pouvez pas ajouter le cluster. Vous devez renouveler le certificat SSL, puis ajouter le cluster.

6. **Facultatif** : affichez l'état de la détection du cluster :

- a. Vérifiez l'état de la détection du cluster à partir de la page **Configuration du cluster**.

Le cluster est ajouté à la base de données Unified Manager après l'intervalle de contrôle par défaut d'environ 15 minutes.

## Configurer les tâches de surveillance de base

### Effectuer un contrôle quotidien

Vous pouvez effectuer une surveillance quotidienne afin de vous assurer que vous n'avez aucun problème de performance immédiat à laquelle vous devez vous préoccuper.

#### Étapes

1. Dans l'interface utilisateur Active IQ Unified Manager, accédez à la page **Inventaire des événements** pour afficher tous les événements actuels et obsolètes.
2. Dans l'option **View**, sélectionnez `Active Performance Events` et déterminez quelle action est nécessaire.

### Utilisez les tendances de performances hebdomadaires et mensuelles pour identifier les problèmes de performances

L'identification des tendances de performances permet de déterminer si le cluster est sur-utilisé ou sous-utilisé en analysant la latence du volume. Vous pouvez utiliser des étapes similaires pour identifier les goulots d'étranglement du processeur, du réseau ou d'autres systèmes.

#### Étapes

1. Identifiez le volume que vous pensez être sous-utilisé ou sur-utilisé.
2. Dans l'onglet **Détails du volume**, cliquez sur **30 d** pour afficher les données historiques.
3. Dans le menu déroulant « données de pause par », sélectionnez **latence**, puis cliquez sur **Envoyer**.
4. Désélectionnez **agrégat** dans le tableau comparatif des composants du cluster, puis comparez la latence du cluster avec celle du tableau de latence du volume.
5. Sélectionnez **agrégat** et désélectionnez tous les autres composants dans le tableau comparatif des composants du cluster, puis comparez la latence globale avec celle du graphique de latence du volume.
6. Comparez le graphique de latence de lecture/écriture sur le tableau de latence du volume.
7. Identifiez si les charges d'application client ont provoqué des conflits au niveau de la charge de travail et rééquilibrez les charges de travail en fonction des besoins.
8. Déterminez si l'agrégat est sur-utilisé et source de conflits, et rééquilibrez les charges de travail si nécessaire.

### Utilisez des seuils de performances pour générer des notifications d'événements

Les événements sont des notifications que la Active IQ 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 que vous surveillez. Vous pouvez configurer des alertes pour envoyer automatiquement une notification par e-mail lorsque des événements de certains types de gravité se produisent.

### Définissez des seuils de performances

Vous pouvez définir des seuils de performance pour contrôler les problèmes de performance stratégiques. Des seuils définis par l'utilisateur déclenchent une notification d'avertissement ou d'événement critique lorsque le système approche ou dépasse le seuil défini.

#### Étapes

1. Créez les seuils d'avertissement et d'événement critique :
  - a. Sélectionnez **Configuration** > **seuils de performances**.
  - b. Cliquez sur **Créer**.
  - c. Sélectionnez le type d'objet et spécifiez un nom et une description de la règle.
  - d. Sélectionnez la condition de compteur d'objets et spécifiez les valeurs limites qui définissent les événements Avertissement et critique.
  - e. Sélectionnez la durée pendant laquelle les valeurs limites doivent être enfreintes pour un événement à envoyer, puis cliquez sur **Enregistrer**.
2. Attribuez la politique de seuil à l'objet de stockage.
  - a. Accédez à la page Inventaire pour le même type d'objet de cluster que vous avez précédemment sélectionné et choisissez **Performance** dans l'option Afficher.
  - b. Sélectionnez l'objet auquel vous souhaitez affecter la stratégie de seuil, puis cliquez sur **affecter stratégie de seuil**.
  - c. Sélectionnez la stratégie que vous avez créée précédemment, puis cliquez sur **affecter stratégie**.

#### Exemple

Vous pouvez définir des seuils définis par l'utilisateur pour en savoir plus sur les problèmes de performance stratégiques. Par exemple, si vous disposez d'un serveur Microsoft Exchange et que vous savez qu'il tombe en panne si la latence du volume dépasse 20 millisecondes, vous pouvez définir un seuil d'avertissement à 12 millisecondes et un seuil critique à 15 millisecondes. Avec ce paramètre de seuil, vous pouvez recevoir des notifications lorsque la latence du volume dépasse la limite.

	Warning		Critical	
Object Counter Condition*	Average Latency ms/op	12	ms/op	15 ms/op

#### Ajouter des 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.

## Ce dont vous avez besoin

- 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 **Événements**, 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 « [sample@domain.com](mailto:sample@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, et déplacez-la dans la zone Ressources sélectionnées.
  - c. Cliquez sur **exclude**, puis saisissez xyz Dans le champ **Name contient**, puis cliquez sur **Add**.
3. Cliquez sur **Événements**, 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](mailto: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**.

## Configurez les paramètres d'alerte

Vous pouvez spécifier les événements provenant de Active IQ Unified Manager qui déclenchent des alertes, les destinataires de ces alertes et la fréquence des alertes.

### Ce dont vous avez besoin

Vous devez avoir le rôle Administrateur d'applications.

### Description de la tâche

Vous pouvez configurer des paramètres d'alerte uniques pour les types d'événements de performance suivants :

- Événements critiques déclenchés par des violations des seuils définis par l'utilisateur
- Événements d'avertissement déclenchés par des violations des seuils définis par l'utilisateur, des seuils définis par le système ou des seuils dynamiques

Par défaut, des alertes par e-mail sont envoyées aux utilisateurs d'administration de Unified Manager pour

tous les nouveaux événements. Vous pouvez envoyer des alertes par e-mail à d'autres utilisateurs en ajoutant les adresses e-mail de ces utilisateurs.



Pour désactiver l'envoi d'alertes pour certains types d'événements, vous devez décocher toutes les cases d'une catégorie d'événement. Cette action n'arrête pas l'apparition des événements dans l'interface utilisateur.

Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Storage Management > Alert Setup**.  
  
La page Configuration des alertes s'affiche.
2. Cliquez sur **Ajouter** et configurez les paramètres appropriés pour chaque type d'événement.  
  
Pour envoyer des alertes par e-mail à plusieurs utilisateurs, entrez une virgule entre chaque adresse e-mail.
3. Cliquez sur **Enregistrer**.

Identification des problèmes de performances dans Active IQ Unified Manager

Si un événement de performance se produit, vous pouvez localiser la source du problème dans Active IQ Unified Manager et utiliser d'autres outils pour le résoudre. Vous recevrez peut-être une notification par e-mail d'un événement ou une notification de cet événement pendant le suivi quotidien.

Étapes

1. Cliquez sur le lien de la notification par e-mail, qui vous mène directement à l'objet de stockage ayant un événement de performances.

Si...	Alors...
Recevoir une notification par e-mail d'un événement	Cliquez sur le lien pour accéder directement à la page des détails de l'événement.
Remarquez l'événement lors de l'analyse de la page Inventaire des événements	Sélectionnez l'événement pour accéder directement à la page des détails de l'événement.

2. Si l'événement a franchi un seuil défini par le système, suivez les actions suggérées dans l'interface utilisateur pour résoudre le problème.
3. Si l'événement a franchi un seuil défini par l'utilisateur, analysez l'événement pour déterminer si vous devez agir.
4. Si le problème persiste, vérifiez les paramètres suivants :
  - Paramètres de protocole sur le système de stockage
  - Paramètres réseau sur n'importe quel commutateur Ethernet ou Fabric
  - Paramètres réseau sur le système de stockage
  - Disposition des disques et metrics des agrégats sur le système de stockage
5. Si le problème persiste, contactez le support technique pour obtenir de l'aide.

# Utilisez le conseiller numérique Active IQ pour consulter les performances du système

Pour tous les systèmes ONTAP qui envoient la télémétrie AutoSupport à NetApp, vous pouvez afficher des données étendues de performances et de capacité. Active IQ affiche les performances du système sur une période plus longue que ce que vous pouvez voir dans System Manager.

Vous pouvez afficher les graphiques de l'utilisation du CPU, de la latence, des opérations d'entrée/sortie par seconde, des opérations d'entrée/sortie par protocole et du débit du réseau. Vous pouvez également télécharger ces données au format .csv pour les analyser avec d'autres outils.

Outre ces données de performances, Active IQ affiche l'efficacité du stockage par charge de travail et compare cette efficacité à celle attendue pour ce type de charge de travail. Vous pouvez consulter les tendances en matière de capacité et obtenir une estimation de la quantité de stockage supplémentaire à ajouter dans une période donnée.



- L'efficacité du stockage est disponible au niveau du client, du cluster et des nœuds, à gauche du tableau de bord principal.
- La performance est disponible au niveau du cluster et du nœud sur la gauche du tableau de bord principal.

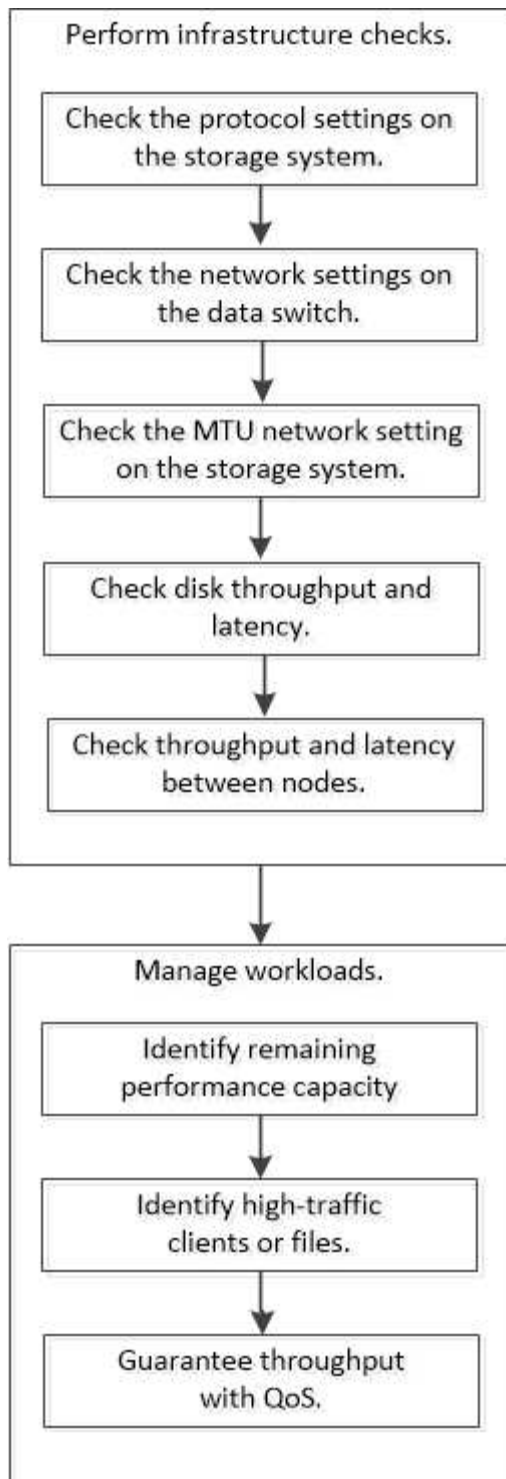
## Informations associées

- ["Documentation du conseiller digital Active IQ"](#)
- ["Liste de lecture vidéo conseiller numérique Active IQ"](#)
- ["Portail Web Active IQ"](#)

# Gérez les problèmes de performance

## Workflow de gestion des performances

Une fois que vous avez identifié un problème de performance, vous pouvez procéder à quelques vérifications de diagnostic de base de votre infrastructure pour éliminer les erreurs de configuration évidentes. Si ceux qui ne identifient pas le problème, vous pouvez commencer par examiner les problèmes liés à la gestion des charges de travail.



## Effectuer des vérifications de base de l'infrastructure

### Vérifiez les paramètres de protocole sur le système de stockage

#### Vérifiez la taille maximale du transfert TCP NFS

Pour NFS, vous pouvez vérifier si la taille maximale du transfert TCP pour les lectures et les écritures peut provoquer un problème de performances. Si vous pensez que la taille ralentit les performances, vous pouvez l'augmenter.

### Ce dont vous avez besoin

- Pour effectuer cette tâche, vous devez disposer des privilèges d'administrateur de cluster.
- Vous devez utiliser des commandes de niveau de privilège avancé pour cette tâche.

### Étapes

1. Changement au niveau de privilège avancé :

```
set -privilege advanced
```

2. Vérifiez la taille maximale du transfert TCP :

```
vserver nfs show -vserver vserver_name -instance
```

3. Si la taille maximale du transfert TCP est trop faible, augmentez la taille :

```
vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer
```

4. Revenir au niveau de privilège administratif :

```
set -privilege admin
```

### Exemple

L'exemple suivant modifie la taille maximale de transfert TCP de SVM1 à 1048576 :

```
cluster1::*> vserver nfs modify -vserver SVM1 -tcp-max-xfer-size 1048576
```

### Vérifiez la taille de lecture/écriture TCP iSCSI

Pour iSCSI, vous pouvez vérifier la taille de lecture/écriture TCP pour déterminer si le paramètre de taille crée un problème de performances. Si la taille est la source d'un problème, vous pouvez le corriger.

### Ce dont vous avez besoin

Des commandes de niveau de privilège avancé sont requises pour cette tâche.

### Étapes

1. Changement au niveau de privilège avancé :

```
set -privilege advanced
```

2. Vérifiez le paramètre de taille de la fenêtre TCP :

```
vserver iscsi show -vserv,er vserver_name -instance
```

3. Modifiez le paramètre de taille de la fenêtre TCP :

```
vserver iscsi modify -vserver vserver_name -tcp-window-size integer
```

4. Revenir au privilège administratif :



```
set -privilege admin
```

### Exemple

L'exemple suivant modifie la taille de la fenêtre TCP de SVM1 à 131,400 octets :

```
cluster1::*> vserver iscsi modify -vserver vs1 -tcp-window-size 131400
```

### Contrôler les réglages multiplexés CIFS

Si des performances réseau CIFS lentes sont à l'origine d'un problème de performances, vous pouvez modifier les paramètres multiplexés pour les améliorer et les corriger.

#### Étapes

1. Contrôler le réglage multiplexé CIFS :

```
vserver cifs options show -vserver -vserver_name -instance
```

2. Modifier le paramètre multiplexé CIFS :

```
vserver cifs options modify -vserver -vserver_name -max-mpx integer
```

### Exemple

L'exemple suivant modifie le nombre maximal de multiplexage activé SVM1 à 255 :

```
cluster1:::> vserver cifs options modify -vserver SVM1 -max-mpx 255
```

### Vérifiez la vitesse du port de l'adaptateur FC

La vitesse du port cible de l'adaptateur doit correspondre à la vitesse du périphérique auquel il se connecte, afin d'optimiser les performances. Si le port est défini sur négociation automatique, il peut prendre plus de temps pour vous reconnecter après un basculement et un rétablissement ou une autre interruption.

#### Ce dont vous avez besoin

Toutes les LIFs qui utilisent cet adaptateur comme port de home port doivent être hors ligne.

#### Étapes

1. Mettez l'adaptateur hors ligne :

```
network fcp adapter modify -node nodename -adapter adapter -state down
```

2. Vérifiez la vitesse maximale de l'adaptateur de port :

```
fcp adapter show -instance
```

3. Modifiez la vitesse du port, si nécessaire :

```
network fcp adapter modify -node nodename -adapter adapter -speed  
{1|2|4|8|10|16|auto}
```

#### 4. Mettez la carte en ligne :

```
network fcp adapter modify -node nodename -adapter adapter -state up
```

#### 5. Mettre en ligne toutes les LIFs sur l'adaptateur :

```
network interface modify -vserver * -lif * { -home-node node1 -home-port e0c }  
-status-admin up
```

### Exemple

L'exemple suivant modifie la vitesse du port de l'adaptateur 0d marche node1 Jusqu'à 2 Gbits/s :

```
cluster1::> network fcp adapter modify -node node1 -adapter 0d -speed 2
```

### Vérifiez les paramètres réseau sur les commutateurs de données

Bien que vous deviez conserver les mêmes paramètres MTU sur vos clients, serveurs et systèmes de stockage (c'est-à-dire les points de terminaison réseau), les périphériques réseau intermédiaires tels que les cartes réseau et les commutateurs doivent être définis sur leurs valeurs MTU maximales pour garantir que les performances ne sont pas affectées.

Pour des performances optimales, tous les composants du réseau doivent être en mesure de transférer des trames Jumbo (IP de 9000 octets, 9022 octets y compris Ethernet). Les commutateurs de données doivent être réglés sur au moins 9022 octets, mais une valeur typique de 9216 est possible avec la plupart des commutateurs.

### Procédure

Pour les commutateurs de données, vérifiez que la taille de MTU est définie sur 9022 ou plus.

Pour plus d'informations, consultez la documentation du fournisseur du commutateur.

### Vérifiez le paramètre réseau MTU sur le système de stockage

Vous pouvez modifier les paramètres réseau sur le système de stockage s'ils ne sont pas identiques à ceux du client ou d'autres terminaux réseau. Alors que le paramètre MTU du réseau de gestion est défini sur 1500, la taille MTU du réseau de données doit être de 9000.

### Description de la tâche

Tous les ports d'un broadcast-domain ont la même taille de MTU, à l'exception du trafic de gestion du port e0M. Si le port fait partie d'un domaine de diffusion, utilisez le `broadcast-domain modify` Commande permettant de modifier la MTU de tous les ports du broadcast-domain modifié.

Notez que les périphériques réseau intermédiaires tels que les cartes réseau et les commutateurs de données peuvent être configurés sur des MTU plus élevés que les noeuds finaux réseau. Pour plus d'informations, voir

"Vérifiez les paramètres réseau sur les commutateurs de données".

### Étapes

1. Vérifiez le paramètre du port MTU sur le système de stockage :

```
network port show -instance
```

2. Modifier la MTU sur le domaine de diffusion utilisé par les ports :

```
network port broadcast-domain modify -ipspace ipspace -broadcast-domain  
broadcast_domain -mtu new_mtu
```

### Exemple

L'exemple suivant modifie le paramètre du port MTU sur 9000 :

```
network port broadcast-domain modify -ipspace Cluster -broadcast-domain  
Cluster -mtu 9000
```

### Vérifiez le débit et la latence des disques

Vous pouvez vérifier les mesures de débit et de latence des disques pour les nœuds de cluster afin de vous aider à effectuer le dépannage.

### Description de la tâche

Des commandes de niveau de privilège avancé sont requises pour cette tâche.

### Étapes

1. Changement au niveau de privilège avancé :

```
set -privilege advanced
```

2. Vérifiez le débit du disque et les mesures de latence :

```
statistics disk show -sort-key latency
```

### Exemple

L'exemple suivant affiche les totaux de chaque opération de lecture ou d'écriture de l'utilisateur pour `node2` marche `cluster1`:

```

::*> statistics disk show -sort-key latency
cluster1 : 8/24/2015 12:44:15

```

Disk	Node	Busy (%)	Total Ops	Read Ops	Write Ops	Read (Bps)	Write (Bps)	*Latency (us)
1.10.20	node2	4	5	3	2	95232	367616	23806
1.10.8	node2	4	5	3	2	138240	386048	22113
1.10.6	node2	3	4	2	2	48128	371712	19113
1.10.19	node2	4	6	3	2	102400	443392	19106
1.10.11	node2	4	4	2	2	122880	408576	17713

## Vérifiez le débit et la latence entre les nœuds

Vous pouvez utiliser le `network test-path` commande permettant d'identifier les goulets d'étranglement réseau ou de présélectionner les chemins réseau entre les nœuds. Vous pouvez exécuter la commande entre les nœuds intercluster ou intracluster.

### Ce dont vous avez besoin

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Des commandes de niveau de privilège avancé sont requises pour cette tâche.
- Pour un chemin intercluster, les clusters source et destination doivent être associés.

### Description de la tâche

Il arrive que les performances du réseau entre les nœuds ne répondent pas aux attentes de votre configuration de chemin. Un taux de transmission de 1 Gbit/s pour le type de transferts de données volumineux vus dans les opérations de réplication SnapMirror, par exemple, ne serait pas cohérent avec une liaison 10 GbE entre les clusters source et destination.

Vous pouvez utiliser le `network test-path` commande pour mesurer le débit et la latence entre les nœuds. Vous pouvez exécuter la commande entre les nœuds intercluster ou intracluster.



Le test sature le chemin du réseau avec des données, vous devez donc exécuter la commande lorsque le système n'est pas occupé, et lorsque le trafic réseau entre les nœuds n'est pas excessif. Le test s'est terminé après dix secondes. La commande ne peut être exécutée qu'entre des nœuds ONTAP 9.

Le `session-type` Option identifie le type d'opération que vous exécutez sur le chemin réseau, par exemple « AsyncMirrorRemote » pour la réplication SnapMirror vers une destination distante. Le type détermine la quantité de données utilisées dans le test. Le tableau suivant définit les types de session :

Type de session	Description
AsyncMirrorlocal	Paramètres utilisés par SnapMirror entre les nœuds du même cluster

AsyncMirrorRemote	Paramètres utilisés par SnapMirror entre les nœuds dans différents clusters (type par défaut)
Transfert de données à distance	Paramètres utilisés par ONTAP pour l'accès distant aux données entre les nœuds d'un même cluster (par exemple, une requête NFS vers un nœud pour un fichier stocké dans un volume sur un autre nœud)

## Étapes

1. Changement au niveau de privilège avancé :

```
set -privilege advanced
```

2. Mesure du débit et de la latence entre les nœuds :

```
network test-path -source-node source_nodename |local -destination-cluster
destination_clustername -destination-node destination_nodename -session-type
Default|AsyncMirrorLocal|AsyncMirrorRemote|SyncMirrorRemote|RemoteDataTransfer
```

Le nœud source doit se trouver dans le cluster local. Le nœud de destination peut être situé sur le cluster local ou dans un cluster en clusters à peering. Une valeur de "local" pour `-source-node` spécifie le nœud sur lequel vous exécutez la commande.

La commande suivante mesure le débit et la latence des opérations de réplication de type SnapMirror entre `node1` sur le cluster local et `node3` marche `cluster2`:

```
cluster1::> network test-path -source-node node1 -destination-cluster
cluster2 -destination-node node3 -session-type AsyncMirrorRemote
Test Duration:      10.88 secs
Send Throughput:    18.23 MB/sec
Receive Throughput: 18.23 MB/sec
MB sent:            198.31
MB received:        198.31
Avg latency in ms:  2301.47
Min latency in ms:  61.14
Max latency in ms:  3056.86
```

3. Revenir au privilège administratif :

```
set -privilege admin
```

## Une fois que vous avez terminé

Si les performances ne répondent pas aux attentes en matière de configuration du chemin, vérifiez les statistiques de performances du nœud, utilisez les outils disponibles pour isoler le problème sur le réseau, vérifiez les paramètres du commutateur, etc.

## Gérer les charges de travail

### Identifiez les performances de capacité restante

La capacité de performance, ou *headroom*, mesure le volume de travail que vous pouvez placer sur un nœud ou un agrégat avant que les performances des charges de travail sur la ressource ne commencent à être affectées par la latence. Connaître la capacité en termes de performances disponible sur le cluster vous aide à provisionner et à équilibrer les charges de travail.

### Ce dont vous avez besoin

Des commandes de niveau de privilège avancé sont requises pour cette tâche.

### Description de la tâche

Vous pouvez utiliser les valeurs suivantes pour l' `-object` option pour collecter et afficher les statistiques de marge :

- Pour les CPU, `resource_headroom_cpu`.
- Pour les agrégats, `resource_headroom_aggr`.

Vous pouvez également effectuer cette tâche à l'aide de System Manager et de Active IQ Unified Manager.

### Étapes

1. Changement au niveau de privilège avancé :

```
set -privilege advanced
```

2. Démarrer la collecte de statistiques de marge en temps réel :

```
statistics start -object resource_headroom_cpu|aggr
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page `man`.

3. Afficher les informations statistiques relatives à la marge en temps réel :

```
statistics show -object resource_headroom_cpu|aggr
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page `man`.

4. Revenir au privilège administratif :

```
set -privilege admin
```

### Exemple

L'exemple suivant affiche les statistiques moyennes sur la marge horaire des nœuds du cluster.

Vous pouvez calculer la capacité de performances disponible d'un nœud en soustrayant la `current_utilization` compteur du `optimal_point_utilization` compteur. Dans cet exemple, la capacité d'utilisation pour CPU\_sti2520-213 Est de -14% (72%-86%), ce qui suggère que le CPU a été surexploité en moyenne au cours de la dernière heure.

Vous avez peut-être spécifié `ewma_daily`, `ewma_weekly`, ou `ewma_monthly` pour obtenir la moyenne des mêmes informations sur des périodes plus longues.

```
sti2520-2131454963690::*> statistics show -object resource_headroom_cpu
-raw -counter ewma_hourly
(statistics show)
```

```
Object: resource_headroom_cpu
Instance: CPU_sti2520-213
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-213
```

Counter	Value
-----	-----
ewma_hourly	-
current_ops	4376
current_latency	37719
current_utilization	86
optimal_point_ops	2573
optimal_point_latency	3589
optimal_point_utilization	72
optimal_point_confidence_factor	1

```
Object: resource_headroom_cpu
Instance: CPU_sti2520-214
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-214
```

Counter	Value
-----	-----
ewma_hourly	-
current_ops	0
current_latency	0
current_utilization	0
optimal_point_ops	0
optimal_point_latency	0
optimal_point_utilization	71
optimal_point_confidence_factor	1

2 entries were displayed.

### Identifiez les clients ou les fichiers à fort trafic

Vous pouvez utiliser la technologie Active Objects de ONTAP pour identifier les clients ou les fichiers responsables d'une quantité disproportionnée de trafic de grappe. Une fois

que vous avez identifié ces « principaux » clients ou fichiers, vous pouvez rééquilibrer les charges de travail du cluster ou prendre d'autres mesures pour résoudre le problème.

### Ce dont vous avez besoin

Vous devez être un administrateur de cluster pour effectuer cette tâche.

### Étapes

1. Afficher les principaux clients accédant au cluster :

```
statistics top client show -node node_name -sort-key sort_column -interval  
seconds_between_updates -iterations iterations -max number_of_instances
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

La commande suivante affiche les principaux clients accédant à cluster1:

```
cluster1::> statistics top client show

cluster1 : 3/23/2016 17:59:10
```

Client	Vserver	Node	Protocol	*Total Ops
172.17.180.170	vs4	siderop1-vs4	nfs	668
172.17.180.169	vs3	siderop1-vs3	nfs	337
172.17.180.171	vs3	siderop1-vs3	nfs	142
172.17.180.170	vs3	siderop1-vs3	nfs	137
172.17.180.123	vs3	siderop1-vs3	nfs	137
172.17.180.171	vs4	siderop1-vs4	nfs	95
172.17.180.169	vs4	siderop1-vs4	nfs	92
172.17.180.123	vs4	siderop1-vs4	nfs	92
172.17.180.153	vs3	siderop1-vs3	nfs	0

2. Afficher les principaux fichiers auxquels a accédé sur le cluster :

```
statistics top file show -node node_name -sort-key sort_column -interval  
seconds_between_updates -iterations iterations -max number_of_instances
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

La commande suivante affiche les principaux fichiers auxquels vous accédez cluster1:



```
cluster1::> statistics top file show
```

```
cluster1 : 3/23/2016 17:59:10
```

			*Total		
	File	Volume	Vserver	Node	Ops
-----	-----	-----	-----	-----	-----
/vol/vol1/vm170-read.dat	vol1	vs4	siderop1-vs4	22	
/vol/vol1/vm69-write.dat	vol1	vs3	siderop1-vs3	6	
/vol/vol2/vm171.dat	vol2	vs3	siderop1-vs3	2	
/vol/vol2/vm169.dat	vol2	vs3	siderop1-vs3	2	
/vol/vol2/p123.dat	vol2	vs4	siderop1-vs4	2	
/vol/vol2/p123.dat	vol2	vs3	siderop1-vs3	2	
/vol/vol1/vm171.dat	vol1	vs4	siderop1-vs4	2	
/vol/vol1/vm169.dat	vol1	vs4	siderop1-vs4	2	
/vol/vol1/vm169.dat	vol1	vs4	siderop1-vs3	2	
/vol/vol1/p123.dat	vol1	vs4	siderop1-vs4	2	

## Débit garanti avec la QoS

### Débit garanti avec les QoS

Grâce à la qualité de service (QoS) du stockage, vous pouvez garantir que les performances des workloads stratégiques ne sont pas dégradées par des charges de travail concurrentes. Vous pouvez fixer un plafond de débit sur une charge de travail concurrente pour limiter son impact sur les ressources système, ou définir un débit *sol* pour une charge de travail critique, afin de garantir qu'il répond aux objectifs de débit minimum, indépendamment de la demande des charges de travail concurrentes. Vous pouvez même fixer un plafond et un sol pour la même charge de travail.

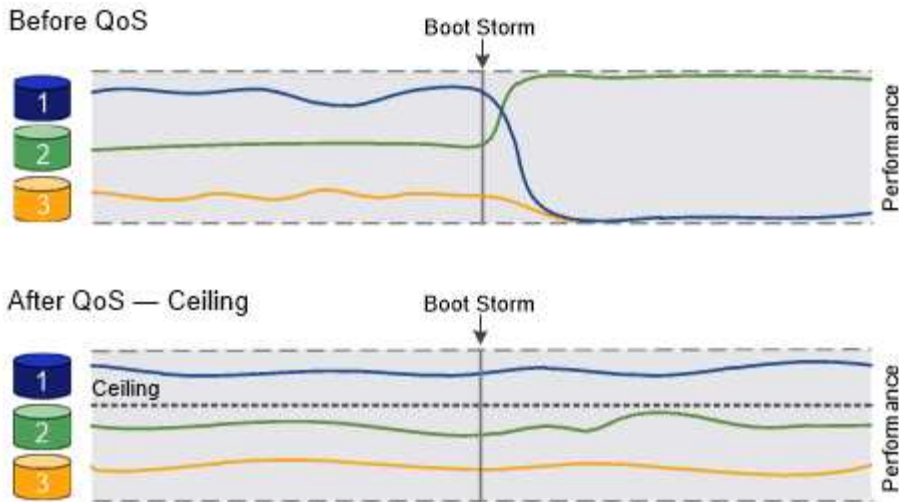
### À propos des plafonds de débit (QoS Max)

Le débit limite le débit pour une charge de travail jusqu'à un nombre maximal d'IOPS ou de Mbit/s, ainsi que les IOPS et les Mbit/s. Dans la figure ci-dessous, le plafond de débit pour la charge de travail 2 garantit qu'il ne « traite » pas les charges de travail 1 et 3.

Un *policy group* définit le plafond de débit pour une ou plusieurs charges de travail. Une charge de travail représente les opérations d'E/S d'un objet *stockage* : un volume, un fichier, qtree ou une LUN, ou l'ensemble des volumes, fichiers, qtrees ou LUN d'un SVM. Vous pouvez spécifier le plafond lorsque vous créez le groupe de règles ou attendre jusqu'à ce que vous contrôliez les charges de travail pour les spécifier.



Le débit des charges de travail peut dépasser jusqu'à 10 % le plafond défini, en particulier si le débit d'une charge de travail change rapidement. Le plafond peut être dépassé de 50 % pour gérer les rafales. Les rafales se produisent sur des nœuds uniques lorsque les jetons s'accumulent jusqu'à 150 %



### À propos du débit au sol (QoS min)

Un plancher de débit garantit que le débit d'une charge de travail ne passe pas en dessous d'un nombre minimal d'IOPS ou de Mo/sec, ou d'IOPS et de Mo/sec. Dans la figure ci-dessous, les niveaux de débit pour la charge de travail 1 et la charge de travail 3 s'assurent qu'ils répondent aux objectifs de débit minimum, indépendamment de la demande par charge de travail 2.



Comme le suggèrent les exemples, un plafond de débit accélère directement le débit. Un plancher de débit accélère indirectement le débit en donnant la priorité aux charges de travail pour lesquelles le sol a été défini.

Vous pouvez spécifier l'étage lors de la création du groupe de règles ou attendre jusqu'à ce que vous surveilliez les charges de travail pour le spécifier.

À partir de la version ONTAP 9.13.1, vous pouvez définir des étages de débit au niveau de l'étendue du SVM avec [\[adaptive-qos-templates\]](#). Dans les versions ONTAP antérieures à 9.13.1, un groupe de règles qui définit un plancher de débit ne peut pas être appliqué à une SVM.



Dans les versions antérieures à ONTAP 9.7, le débit est garanti lorsque la capacité de performance est suffisante.

Dans la ONTAP 9.7 et versions ultérieures, le débit au sol peut être garanti même en cas de capacité de performance insuffisante. Ce nouveau comportement de plancher s'appelle planchers v2. Pour respecter les garanties, au sol v2, peut offrir une plus grande latence sur les charges de travail sans débit ni travail dépassant les paramètres au sol. Au sol v2 s'applique à la QoS et à la qualité de service adaptative.

L'option d'activation/désactivation du nouveau comportement des étages v2 est disponible dans ONTAP 9.7P6 et versions ultérieures. Une charge de travail peut tomber sous le plancher spécifié pendant des opérations critiques comme `volume move trigger-cutover`. Même lorsque vous disposez d'une capacité suffisante et que vos opérations stratégiques n'ont pas lieu, le débit d'une charge de travail peut tomber en dessous du seuil spécifié de 5 %. Si les étages sont surprovisionnés et que la capacité de performance n'est pas disponible, certaines charges de travail peuvent tomber en dessous de l'étage spécifié.



## À propos des groupes de règles de qualité de service partagés et non partagés

À partir de ONTAP 9.4, vous pouvez utiliser un groupe de règles QoS *non-partagé* pour spécifier que le plafond ou le sol de débit défini s'applique à chaque charge de travail membre individuellement. Le comportement des groupes de règles *shared* dépend du type de stratégie :

- Pour les plafonds de débit, le débit total des charges de travail affectées au groupe de règles partagées ne peut dépasser le plafond spécifié.
- Pour les étages de débit, le groupe de règles partagées ne peut être appliqué qu'à une seule charge de travail.

## À propos de la QoS adaptative

En principe, la valeur du groupe de règles que vous attribuez à un objet de stockage est fixe. Vous devez modifier la valeur manuellement lorsque la taille de l'objet de stockage change. Une augmentation de l'espace utilisé sur un volume, par exemple, nécessite généralement une augmentation correspondante du plafond de débit spécifié pour le volume.

*Adaptive QoS* ajuste automatiquement la valeur du groupe de règles en fonction de la taille de la charge de travail, en maintenant le rapport IOPS/To|Go en fonction de la taille des modifications de la charge de travail. C'est un avantage significatif pour la gestion de centaines, voire de milliers de charges de travail dans un déploiement à grande échelle.

Généralement, vous utilisez la QoS adaptative pour ajuster les plafonds de débit, mais vous pouvez également l'utiliser pour gérer le débit (en cas d'augmentation de la taille des charges de travail). La taille du workload est exprimée en espace alloué à l'objet de stockage ou en espace utilisé par l'objet de stockage.



L'espace utilisé est disponible pour les étages de débit dans ONTAP 9.5 et versions ultérieures. Elle n'est pas prise en charge pour les étages de débit dans ONTAP 9.4 et les versions antérieures.

- Une politique *Allocated space* maintient le ratio IOPS/To|Go en fonction de la taille nominale de l'objet de stockage. Si le rapport est de 100 IOPS/Go, un volume de 150 Go plafonné à 15,000 IOPS, tant que la taille du volume reste celle-ci. Si le volume a été redimensionné de façon à 300 Go, la QoS adaptative ajuste le débit au plafond à 30,000 000 IOPS.
- Une règle *Used space* (par défaut) maintient le ratio IOPS/To|Go en fonction de la quantité de données réelles stockées avant le stockage efficace. Si le rapport est de 100 IOPS/Go, un volume de 150 Go contenant 100 Go de données stockées aurait un débit plafond de 10,000 000 IOPS. À mesure que la

quantité d'espace utilisée change, la QoS adaptative ajuste le plafond de débit en fonction du rapport.

Depuis ONTAP 9.5, vous pouvez spécifier une taille de bloc d'E/S pour votre application afin d'indiquer une limite de débit en IOPS et en Mbit/s. La limite de Mbit/s est calculée à partir de la taille de bloc multipliée par la limite d'IOPS. Par exemple, une taille de bloc d'E/S de 32 Ko pour une limite d'IOPS de 6144 IOPS/To permet d'obtenir une limite de 192 Mbit/s en Mbit/s.

Vous pouvez vous attendre à ce que le comportement suivant soit à la fois pour les plafonds de rendement et pour les planchers :

- Lorsqu'une charge de travail est affectée à un groupe de règles QoS adaptative, le plafond ou le sol est immédiatement mis à jour.
- Lorsqu'une charge de travail d'un groupe de règles de QoS adaptative est redimensionnée, la limite ou le sol est mis à jour en cinq minutes environ.

Le débit doit augmenter d'au moins 10 000 IOPS avant la mise à jour.

Les groupes de règles de QoS adaptative sont toujours non partagés : le plafond ou l'étage de débit défini s'applique à chaque charge de travail membre individuellement.

À partir de la version ONTAP 9.6, les niveaux de débit sont pris en charge par ONTAP Select Premium avec SSD.

### Modèle de groupe de règles adaptatif

À partir de la version ONTAP 9.13.1, vous pouvez définir un modèle de QoS adaptative sur une SVM. Les modèles de groupes de règles adaptatifs vous permettent de définir des seuils et des plafonds de débit pour tous les volumes d'une SVM.

Les modèles de groupes de règles adaptatives ne peuvent être définis qu'après la création du SVM. Utilisez le `vserver modify` commande avec `-qos-adaptive-policy-group-template` paramètre permettant de définir la règle.

Lorsque vous définissez un modèle de groupe de règles adaptatives, les volumes créés ou migrés après avoir défini la règle héritent automatiquement de la règle. L'affectation du modèle de règle n'a aucun impact sur les volumes existants du SVM. Si vous désactivez la policy sur le SVM, tout volume ultérieurement migré vers ou créé sur le SVM ne recevra pas la policy. La désactivation du modèle de groupe de règles adaptatives n'a pas d'impact sur les volumes qui ont hérité du modèle de règles car ils conservent le modèle de règles.

Pour plus d'informations, voir [Définissez un modèle de groupe de règles adaptatives](#).

### Assistance générale

Le tableau ci-dessous présente les différences en matière de prise en charge des plafonds de débit, des étages de débit et de la QoS adaptative.

Ressource ou fonctionnalité	Plafond de débit	Plancher de débit	Débit au sol v2	La QoS adaptative
Version ONTAP 9	Tout	9.2 et versions ultérieures	9.7 et versions ultérieures	9.3 et versions ultérieures

Ressource ou fonctionnalité	Plafond de débit	Plancher de débit	Débit au sol v2	La QoS adaptative
Plateformes	Tout	<ul style="list-style-type: none"> <li>• AFF</li> <li>• C190 *</li> <li>• ONTAP Select Premium avec SSD *</li> </ul>	<ul style="list-style-type: none"> <li>• AFF</li> <li>• C190</li> <li>• ONTAP Select Premium avec SSD</li> </ul>	Tout
Protocoles	Tout	Tout	Tout	Tout
FabricPool	Oui.	Oui, si la règle de Tiering est définie sur « none » et si aucun bloc n'est dans le cloud.	Oui, si la règle de Tiering est définie sur « none » et si aucun bloc n'est dans le cloud.	Non
SnapMirror synchrone	Oui.	Non	Non	Oui.

La prise en charge des baies ONTAP Select et C190 a débuté avec la version ONTAP 9.6.

### Charges de travail prises en charge pour les plafonds de débit

Le tableau ci-dessous présente la prise en charge des charges de travail pour les plafonds de débit dans la version ONTAP 9. Les volumes root, les miroirs de partage de charge et les miroirs de protection des données ne sont pas pris en charge.

Support de charge de travail - plafond	ONTAP 9.0	ONTAP 9.1	ONTAP 9.2	ONTAP 9.3	ONTAP 9.4 - 9.7	ONTAP 9.8 et versions ultérieures
Volumétrie	oui	oui	oui	oui	oui	oui
Fichier	oui	oui	oui	oui	oui	oui
LUN	oui	oui	oui	oui	oui	oui
SVM	oui	oui	oui	oui	oui	oui
Volume FlexGroup	non	non	non	oui	oui	oui
qtrees*	non	non	non	non	non	oui

<b>Support de charge de travail - plafond</b>	<b>ONTAP 9.0</b>	<b>ONTAP 9.1</b>	<b>ONTAP 9.2</b>	<b>ONTAP 9.3</b>	<b>ONTAP 9.4 - 9.7</b>	<b>ONTAP 9.8 et versions ultérieures</b>
Plusieurs charges de travail par groupe de règles	oui	oui	oui	oui	oui	oui
Groupes de stratégies non partagés	non	non	non	non	oui	oui

Depuis la version ONTAP 9.8, l'accès NFS est pris en charge dans les qtrees des volumes FlexVol et FlexGroup sur lesquels NFS est activé. Depuis la version ONTAP 9.9.1, l'accès SMB est également pris en charge dans les qtrees des volumes FlexVol et FlexGroup sur lesquels SMB est activé.

### Charges de travail prises en charge pour le débit au sol

Le tableau ci-dessous présente la prise en charge des charges de travail pour les débits par la version ONTAP 9. Les volumes root, les miroirs de partage de charge et les miroirs de protection des données ne sont pas pris en charge.

<b>Soutien de la charge de travail - plancher</b>	<b>ONTAP 9.2</b>	<b>ONTAP 9.3</b>	<b>ONTAP 9.4 - 9.7</b>	<b>ONTAP 9.8 - 9.13.0</b>	<b>ONTAP 9.13.1 et versions ultérieures</b>
Volumétrie	oui	oui	oui	oui	oui
Fichier	non	oui	oui	oui	oui
LUN	oui	oui	oui	oui	oui
SVM	non	non	non	non	oui
Volume FlexGroup	non	non	oui	oui	oui
qtrees *	non	non	non	oui	oui
Plusieurs charges de travail par groupe de règles	non	non	oui	oui	oui
Groupes de stratégies non partagés	non	non	oui	oui	oui

\\*à partir de ONTAP 9.8, l'accès NFS est pris en charge dans les qtrees des volumes FlexVol et FlexGroup sur lesquels NFS est activé. Depuis la version ONTAP 9.9.1, l'accès SMB est également pris en charge dans les qtrees des volumes FlexVol et FlexGroup sur lesquels SMB est activé.

## Prise en charge de workloads pour la QoS adaptative

Le tableau ci-dessous présente la prise en charge des workloads pour la QoS adaptative par la version ONTAP 9. Les volumes root, les miroirs de partage de charge et les miroirs de protection des données ne sont pas pris en charge.

Prise en charge des workloads : QoS adaptative	ONTAP 9.3	ONTAP 9.4 - 9.13.0	ONTAP 9.13.1 et versions ultérieures
Volumétrie	oui	oui	oui
Fichier	non	oui	oui
LUN	non	oui	oui
SVM	non	non	oui
Volume FlexGroup	non	oui	oui
Plusieurs charges de travail par groupe de règles	oui	oui	oui
Groupes de stratégies non partagés	oui	oui	oui

## Nombre maximal de charges de travail et de groupes de règles

Le tableau ci-dessous indique le nombre maximal de charges de travail et de groupes de règles par la version ONTAP 9.

Prise en charge des workloads	ONTAP 9.3 et versions antérieures	ONTAP 9.4 et versions ultérieures
Charges de travail maximales par cluster	12,000	40,000
Nombre maximal de workloads par nœud	12,000	40,000
Nombre maximal de stratégies groupes	12,000	12,000

## Activer ou désactiver le débit planchers v2

Vous pouvez activer ou désactiver le débit planchers v2 sur AFF. La valeur par défaut est activée. Lorsque la technologie planchers v2 est activée, le débit au sol peut être atteint lorsque les contrôleurs sont utilisés de façon intensive, au détriment d'une latence plus élevée sur d'autres charges de travail. Au niveau de la QoS et de la QoS adaptative.

### Étapes

1. Changement au niveau de privilège avancé :

```
set -privilege advanced
```

2. Entrez l'une des commandes suivantes :

Les fonctions que vous recherchez...	Utilisez cette commande :
Désactiver les étages v2	<code>qos settings throughput-floors-v2 -enable false</code>
Activation de la version 2	<code>qos settings throughput-floors-v2 -enable true</code>



Pour désactiver le débit planchers v2 dans un cluster MetroCluster, vous devez exécuter le

```
qos settings throughput-floors-v2 -enable false
```

contrôlez à la fois les clusters source et de destination.

```
cluster1::*> qos settings throughput-floors-v2 -enable false
```

### Flux de travail de QoS du stockage

Si vous connaissez déjà les exigences de performance des workloads que vous souhaitez gérer avec QoS, vous pouvez définir la limite de débit lors de la création du groupe de règles. Sinon, vous pouvez attendre jusqu'à ce que vous contrôlons les charges de travail pour spécifier la limite.

### Fixer un plafond de débit avec la QoS

Vous pouvez utiliser le `max-throughput` Champ permettant à un groupe de règles de définir une limite de débit pour les workloads d'objets de stockage (QoS max). Vous pouvez appliquer le groupe de règles lors de la création ou de la modification de l'objet de stockage.

### Ce dont vous avez besoin

- Pour créer une « policy group » il faut être un administrateur de cluster.
- Vous devez être un administrateur de cluster pour appliquer une « policy group » à un SVM.

### Description de la tâche

- Depuis ONTAP 9.4, vous pouvez utiliser un groupe de règles QoS *non-partagé* pour spécifier que le plafond de débit défini s'applique à chaque charge de travail membre individuellement. Sinon, le groupe de règles est *Shared*: le débit total des charges de travail affectées au groupe de règles ne peut pas dépasser le plafond spécifié.

Régalez `-is-shared=false` pour le `qos policy-group create` commande permettant de spécifier un groupe de polices non partagé.



- Vous pouvez spécifier la limite de débit pour le plafond en IOPS, Mo/s ou IOPS, Mo/s. Si vous spécifiez les IOPS et Mo/s, la première limite atteinte est appliquée.



Si vous définissez une limite et un sol pour la même charge de travail, vous pouvez spécifier la limite de débit pour le plafond des IOPS uniquement.

- Un objet de stockage faisant l'objet d'une limite QoS doit être contenu par le SVM auquel appartient le groupe de règles. Plusieurs « policy group » peuvent appartenir à la même SVM.
- Vous ne pouvez pas affecter un objet de stockage à un groupe de règles si son objet contenant ou ses objets enfants appartiennent à ce groupe.
- Il s'agit d'une meilleure pratique de QoS pour appliquer un groupe de règles au même type d'objets de stockage.

## Étapes

### 1. Création d'une « policy group » :

```
qos policy-group create -policy-group policy_group -vserver SVM -max
-throughput number_of_iops|Mb/S|iops,Mb/S -is-shared true|false
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man. Vous pouvez utiliser le `qos policy-group modify` commande permettant d'ajuster les plafonds de débit.

La commande suivante crée la « policy group » partagée `pg-vs1` Avec un débit maximum de 5,000 000 IOPS :

```
cluster1::> qos policy-group create -policy-group pg-vs1 -vserver vs1
-max-throughput 5000iops -is-shared true
```

La commande suivante crée le « policy group » non partagé `pg-vs3` Avec un débit maximum de 100 400 IOPS et 80 Ko/S :

```
cluster1::> qos policy-group create -policy-group pg-vs3 -vserver vs3
-max-throughput 100iops,400KB/s -is-shared false
```

La commande suivante crée le « policy group » non partagé `pg-vs4` sans limite de débit :

```
cluster1::> qos policy-group create -policy-group pg-vs4 -vserver vs4
-is-shared false
```

### 2. Appliquer une « policy group » à un SVM, fichier, volume ou LUN :

```
storage_object create -vserver SVM -qos-policy-group policy_group
```

Pour connaître la syntaxe complète des commandes, consultez les pages de manuels. Vous pouvez utiliser le `storage_object modify` commande pour appliquer un autre groupe de règles à l'objet de stockage.

La commande suivante applique la « policy group » pg-vs1 À la SVM vs1:

```
cluster1::> vserver create -vserver vs1 -qos-policy-group pg-vs1
```

Les commandes suivantes appliquent la « policy group » pg-app aux volumes app1 et app2:

```
cluster1::> volume create -vserver vs2 -volume app1 -aggregate aggr1  
-qos-policy-group pg-app
```

```
cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr1  
-qos-policy-group pg-app
```

### 3. Surveillance des performances des groupes de règles :

```
qos statistics performance show
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.



Contrôle des performances depuis le cluster. N'utilisez pas d'outil sur l'hôte pour surveiller les performances.

La commande suivante affiche les performances de « policy group » :

```
cluster1::> qos statistics performance show
```

Policy Group	IOPS	Throughput	Latency
-total-	12316	47.76MB/s	1264.00us
pg_vs1	5008	19.56MB/s	2.45ms
_System-Best-Effort	62	13.36KB/s	4.13ms
_System-Background	30	0KB/s	0ms

### 4. Contrôle de la performance des charges de travail :

```
qos statistics workload performance show
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.



Contrôle des performances depuis le cluster. N'utilisez pas d'outil sur l'hôte pour surveiller les performances.

La commande suivante indique les performances des workloads :

```
cluster1::> qos statistics workload performance show
```

Workload	ID	IOPS	Throughput	Latency
-total-	-	12320	47.84MB/s	1215.00us
app1-wid7967	7967	7219	28.20MB/s	319.00us
vs1-wid12279	12279	5026	19.63MB/s	2.52ms
_USERSPACE_APPS	14	55	10.92KB/s	236.00us
_Scan_Backgro..	5688	20	0KB/s	0ms



Vous pouvez utiliser le `qos statistics workload latency show` Commande pour afficher les statistiques de latence détaillées pour les workloads de QoS.

### Définissez un seuil de débit avec la QoS

Vous pouvez utiliser le `min-throughput` Champ permettant à un groupe de règles de définir un étage de débit pour les workloads d'objets de stockage (QoS min). Vous pouvez appliquer le groupe de règles lors de la création ou de la modification de l'objet de stockage. Depuis la version ONTAP 9.8, vous pouvez spécifier le seuil de débit en IOPS ou Mbit/s, ou IOPS et Mbit/s.

#### Avant de commencer

- Vous devez exécuter ONTAP 9.2 ou version ultérieure. Les étages de débit sont disponibles à partir de ONTAP 9.2.
- Pour créer une « policy group » il faut être un administrateur de cluster.
- À partir de la version ONTAP 9.13.1, vous pouvez appliquer des planchers de débit au niveau de la SVM en utilisant une [modèle de groupe de règles adaptatif](#). Vous ne pouvez pas définir de modèle de « policy group » adaptatif sur une SVM disposant d'une « policy group » QoS.

#### Description de la tâche

- Depuis ONTAP 9.4, vous pouvez utiliser un groupe de règles QoS *non-partagé* pour spécifier que le niveau de débit défini soit appliqué individuellement à chaque charge de travail membre. C'est la seule condition dans laquelle un groupe de règles pour un étage de débit peut être appliqué à plusieurs charges de travail.

Réglez `-is-shared=false` pour le `qos policy-group create` commande permettant de spécifier une « policy group » non partagée.

- Le débit d'une charge de travail peut tomber en dessous du seuil spécifié si la capacité de performance est insuffisante (marge) sur le nœud ou l'agrégat.
- Un objet de stockage faisant l'objet d'une limite QoS doit être contenu par le SVM auquel appartient le groupe de règles. Plusieurs « policy group » peuvent appartenir à la même SVM.
- Il s'agit d'une meilleure pratique de QoS pour appliquer un groupe de règles au même type d'objets de stockage.
- Un groupe de règles qui définit un étage de débit ne peut pas être appliqué à un SVM.

#### Étapes

1. Vérifier que la capacité de performance sur le nœud ou l'agrégat est appropriée, comme décrit dans

"Identification de la capacité de performance restante".

## 2. Création d'une « policy group » :

```
qos policy-group create -policy group policy_group -vserver SVM -min  
-throughput qos_target -is-shared true|false
```

Pour connaître la syntaxe complète de la commande, consultez la page man de votre version de ONTAP. Vous pouvez utiliser le `qos policy-group modify` commande permettant de régler les étages de débit.

La commande suivante crée la « policy group » partagée `pg-vs2` Avec un débit minimal de 1,000 000 IOPS :

```
cluster1::> qos policy-group create -policy group pg-vs2 -vserver vs2  
-min-throughput 1000iops -is-shared true
```

La commande suivante crée le « policy group » non partagé `pg-vs4` sans limite de débit :

```
cluster1::> qos policy-group create -policy group pg-vs4 -vserver vs4  
-is-shared false
```

## 3. Appliquer une « policy group » à un volume ou une LUN :

```
storage_object create -vserver SVM -qos-policy-group policy_group
```

Pour connaître la syntaxe complète des commandes, consultez les pages de manuels. Vous pouvez utiliser le `_storage_object_modify` commande pour appliquer un autre groupe de règles à l'objet de stockage.

La commande suivante applique la « policy group » `pg-app2` au volume `app2`:

```
cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr1  
-qos-policy-group pg-app2
```

## 4. Surveillance des performances des groupes de règles :

```
qos statistics performance show
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.



Contrôle des performances depuis le cluster. N'utilisez pas d'outil sur l'hôte pour surveiller les performances.

La commande suivante affiche les performances de « policy group » :

```
cluster1::> qos statistics performance show
```

Policy Group	IOPS	Throughput	Latency
-total-	12316	47.76MB/s	1264.00us
pg_app2	7216	28.19MB/s	420.00us
_System-Best-Effort	62	13.36KB/s	4.13ms
_System-Background	30	0KB/s	0ms

## 5. Contrôle de la performance des charges de travail :

```
qos statistics workload performance show
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page [man](#).



Contrôle des performances depuis le cluster. N'utilisez pas d'outil sur l'hôte pour surveiller les performances.

La commande suivante indique les performances des workloads :

```
cluster1::> qos statistics workload performance show
```

Workload	ID	IOPS	Throughput	Latency
-total-	-	12320	47.84MB/s	1215.00us
app2-wid7967	7967	7219	28.20MB/s	319.00us
vs1-wid12279	12279	5026	19.63MB/s	2.52ms
_USERSPACE_APPS	14	55	10.92KB/s	236.00us
_Scan_Backgro...	5688	20	0KB/s	0ms



Vous pouvez utiliser le `qos statistics workload latency show` Commande pour afficher les statistiques de latence détaillées pour les workloads de QoS.

### Utilisez les groupes de règles de QoS adaptatifs

Vous pouvez utiliser un groupe de règles *Adaptive QoS* pour dimensionner automatiquement un plafond de débit ou une taille de sol en fonction du volume, tout en maintenant le rapport IOPS/To|GBs lorsque la taille du volume change. C'est un avantage significatif pour la gestion de centaines, voire de milliers de charges de travail dans un déploiement à grande échelle.

#### Avant de commencer

- Vous devez exécuter ONTAP 9.3 ou une version ultérieure. Les groupes de règles de QoS adaptative sont disponibles à partir de la version ONTAP 9.3.
- Pour créer une « policy group » il faut être un administrateur de cluster.

#### Description de la tâche

Un objet de stockage peut être membre d'un groupe de règles adaptative ou d'un groupe de règles non adaptatif, mais pas des deux à la fois. Le SVM de l'objet de stockage et la politique doivent être identiques. L'objet de stockage doit être en ligne.

Les groupes de règles de QoS adaptative sont toujours non partagés : le plafond ou l'étage de débit défini s'applique à chaque charge de travail membre individuellement.

Le rapport entre les limites de débit et la taille de l'objet de stockage est déterminé par l'interaction des champs suivants :

- `expected-iops` Correspond au nombre minimal d'IOPS prévu par To|Go alloué.



``expected-iops`` Est garanti sur les plateformes AFF uniquement. ``expected-iops`` La garantie pour FabricPool est uniquement si la règle de Tiering est définie sur « aucune » et qu'aucun bloc n'est présent dans le cloud. ``expected-iops`` Est garanti pour les volumes qui ne font pas partie d'une relation SnapMirror synchrone.

- `peak-iops` Est le nombre maximal d'IOPS possible par To alloué ou utilisé|Go.
- `expected-iops-allocation` indique si l'espace alloué (par défaut) ou utilisé est utilisé pour les iops attendues.



`expected-iops-allocation` Est disponible dans ONTAP 9.5 et versions ultérieures. Elle n'est pas prise en charge par ONTAP 9.4 et les versions antérieures.

- `peak-iops-allocation` indique si l'espace alloué ou l'espace utilisé (par défaut) est utilisé pour `peak-iops`.
- `absolute-min-iops` Correspond au nombre minimal d'IOPS absolu. Vous pouvez utiliser ce champ avec de très petits objets de stockage. Elle remplace les deux `peak-iops` et/ou `expected-iops` quand `absolute-min-iops` est supérieur au calcul `expected-iops`.

Par exemple, si vous définissez `expected-iops` À 1,000 000 IOPS/To et la taille du volume est inférieure à 1 Go, le calcul est effectué `expected-iops` Il s'agit d'une IOP fractionnaires. Le calculé `peak-iops` sera une fraction encore plus petite. Vous pouvez éviter cela en définissant le paramètre `absolute-min-iops` à une valeur réaliste.

- `block-size` Spécifie la taille du bloc d'E/S de l'application. La valeur par défaut est 32 Ko. Les valeurs valides sont de 8 Ko, 16 Ko, 32 K, 64 Ko, N'IMPORTE QUEL. TOUTE signifie que la taille de bloc n'est pas appliquée.

Trois groupes de règles de QoS adaptative par défaut sont disponibles, comme illustré dans le tableau ci-dessous. Vous pouvez appliquer ces « policy group » directement à un volume.

Groupe de règles par défaut	IOPS/To attendu	Pic d'IOPS/To	IOPS min. Absolu
extreme	6,144	12,288	1000

performance	2,048	4,096	500
value	128	512	75

Vous ne pouvez pas affecter un objet de stockage à un groupe de règles si son objet contenant ou ses objets enfants appartiennent à un groupe de règles. Le tableau suivant répertorie les restrictions.

Si vous attribuez...	Vous ne pouvez alors pas affecter...
SVM vers une « policy group »	Tout objet de stockage contenu par la SVM vers une « policy group »
Volume vers une « policy group »	Le volume contenant un SVM ou toute LUN enfant vers un « policy group »
LUN vers une « policy group »	La LUN contenant le volume ou le SVM à une « policy group »
Fichier dans une « policy group »	Fichier contenant le volume ou SVM vers une « policy group »

## Étapes

### 1. Création d'une « policy group » QoS adaptative :

```
qos adaptive-policy-group create -policy group policy_group -vserver SVM
-expected-iops number_of_iops/TB|GB -peak-iops number_of_iops/TB|GB -expected
-iops-allocation-space|used-space -peak-iops-allocation allocated-space|used-
space -absolute-min-iops number_of_iops -block-size 8K|16K|32K|64K|ANY
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.



-expected-iops-allocation et -block-size Est disponible dans ONTAP 9.5 et versions ultérieures. Ces options ne sont pas prises en charge par ONTAP 9.4 et les versions antérieures.

La commande suivante crée une « policy group » QoS adaptative *adpg-appl* avec -expected-iops Défini sur 300 IOPS/To, -peak-iops Définis sur 1,000 IOPS/To, -peak-iops-allocation réglez sur used-space, et -absolute-min-iops Définissez sur 50 IOPS :

```
cluster1::> qos adaptive-policy-group create -policy group adpg-appl
-vserver vs2 -expected-iops 300iops/tb -peak-iops 1000iops/TB -peak-iops
-allocation used-space -absolute-min-iops 50iops
```

### 2. Appliquer une « policy group » QoS adaptative à un volume :

```
volume create -vserver SVM -volume volume -aggregate aggregate -size number_of
TB|GB -qos-adaptive-policy-group policy_group
```

Pour connaître la syntaxe complète des commandes, consultez les pages de manuels.

La commande suivante applique la « policy group » de QoS adaptative `adpg-app1` au volume `app1`:

```
cluster1::> volume create -vserver vs1 -volume app1 -aggregate aggr1  
-size 2TB -qos-adaptive-policy-group adpg-app1
```

Les commandes suivantes appliquent le groupe de règles de QoS adaptative par défaut `extreme` au nouveau volume `app4` et au volume existant `app5`. Le plafond de débit défini pour le groupe de règles s'applique aux volumes `app4` et `app5` chaque participant :

```
cluster1::> volume create -vserver vs4 -volume app4 -aggregate aggr4  
-size 2TB -qos-adaptive-policy-group extreme
```

```
cluster1::> volume modify -vserver vs5 -volume app5 -qos-adaptive-policy  
-group extreme
```

### Définissez un modèle de groupe de règles adaptatives

À partir de la ONTAP 9.13.1, vous pouvez appliquer des seuils et des plafonds de débit au niveau des SVM en utilisant un modèle de groupe de règles adaptatif.

#### Description de la tâche

- Le modèle de groupe de règles adaptatives est une règle par défaut `apg1`. La règle peut être modifiée à tout moment. Elle peut uniquement être définie avec l'interface de ligne de commandes ou l'API REST de ONTAP et s'applique uniquement aux SVM existants.
- Le modèle de groupe de règles adaptatives n'a d'impact que sur les volumes créés sur le SVM ou migrés vers celui-ci une fois la règle définie. Les volumes existants de la SVM conservent leur état existant.

Si vous désactivez le modèle de « Adaptive policy group », les volumes de la SVM conservent leurs règles existantes. Seuls les volumes créés ou migrés vers le SVM seront affectés par l'interruption.

- Vous ne pouvez pas définir de modèle de « policy group » adaptatif sur une SVM disposant d'une « policy group » QoS.
- Les modèles de groupes de règles adaptatifs sont conçus pour les plateformes AFF. Un modèle de groupe de règles adaptatives peut être défini sur d'autres plates-formes, mais la stratégie peut ne pas imposer un débit minimal. De même, vous pouvez ajouter un modèle de groupe de règles adaptatives à un SVM dans un agrégat FabricPool ou dans un agrégat ne prenant pas en charge un débit minimal, mais le débit ne sera pas appliqué.
- Si le SVM se trouve dans une configuration MetroCluster ou une relation SnapMirror, le modèle de groupe de règles adaptatives sera appliqué sur le SVM en miroir.

#### Étapes

1. Modifier le SVM pour appliquer le modèle Adaptive policy group : `vserver modify -qos-adaptive-policy-group-template apg1`



2. Vérifiez que la règle a été définie : `vserver show -fields qos-adaptive-policy-group`

## Informations sur le copyright

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

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

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