



# Surveiller et résoudre les problèmes

## StorageGRID 11.9

NetApp  
November 08, 2024

# Sommaire

- Surveillance et dépannage d'un système StorageGRID ..... 1
  - Surveiller le système StorageGRID ..... 1
  - Dépanner le système StorageGRID ..... 187
  - Examiner les journaux d'audit ..... 240

# Surveillance et dépannage d'un système StorageGRID

## Surveiller le système StorageGRID

### Surveiller un système StorageGRID

Surveillez régulièrement votre système StorageGRID pour vous assurer qu'il fonctionne comme prévu.

#### Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).



Pour modifier les unités des valeurs de stockage affichées dans le Gestionnaire de grille, sélectionnez la liste déroulante utilisateur dans le coin supérieur droit du Gestionnaire de grille, puis sélectionnez **Préférences utilisateur**.

#### Description de la tâche

Ces instructions expliquent comment :

- ["Affichez et gérez le tableau de bord"](#)
- ["Afficher la page nœuds"](#)
- ["Surveiller régulièrement ces aspects du système :"](#)
  - ["État du système"](#)
  - ["Capacité de stockage"](#)
  - ["Gestion du cycle de vie des informations"](#)
  - ["Ressources réseau et système"](#)
  - ["Activité des locataires"](#)
  - ["Opérations d'équilibrage de la charge"](#)
  - ["Connexions de fédération de grille"](#)
- ["Gérer les alertes"](#)
- ["Afficher les fichiers journaux"](#)
- ["Configurez les messages d'audit et les destinations des journaux"](#)
- ["Utiliser un serveur syslog externe"](#) pour collecter des informations d'audit
- ["Utilisez SNMP pour la surveillance"](#)
- ["Obtenir des données StorageGRID supplémentaires"](#), y compris les mesures et les diagnostics

#### Affichez et gérez le tableau de bord

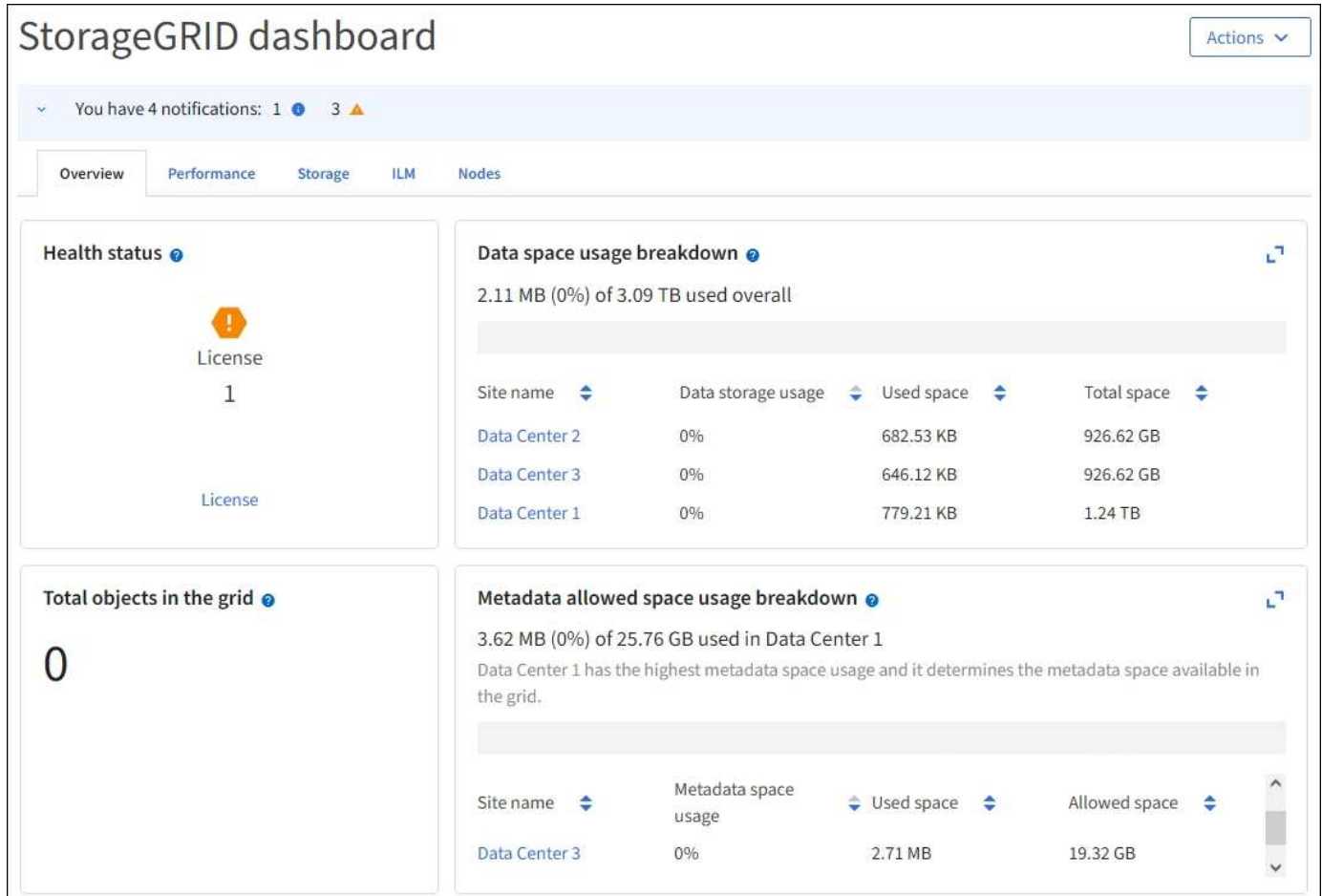
Vous pouvez utiliser le tableau de bord pour surveiller les activités du système en un coup d'œil. Vous pouvez créer des tableaux de bord personnalisés pour contrôler votre

## implémentation de StorageGRID.



Pour modifier les unités des valeurs de stockage affichées dans le Gestionnaire de grille, sélectionnez la liste déroulante utilisateur dans le coin supérieur droit du Gestionnaire de grille, puis sélectionnez **Préférences utilisateur**.

Votre tableau de bord peut varier en fonction de la configuration du système.



### Afficher le tableau de bord



Le tableau de bord se compose d'onglets contenant des informations spécifiques sur le système StorageGRID. Chaque onglet contient des catégories d'informations affichées sur les cartes.

Vous pouvez utiliser le tableau de bord fourni par le système, tel qu'il est. En outre, vous pouvez créer des tableaux de bord personnalisés contenant uniquement les onglets et cartes pertinents pour la surveillance de votre implémentation de StorageGRID.

Les onglets du tableau de bord fournis par le système contiennent des cartes présentant les types d'informations suivants :

Du tableau de bord fourni par le système	Contient
Présentation	Informations générales sur la grille, telles que les alertes actives, l'utilisation de l'espace et le nombre total d'objets de la grille.

Du tableau de bord fourni par le système	Contient
Performances	Utilisation de l'espace, stockage utilisé au fil du temps, opérations S3, durée de la demande, taux d'erreur.
Stockage	Utilisation des quotas des locataires et de l'espace logique. Prévisions de l'utilisation de l'espace pour les données utilisateur et les métadonnées.
ILM	File d'attente de gestion du cycle de vie des informations et taux d'évaluation.
Nœuds	Utilisation du CPU, des données et de la mémoire par nœud. Opérations S3 par nœud. Distribution nœud à site.

Certaines cartes peuvent être agrandies pour faciliter la visualisation. Sélectionnez l'icône Agrandir  dans le coin supérieur droit de la carte. Pour fermer une carte agrandie, sélectionnez l'icône réduire  ou sélectionnez **Fermer**.

## Gestion des tableaux de bord

Si vous disposez d'un accès racine (voir "[Autorisations de groupe d'administration](#)"), vous pouvez effectuer les tâches de gestion suivantes pour les tableaux de bord :

- Créez un tableau de bord personnalisé à partir de zéro. Vous pouvez utiliser des tableaux de bord personnalisés pour contrôler quelles informations StorageGRID sont affichées et comment elles sont organisées.
- Cloner un tableau de bord pour créer des tableaux de bord personnalisés.
- Définir un tableau de bord actif pour un utilisateur. Le tableau de bord actif peut être celui fourni par le système ou un tableau de bord personnalisé.
- Définissez un tableau de bord par défaut, qui correspond à ce que tous les utilisateurs voient, à moins qu'ils n'activent leur propre tableau de bord.
- Modifiez le nom d'un tableau de bord.
- Modifiez un tableau de bord pour ajouter ou supprimer des onglets et des cartes. Vous pouvez avoir un minimum de 1 et un maximum de 20 onglets.
- Déposer un tableau de bord.



Si vous disposez d'une autre autorisation que l'accès racine, vous ne pouvez définir qu'un tableau de bord actif.

Pour gérer les tableaux de bord, sélectionnez **actions > gérer les tableaux de bord**.



StorageGRID dashboard

Vous avez 4 notifications: 1  3 

Overview Performance Storage ILM Nodes

Actions 

Clone active dashboard

Manage dashboards

## Configurer les tableaux de bord

Pour créer un nouveau tableau de bord en clonant le tableau de bord actif, sélectionnez **actions** > **Cloner le tableau de bord actif**.

Pour modifier ou cloner un tableau de bord existant, sélectionnez **actions** > **gérer les tableaux de bord**.



Le tableau de bord fourni par le système ne peut pas être modifié ou supprimé.

Lors de la configuration d'un tableau de bord, vous pouvez :

- Ajouter ou supprimer des onglets
- Renommez les onglets et donnez des noms uniques aux nouveaux onglets
- Ajoutez, supprimez ou réorganisez (faites glisser) des cartes pour chaque onglet
- Sélectionnez la taille des cartes individuelles en sélectionnant **S**, **M**, **L** ou **XL** en haut de la carte

Site name	Data storage usage	Used space	Total space
Data Center 1	0%	1.79 MB	1.24 TB
Data Center 2	0%	921.11 KB	926.62 GB
Data Center 3	0%	790.21 KB	926.62 GB

## Afficher la page nœuds

### Afficher la page nœuds

Si vous avez besoin d'informations plus détaillées sur votre système StorageGRID que le tableau de bord ne l'indique, vous pouvez utiliser la page nœuds pour afficher les mesures de la grille dans son intégralité, de chaque site de la grille et de chaque nœud d'un site.

Le tableau nœuds répertorie les informations récapitulatives pour l'ensemble de la grille, chaque site et chaque nœud. Si un nœud est déconnecté ou dispose d'une alerte active, une icône s'affiche en regard du nom du nœud. Si le nœud est connecté et ne dispose d'aucune alerte active, aucune icône n'est affichée.



Lorsqu'un nœud n'est pas connecté à la grille, comme lors de la mise à niveau ou lorsqu'il est déconnecté, certains metrics peuvent être indisponibles ou exclus des totaux site et grid. Après qu'un nœud se reconnecte à la grille, attendez plusieurs minutes que les valeurs se stabilisent.



Pour modifier les unités des valeurs de stockage affichées dans le Gestionnaire de grille, sélectionnez la liste déroulante utilisateur dans le coin supérieur droit du Gestionnaire de grille, puis sélectionnez **Préférences utilisateur**.






Les captures d'écran illustrées sont des exemples. Vos résultats peuvent varier en fonction de votre version de StorageGRID.

## Nodes



View the list and status of sites and grid nodes.

Search... Total node count: 12

Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID Webscale Deployment	Grid	0%	0%	—
DC1	Site	0%	0%	—
 DC1-ADM1	Primary Admin Node	—	—	6%
 DC1-ARC1	Archive Node	—	—	1%
 DC1-G1	Gateway Node	—	—	3%
DC1-S1	Storage Node	0%	0%	6%
DC1-S2	Storage Node	0%	0%	8%
DC1-S3	Storage Node	0%	0%	4%

### Icônes d'état de connexion


Si un nœud est déconnecté de la grille, l'une des icônes suivantes s'affiche en regard du nom du nœud.


Icône	Description	Action requise
	<p><b>Non connecté - Inconnu</b></p> <p>Pour une raison inconnue, un nœud est déconnecté ou les services du nœud sont arrêtés de manière inattendue. Par exemple, un service du nœud peut être arrêté, ou le nœud a perdu sa connexion réseau en raison d'une panne de courant ou d'une panne imprévue.</p> <p>L'alerte <b>Impossible de communiquer avec le nœud</b> peut également être déclenchée. D'autres alertes peuvent également être actives.</p>	<p>Nécessite une attention immédiate. "Sélectionnez chaque alerte" et suivre les actions recommandées.</p> <p>Par exemple, vous devrez peut-être redémarrer un service qui a arrêté ou redémarré l'hôte du nœud.</p> <p><b>Remarque</b> : un nœud peut apparaître comme inconnu pendant les opérations d'arrêt gérées. Dans ces cas, vous pouvez ignorer l'état Inconnu.</p>
	<p><b>Non connecté - Arrêt administratif</b></p> <p>Pour une raison prévue, le nœud n'est pas connecté au grid.</p> <p>Par exemple, le nœud ou les services du nœud ont été normalement arrêtés, le nœud est en cours de redémarrage ou le logiciel est mis à niveau. Une ou plusieurs alertes peuvent également être actives.</p> <p>En fonction du problème sous-jacent, ces nœuds sont souvent remis en ligne sans intervention.</p>	<p>Déterminez si des alertes affectent ce nœud.</p> <p>Si une ou plusieurs alertes sont actives "Sélectionnez chaque alerte" et suivez les actions recommandées.</p>


Si un nœud est déconnecté de la grille, une alerte sous-jacente peut apparaître, mais seule l'icône « non connecté » s'affiche. Pour afficher les alertes actives d'un nœud, sélectionnez le nœud.

#### Icônes d'alerte

Si une alerte est active pour un nœud, l'une des icônes suivantes s'affiche à côté du nom du nœud :

 **Critique** : il existe une condition anormale qui a arrêté les opérations normales d'un nœud ou d'un service StorageGRID. Vous devez immédiatement résoudre le problème sous-jacent. Une interruption du service et une perte de données peuvent se produire si le problème n'est pas résolu.

 **Majeur** : il existe une condition anormale qui affecte les opérations en cours ou qui approche du seuil pour une alerte critique. Vous devez examiner les alertes majeures et résoudre tous les problèmes sous-jacents pour vérifier que leur condition anormale n'arrête pas le fonctionnement normal d'un nœud ou d'un service StorageGRID.

 **Mineur** : le système fonctionne normalement, mais il existe une condition anormale qui pourrait affecter la capacité de fonctionnement du système s'il continue. Vous devez surveiller et résoudre les alertes mineures qui ne sont pas claires par elles-mêmes pour vous assurer qu'elles n'entraînent pas de problème plus grave.



## Afficher les détails d'un système, d'un site ou d'un nœud

Pour filtrer les informations affichées dans la table nœuds, entrez une chaîne de recherche dans le champ **Search**. Vous pouvez effectuer une recherche par nom de système, nom d'affichage ou type (par exemple, entrez **gat** pour localiser rapidement tous les nœuds de passerelle).

Pour afficher les informations de la grille, du site ou du nœud :

- Sélectionnez le nom de la grille pour afficher un récapitulatif des agrégats des statistiques de l'ensemble du système StorageGRID.
- Sélectionnez un site de data Center spécifique pour afficher un résumé global des statistiques pour tous les nœuds de ce site.
- Sélectionnez un nœud spécifique pour afficher des informations détaillées sur ce nœud.

## Afficher l'onglet vue d'ensemble

L'onglet Présentation fournit des informations de base sur chaque nœud. Il affiche également toutes les alertes qui affectent actuellement le nœud.

L'onglet vue d'ensemble s'affiche pour tous les nœuds.

### Informations sur le nœud

La section informations sur les nœuds de l'onglet vue d'ensemble répertorie les informations de base sur le nœud.

**NYC-ADM1 (Primary Admin Node)** [↗](#)

**Overview** Hardware Network Storage Load balancer Tasks

**Node information** [?](#)

Display name: NYC-ADM1

System name: DC1-ADM1

Type: Primary Admin Node

ID: 3adb1aa8-9c7a-4901-8074-47054aa06ae6


Connection state: **Connected**


Software version: 11.7.0



IP addresses: 10.96.105.85 - eth0 (Grid Network)

[Show additional IP addresses](#)

Les informations de présentation d'un nœud incluent les éléments suivants :

- **Nom d’affichage** (affiché uniquement si le nœud a été renommé) : le nom d’affichage actuel du nœud. Utilisez la "[Renommez la grille, les sites et les nœuds](#)" procédure pour mettre à jour cette valeur.
- **Nom du système** : le nom que vous avez saisi pour le nœud lors de l’installation. Les noms de système sont utilisés pour les opérations StorageGRID internes et ne peuvent pas être modifiés.
- **Type** : le type de nœud — nœud Admin, nœud Admin principal, nœud de stockage ou nœud passerelle.
- **ID** : identificateur unique du nœud, qui est également appelé UUID.
- **Etat de connexion** : l’un des trois États. L’icône de l’état le plus grave est affichée.
  - **Inconnu**  : pour une raison inconnue, le nœud n’est pas connecté à la grille ou un ou plusieurs services sont arrêtés de façon inattendue. Par exemple, la connexion réseau entre les nœuds a été perdue, l’alimentation est en panne ou un service est en panne. L’alerte **Impossible de communiquer avec le nœud** peut également être déclenchée. D’autres alertes peuvent également être actives. Cette situation exige une attention immédiate.
 



Un nœud peut apparaître comme inconnu lors des opérations d’arrêt géré. Dans ces cas, vous pouvez ignorer l’état Inconnu.
  - **Administrativement arrêté**  : le nœud n’est pas connecté à la grille pour une raison prévue. Par exemple, le nœud ou les services du nœud ont été normalement arrêtés, le nœud est en cours de redémarrage ou le logiciel est mis à niveau. Une ou plusieurs alertes peuvent également être actives.
  - **Connecté**  : le nœud est connecté à la grille.
- **Stockage utilisé** : pour les nœuds de stockage uniquement.
  - **Données d’objet** : pourcentage de l’espace total utilisable pour les données d’objet qui ont été utilisées sur le nœud de stockage.
  - **Métadonnées d’objet** : pourcentage de l’espace total autorisé pour les métadonnées d’objet qui ont été utilisées sur le nœud de stockage.
- **Version du logiciel** : la version de StorageGRID installée sur le nœud.
- **Groupes HA** : pour les nœuds d’administration et de passerelle uniquement. Indique si une interface réseau sur le nœud est incluse dans un groupe haute disponibilité et si cette interface est l’interface principale.
- **Adresses IP** : adresses IP du nœud. Cliquez sur **Afficher des adresses IP supplémentaires** pour afficher les adresses IPv4 et IPv6 du nœud ainsi que les mappages d’interface.

## Alertes

La section alertes de l’onglet vue d’ensemble répertorie tous les "[alertes affectant actuellement ce nœud qui n’ont pas été neutralisées](#)". Sélectionnez le nom de l’alerte pour afficher des détails supplémentaires et les actions recommandées.

## Alerts

Alert name	Severity	Time triggered	Current values
<a href="#">Low installed node memory</a> The amount of installed memory on a node is low.	<span style="color: red;">✖</span> Critical	11 hours ago	Total RAM size: 8.37 GB

Des alertes sont également incluses pour "états de connexion de nœud".

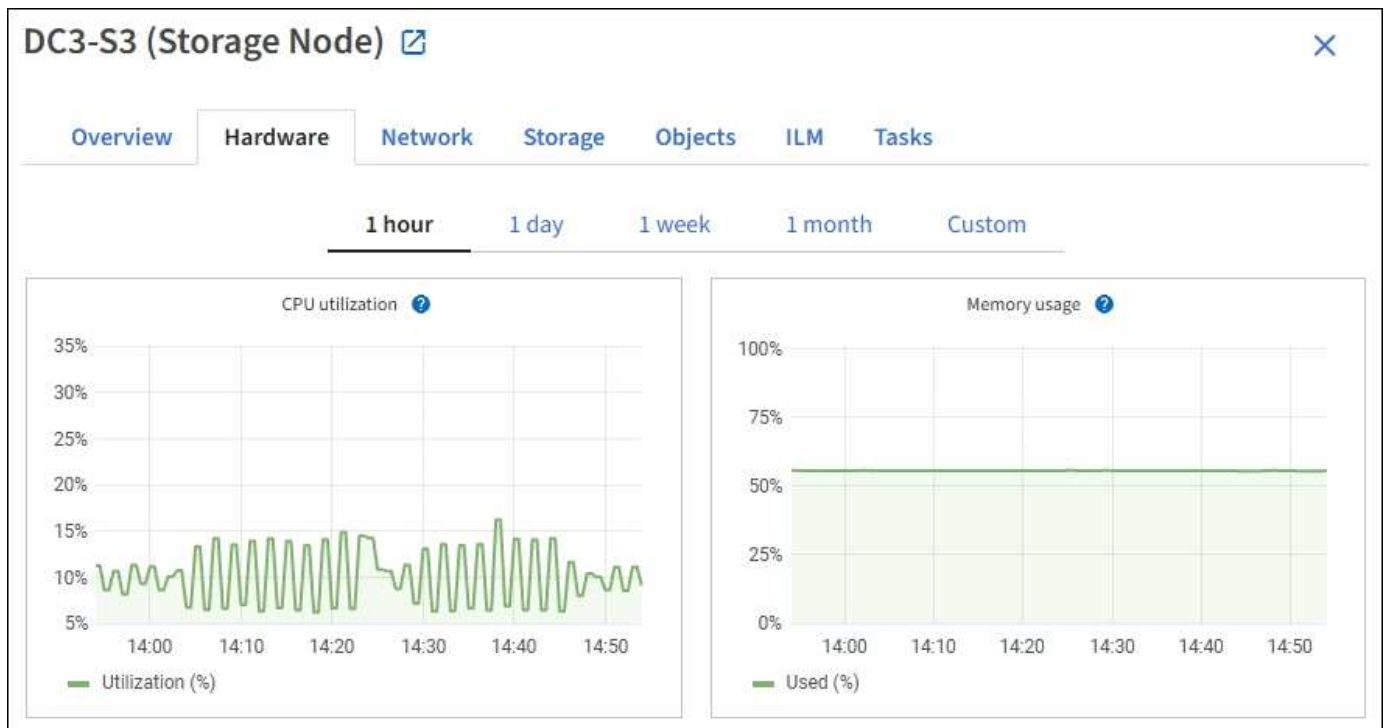
## Afficher l'onglet matériel

L'onglet matériel affiche l'utilisation du CPU et de la mémoire pour chaque nœud, ainsi que des informations supplémentaires sur le matériel des appliances.



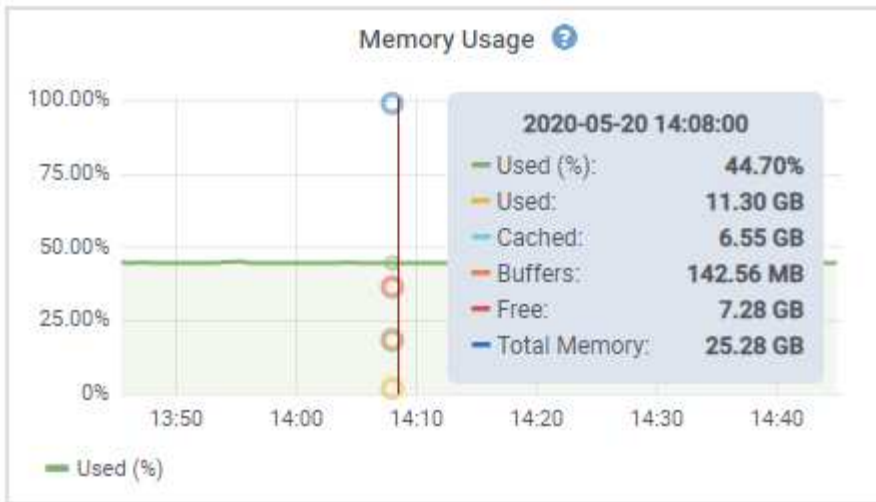
Le Gestionnaire de grille est mis à jour avec chaque version et peut ne pas correspondre aux exemples de captures d'écran de cette page.

L'onglet matériel s'affiche pour tous les nœuds.



Pour afficher un intervalle de temps différent, sélectionnez l'une des commandes au-dessus du graphique ou du graphique. Vous pouvez afficher les informations disponibles pour les intervalles de 1 heure, 1 jour, 1 semaine ou 1 mois. Vous pouvez également définir un intervalle personnalisé, qui vous permet de spécifier des plages de date et d'heure.

Pour afficher des détails sur l'utilisation du CPU et de la mémoire, placez votre curseur sur chaque graphique.



Si le nœud est un nœud d'appliance, cet onglet inclut également une section contenant des informations supplémentaires sur le matériel de l'appliance.

### Afficher des informations sur les nœuds de stockage de l'appliance

La page nœuds répertorie les informations relatives à l'état des services et à toutes les ressources de calcul, de périphérique de disque et de réseau pour chaque nœud de stockage d'appliance. Vous pouvez également afficher la mémoire, le matériel de stockage, la version du firmware des contrôleurs, les ressources réseau, les interfaces réseau, les adresses réseau et de réception et de transmission des données.

### Étapes

1. Sur la page nœuds, sélectionnez un nœud de stockage d'appliance.
2. Sélectionnez **vue d'ensemble**.

La section informations sur le nœud de l'onglet Présentation affiche un récapitulatif des informations sur le nœud, telles que le nom, le type, l'ID et l'état de connexion du nœud. La liste des adresses IP inclut le nom de l'interface pour chaque adresse, comme suit :


- **Eth** : réseau Grid, réseau Admin ou réseau client.
- **Hic** : un des ports physiques 10, 25 ou 100 GbE de l'appareil. Ces ports peuvent être liés ensemble et connectés au réseau StorageGRID Grid Network (eth0) et au réseau client (eth2).
- **mtc** : l'un des ports physiques 1 GbE de l'appareil. Une ou plusieurs interfaces mtc sont liées pour former l'interface réseau d'administration StorageGRID (eth1). Vous pouvez laisser d'autres interfaces mtc disponibles pour une connectivité locale temporaire pour un technicien du centre de données.

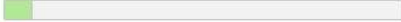
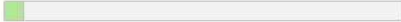
[Overview](#) [Hardware](#) [Network](#) [Storage](#) [Objects](#) [ILM](#) [Tasks](#)Node information [?](#)

Name: DC2-SGA-010-096-106-021

Type: Storage Node

ID: f0890e03-4c72-401f-ae92-245511a38e51

Connection state:  Connected

Storage used: Object data  7% [?](#)  
Object metadata  5% [?](#)

Software version: 11.6.0 (build 20210915.1941.afce2d9)

IP addresses: 10.96.106.21 - eth0 (Grid Network)

[Hide additional IP addresses](#) [^](#)

Interface <a href="#">?</a>	IP address <a href="#">?</a>
eth0 (Grid Network)	10.96.106.21
eth0 (Grid Network)	fe80::2a0:98ff:fe64:6582
hic2	10.96.106.21
hic4	10.96.106.21
mtc2	169.254.0.1

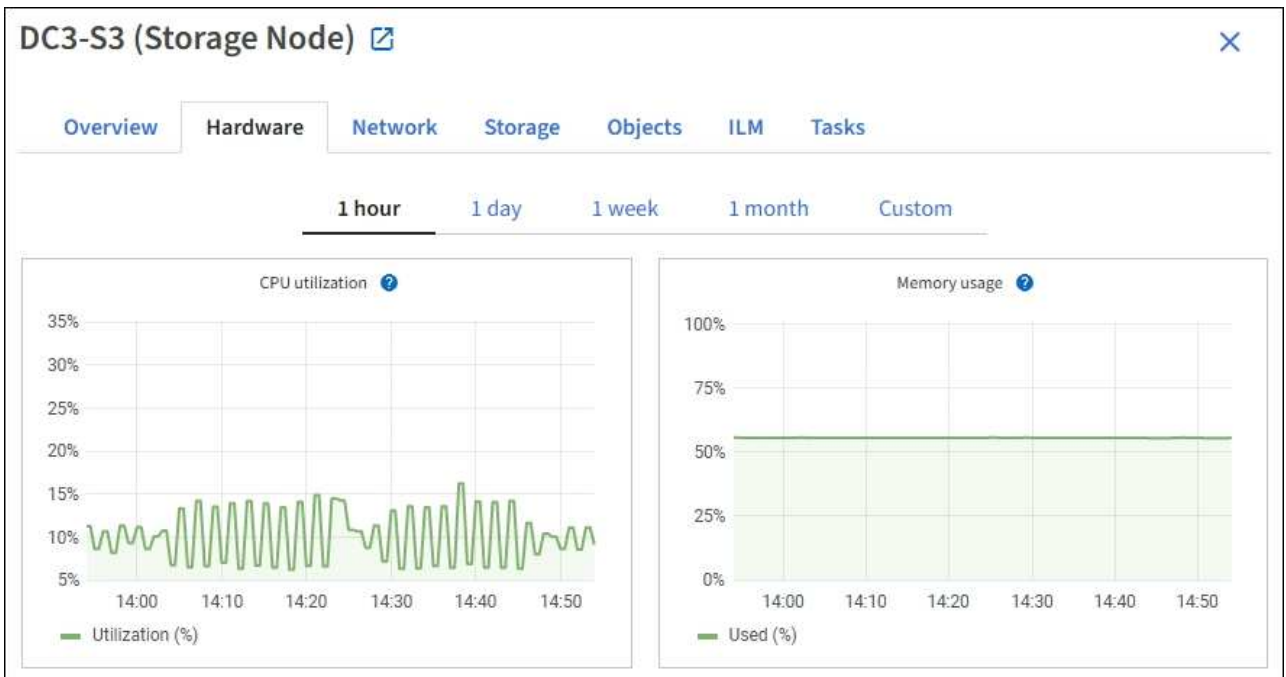
## Alerts

Alert name <a href="#">?</a>	Severity <a href="#">?</a> <a href="#">?</a>	Time triggered <a href="#">?</a>	Current values
<a href="#">ILM placement unachievable</a> <a href="#">?</a>	 Major	2 hours ago <a href="#">?</a>	
A placement instruction in an ILM rule cannot be achieved for certain objects.			

La section alertes de l'onglet Overview affiche toutes les alertes actives du nœud.

3. Sélectionnez **matériel** pour plus d'informations sur l'appareil.

- Affichez les graphiques d'utilisation de l'UC et de la mémoire pour déterminer les pourcentages d'utilisation de l'UC et de la mémoire au fil du temps. Pour afficher un intervalle de temps différent, sélectionnez l'une des commandes au-dessus du graphique ou du graphique. Vous pouvez afficher les informations disponibles pour les intervalles de 1 heure, 1 jour, 1 semaine ou 1 mois. Vous pouvez également définir un intervalle personnalisé, qui vous permet de spécifier des plages de date et d'heure.



- b. Faites défiler vers le bas pour afficher le tableau des composants de l'appareil. Ce tableau contient des informations telles que le nom du modèle de l'appliance, les noms des contrôleurs, les numéros de série et les adresses IP, ainsi que l'état de chaque composant.



Certains champs, tels que le contrôleur de calcul BMC IP et le matériel de calcul, apparaissent uniquement pour les appliances dotées de cette fonctionnalité.

Les composants des tiroirs de stockage et des tiroirs d'extension s'ils font partie de l'installation apparaissent dans un tableau séparé sous le tableau de l'appliance.

## StorageGRID Appliance

Appliance model: ?	SG6060	
Storage controller name: ?	StorageGRID-Lab79-SG6060-7-134	
Storage controller A management IP: ?	10.2	
Storage controller B management IP: ?	10.2	
Storage controller WWID: ?	6d039ea0000173e50000000065b7b761	
Storage appliance chassis serial number: ?	721924500068	
Storage controller firmware version: ?	08.53.00.09	
Storage controller SANtricity OS version: ?	11.50.3R2	
Storage controller NVSRAM version: ?	N280X-853834-DG1	
Storage hardware: ?	Nominal	
Storage controller failed drive count: ?	0	
Storage controller A: ?	Nominal	
Storage controller B: ?	Nominal	
Storage controller power supply A: ?	Nominal	
Storage controller power supply B: ?	Nominal	
Storage data drive type: ?	NL-SAS HDD	
Storage data drive size: ?	4.00 TB	
Storage RAID mode: ?	DDP16	
Storage connectivity: ?	Nominal	
Overall power supply: ?	Degraded	
Compute controller BMC IP: ?	10.2	
Compute controller serial number: ?	721917500060	
Compute hardware: ?	Needs Attention	
Compute controller CPU temperature: ?	Nominal	
Compute controller chassis temperature: ?	Nominal	
Compute controller power supply A: ?	Failed	
Compute controller power supply B: ?	Nominal	

## Storage shelves

Shelf chassis serial number ?	Shelf ID ?	Shelf status ?	IOM status ?	Power supply status ?	Drawer status ?	Fan status
721924500068	99	Nominal	N/A	Nominal	Nominal	Nominal

Dans la table Appliance	Description
Modèle de type appliance	Le numéro de modèle de cette appliance StorageGRID est indiqué dans SANtricity OS.
Nom du contrôleur de stockage	Nom de cette appliance StorageGRID représenté dans SANtricity OS.
IP de gestion A du contrôleur de stockage	Adresse IP du port de gestion 1 du contrôleur de stockage A. cette adresse IP vous permet d'accéder à SANtricity OS pour résoudre les problèmes de stockage.
IP de gestion du contrôleur de stockage B	Adresse IP du port de gestion 1 du contrôleur de stockage B. cette adresse IP vous permet d'accéder à SANtricity OS pour résoudre les problèmes de stockage.  Certains modèles d'appliance ne disposent pas de contrôleur de stockage B.

Dans la table Appliance	Description
WWID du contrôleur de stockage	Identifiant universel du contrôleur de stockage indiqué dans SANtricity OS.
Numéro de série du châssis de l'appliance de stockage	Numéro de série du châssis de l'appareil.
Version du firmware du contrôleur de stockage	Version du firmware du contrôleur de stockage de cette appliance.
Version du contrôleur de stockage SANtricity OS	Version SANtricity OS du contrôleur de stockage A.
Version NVSRAM du contrôleur de stockage	Version NVSRAM du contrôleur de stockage telle que signalée par le Gestionnaire système SANtricity.  Pour les SG6060 et SG6160, si la version de NVSRAM ne correspond pas entre les deux contrôleurs, la version du contrôleur A s'affiche. Si le contrôleur A n'est pas installé ou opérationnel, la version du contrôleur B s'affiche.
Matériel de stockage	État global du matériel du contrôleur de stockage. Si SANtricity System Manager signale un état de nécessité une intervention pour le matériel de stockage, le système StorageGRID signale également cette valeur.  Si l'état est « nécessite une intervention », vérifiez d'abord le contrôleur de stockage à l'aide de SANtricity OS. Ensuite, assurez-vous qu'il n'existe aucune autre alerte qui s'applique au contrôleur de calcul.
Nombre de disques défectueux du contrôleur de stockage	Le nombre de disques qui ne sont pas optimaux.
Contrôleur de stockage A	L'état du contrôleur de stockage A.
Contrôleur de stockage B	État du contrôleur de stockage B. certains modèles d'appliance ne disposent pas d'un contrôleur de stockage B.
Alimentation A du contrôleur de stockage	L'état de l'alimentation A du contrôleur de stockage.
Alimentation B du contrôleur de stockage	L'état de l'alimentation B du contrôleur de stockage.
Type de disque de données de stockage	Type de disque dur (HDD) ou SSD (Solid State Drive) de l'appliance.



Dans la table Appliance	Description
Taille du disque de stockage des données	<p>La taille effective d'un lecteur de données.</p> <p>Pour le SG6160, la taille du disque cache s'affiche également.</p> <p><b>Remarque</b> : pour les nœuds avec tiroirs d'extension, utilisez plutôt le <a href="#">Taille de disque des données pour chaque tiroir</a>. La taille effective du disque peut varier en fonction du tiroir.</p>
Mode de stockage RAID	Mode RAID configuré pour l'appliance.
Connectivité du stockage	État de la connectivité du stockage.
Bloc d'alimentation général	L'état de toutes les alimentations de l'appareil.
IP BMC du contrôleur de calcul	<p>Adresse IP du port du contrôleur de gestion de la carte mère (BMC) dans le contrôleur de calcul. Vous utilisez cette adresse IP pour vous connecter à l'interface BMC afin de surveiller et de diagnostiquer le matériel de l'appliance.</p> <p>Ce champ ne s'affiche pas pour les modèles d'appliance qui ne contiennent pas de contrôleur BMC.</p>
Numéro de série du contrôleur de calcul	Numéro de série du contrôleur de calcul.
Matériel de calcul	L'état du matériel du contrôleur de calcul. Ce champ ne s'affiche pas pour les modèles d'appliance qui ne disposent pas de matériel de calcul et de stockage distinct.
Température du processeur du contrôleur de calcul	L'état de température de l'UC du contrôleur de calcul.
Température du châssis du contrôleur de calcul	État de température du contrôleur de calcul.

+

Dans le tableau tiroirs de stockage	Description
Numéro de série du châssis du tiroir	Numéro de série du châssis du tiroir de stockage.

Dans le tableau tiroirs de stockage	Description
ID du tiroir	Identificateur numérique du tiroir de stockage. <ul style="list-style-type: none"> <li>• 99 : tiroir contrôleur de stockage</li> <li>• 0 : premier tiroir d'extension</li> <li>• 1 : second tiroir d'extension</li> </ul> <b>Remarque</b> : les étagères d'extension s'appliquent uniquement aux SG6060 et SG6160.
État du tiroir	État global du shelf de stockage.
État du module d'E/S.	L'état des modules d'entrée/sortie (IOM) de tous les tiroirs d'extension. S/O s'il ne s'agit pas d'un tiroir d'extension.
État de l'alimentation électrique	État global des alimentations du tiroir de stockage.
État du tiroir	L'état des tiroirs dans le tiroir de rangement. N/A si la tablette ne contient pas de tiroirs.
État du ventilateur	État général des ventilateurs dans le shelf de stockage.
Emplacements de lecteur	Nombre total de slots de disque dans le shelf de stockage.
Disques de données	Nombre de disques du tiroir de stockage utilisés pour le stockage de données.
taille du lecteur de données	Taille effective d'un disque de données dans le tiroir de stockage.
Disques en cache	Nombre de disques du tiroir de stockage utilisés comme cache.
Taille du lecteur de cache	La taille du plus petit lecteur de cache dans le tiroir de stockage. En principe, les disques en cache sont de la même taille.
État de la configuration	L'état de configuration du tiroir de stockage.

a. Confirmer que tous les États sont « nominal ».

Si un état n'est pas « nominal », passez en revue les alertes actuelles. Vous pouvez également utiliser SANtricity System Manager pour en savoir plus sur certaines de ces valeurs matérielles. Reportez-vous aux instructions d'installation et d'entretien de votre appareil.

4. Sélectionnez **réseau** pour afficher les informations de chaque réseau.

Le graphique trafic réseau fournit un récapitulatif du trafic réseau global.



a. Consultez la section interfaces réseau.

Network interfaces						
Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status	
eth0	00:50:56:A7:66:75	10 Gigabit	Full	Off	Up	

Utilisez le tableau suivant avec les valeurs de la colonne **Speed** du tableau interfaces réseau pour déterminer si les ports réseau 10/25-GbE de l'apppliance ont été configurés pour utiliser le mode actif/sauvegarde ou le mode LACP.



Les valeurs indiquées dans le tableau supposent que les quatre liens sont utilisés.

Mode de liaison	Mode du lien	Vitesse de la liaison HIC individuelle (hic 1, hi2, hic 3, hic 4)	Vitesse réseau prévue pour la grille/le client (eth0, eth2)
Agrégat	LACP	25	100
Fixe	LACP	25	50
Fixe	Actif/sauvegarde	25	25
Agrégat	LACP	10	40
Fixe	LACP	10	20
Fixe	Actif/sauvegarde	10	10

Pour plus d'informations sur la configuration des ports 10/25-GbE, reportez-vous à la section "[Configurer les liaisons réseau](#)".

b. Passez en revue la section communication réseau.

Les tableaux de réception et de transmission indiquent le nombre d'octets et de paquets reçus et envoyés sur chaque réseau ainsi que d'autres mesures de réception et de transmission.

### Network communication

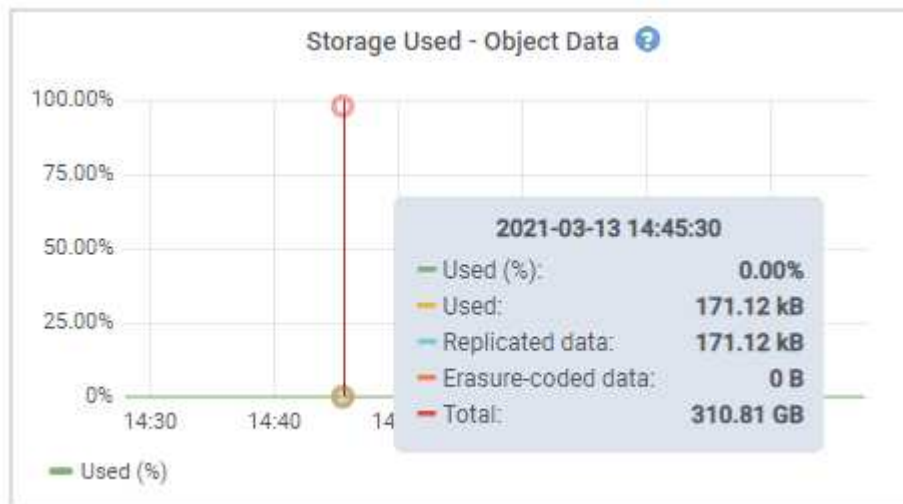
Receive

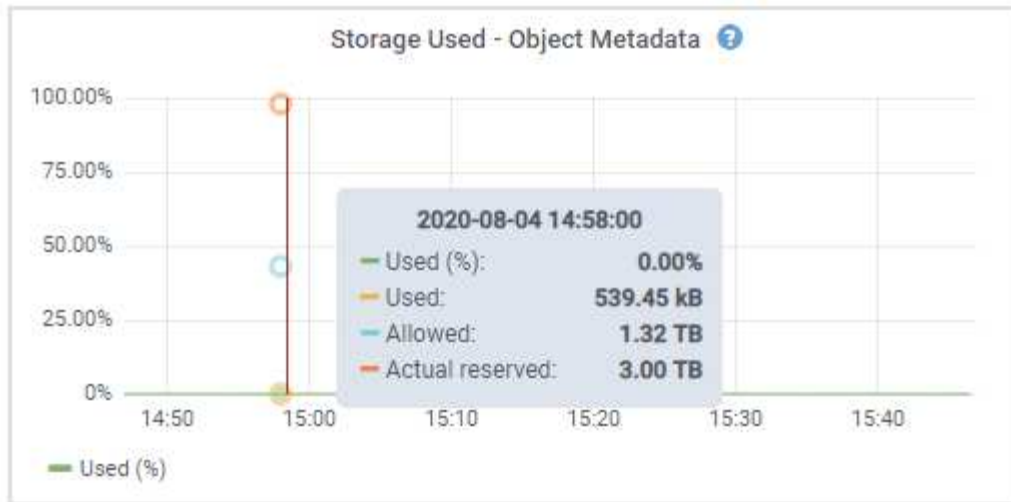
Interface	Data	Packets	Errors	Dropped	Frame overruns	Frames
eth0	2.89 GB	19,421,503	0	24,032	0	0

Transmit

Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	3.64 GB	18,494,381	0	0	0	0

- Sélectionnez **Storage** pour afficher les graphiques qui affichent les pourcentages de stockage utilisés dans le temps pour les données d'objet et les métadonnées d'objet, ainsi que des informations sur les unités de disque, les volumes et les magasins d'objets.





- a. Faites défiler vers le bas pour afficher les quantités de stockage disponibles pour chaque volume et magasin d'objets.

Le nom mondial de chaque disque correspond à l'identifiant universel (WWID) du volume qui s'affiche lorsque vous affichez les propriétés standard du volume dans SANtricity OS (le logiciel de gestion connecté au contrôleur de stockage de l'appliance).

Pour vous aider à interpréter les statistiques de lecture et d'écriture du disque relatives aux points de montage du volume, la première partie du nom affichée dans la colonne **Name** de la table Disk Devices (c'est-à-dire *sd*, *sdd*, *sde*, etc.) correspond à la valeur indiquée dans la colonne **Device** de la table volumes.

## Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.67%	0 bytes/s	50 KB/s
sdc(8:16,sdb)	N/A	0.03%	0 bytes/s	4 KB/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s

## Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.75 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.05 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled

## Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	124.60 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

### Affiche des informations sur les nœuds d'administration de l'appliance et les nœuds de passerelle

La page nœuds répertorie les informations relatives à l'état des services et à toutes les ressources de calcul, de périphérique de disque et de réseau pour chaque appliance de services utilisée comme nœud d'administration ou comme nœud de passerelle. Vous pouvez également afficher la mémoire, le matériel de stockage, les ressources réseau, les interfaces réseau, les adresses réseau, et recevoir et transmettre des données.

### Étapes

1. Sur la page nœuds, sélectionnez un nœud d'administration d'appliance ou un nœud de passerelle d'appliance.
2. Sélectionnez **vue d'ensemble**.

La section informations sur le nœud de l'onglet Présentation affiche un récapitulatif des informations sur le nœud, telles que le nom, le type, l'ID et l'état de connexion du nœud. La liste des adresses IP inclut le nom de l'interface pour chaque adresse, comme suit :

- **Adllb** et **adlli** : affiché si la liaison actif/sauvegarde est utilisée pour l'interface réseau d'administration
- **Eth** : réseau Grid, réseau Admin ou réseau client.
- **Hic** : un des ports physiques 10, 25 ou 100 GbE de l'appareil. Ces ports peuvent être liés ensemble et connectés au réseau StorageGRID Grid Network (eth0) et au réseau client (eth2).
- **mtc** : l'un des ports physiques 1 GbE de l'appareil. Une ou plusieurs interfaces mtc sont liées pour former l'interface réseau Admin (eth1). Vous pouvez laisser d'autres interfaces mtc disponibles pour une connectivité locale temporaire pour un technicien du centre de données.

**10-224-6-199-ADM1 (Primary Admin Node)**

Overview Hardware Network Storage Load balancer Tasks SANtricity System Manager

**Node information**

Name: 10-224-6-199-ADM1  
 Type: Primary Admin Node  
 ID: 6fdc1890-ca0a-4493-acdd-72ed317d95fb  
 Connection state: ✔ Connected  
 Software version: 11.6.0 (build 20210928.1321.6687ee3)  
 IP addresses: 172.16.6.199 - eth0 (Grid Network)  
 10.224.6.199 - eth1 (Admin Network)  
 47.47.7.241 - eth2 (Client Network)

[Hide additional IP addresses](#)

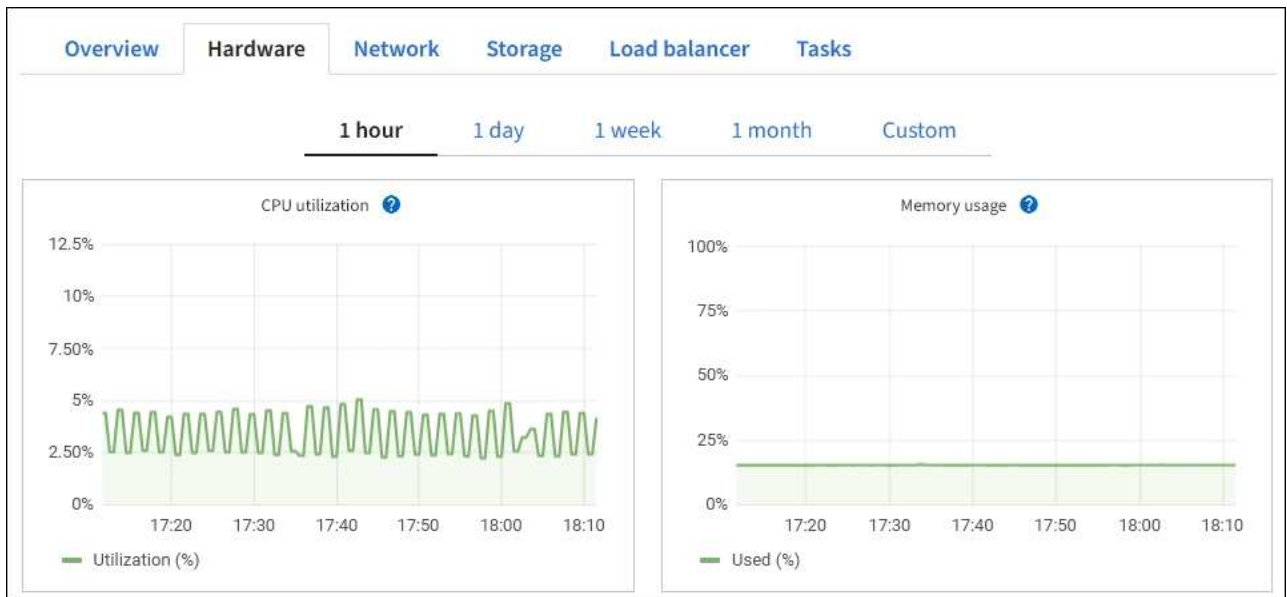
Interface	IP address
eth2 (Client Network)	47.47.7.241
eth2 (Client Network)	fd20:332:332:0:e42:a1ff:fe86:b5b0
eth2 (Client Network)	fe80::e42:a1ff:fe86:b5b0
hic1	47.47.7.241
hic2	47.47.7.241
hic3	47.47.7.241

La section alertes de l'onglet Overview affiche toutes les alertes actives du nœud.

### 3. Sélectionnez **matériel** pour plus d'informations sur l'appareil.

- affichez les graphiques d'utilisation de l'UC et de la mémoire pour déterminer les pourcentages d'utilisation de l'UC et de la mémoire au fil du temps. Pour afficher un intervalle de temps différent, sélectionnez l'une des commandes au-dessus du graphique ou du graphique. Vous pouvez afficher les informations disponibles pour les intervalles de 1 heure, 1 jour, 1 semaine ou 1 mois. Vous pouvez également définir un intervalle personnalisé, qui vous permet de spécifier des plages de date et

d'heure.



- b. Faites défiler vers le bas pour afficher le tableau des composants de l'appareil. Ce tableau contient des informations telles que le nom du modèle, le numéro de série, la version du micrologiciel du contrôleur et l'état de chaque composant.

StorageGRID Appliance		
Appliance model: ?	SG100	
Storage controller failed drive count: ?	0	
Storage data drive type: ?	SSD	
Storage data drive size: ?	960.20 GB	
Storage RAID mode: ?	RAID1 [healthy]	
Storage connectivity: ?	Nominal	
Overall power supply: ?	Nominal	
Compute controller BMC IP: ?	10.60.8.38	
Compute controller serial number: ?	372038000093	
Compute hardware: ?	Nominal	
Compute controller CPU temperature: ?	Nominal	
Compute controller chassis temperature: ?	Nominal	
Compute controller power supply A: ?	Nominal	
Compute controller power supply B: ?	Nominal	

Dans la table Appliance	Description
Modèle de type appliance	Numéro de modèle de cette appliance StorageGRID.



Dans la table Appliance	Description
Nombre de disques défectueux du contrôleur de stockage	Le nombre de disques qui ne sont pas optimaux.
Type de disque de données de stockage	Type de disque dur (HDD) ou SSD (Solid State Drive) de l'apppliance.
Taille du disque de stockage des données	La taille effective d'un lecteur de données.
Mode de stockage RAID	Mode RAID de l'appareil.
Bloc d'alimentation général	L'état de toutes les alimentations de l'appareil.
IP BMC du contrôleur de calcul	Adresse IP du port du contrôleur de gestion de la carte mère (BMC) dans le contrôleur de calcul. Vous pouvez utiliser cette adresse IP pour vous connecter à l'interface BMC afin de surveiller et de diagnostiquer le matériel de l'apppliance.  Ce champ ne s'affiche pas pour les modèles d'apppliance qui ne contiennent pas de contrôleur BMC.
Numéro de série du contrôleur de calcul	Numéro de série du contrôleur de calcul.
Matériel de calcul	L'état du matériel du contrôleur de calcul.
Température du processeur du contrôleur de calcul	L'état de température de l'UC du contrôleur de calcul.
Température du châssis du contrôleur de calcul	État de température du contrôleur de calcul.

a. Confirmer que tous les États sont « nominal ».

Si un état n'est pas « nominal », passez en revue les alertes actuelles.

4. Sélectionnez **réseau** pour afficher les informations de chaque réseau.

Le graphique trafic réseau fournit un récapitulatif du trafic réseau global.



a. Consultez la section interfaces réseau.

Network interfaces						
Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status	
eth0	0C:42:A1:86:B5:B0	100 Gigabit	Full	Off	Up	
eth1	B4:A9:FC:71:68:36	Gigabit	Full	Off	Up	
eth2	0C:42:A1:86:B5:B0	100 Gigabit	Full	Off	Up	
hic1	0C:42:A1:86:B5:B0	25 Gigabit	Full	On	Up	
hic2	0C:42:A1:86:B5:B0	25 Gigabit	Full	On	Up	
hic3	0C:42:A1:86:B5:B0	25 Gigabit	Full	On	Up	
hic4	0C:42:A1:86:B5:B0	25 Gigabit	Full	On	Up	
mtc1	B4:A9:FC:71:68:36	Gigabit	Full	On	Up	
mtc2	B4:A9:FC:71:68:35	Gigabit	Full	On	Up	

Utilisez le tableau suivant avec les valeurs de la colonne **Speed** du tableau interfaces réseau pour déterminer si les quatre ports réseau 40/100-GbE de l’appliance ont été configurés pour utiliser le mode actif/sauvegarde ou le mode LACP.



Les valeurs indiquées dans le tableau supposent que les quatre liens sont utilisés.

Mode de liaison	Mode du lien	Vitesse de la liaison HIC individuelle (hic 1, hi2, hic 3, hic 4)	Vitesse réseau prévue pour la grille/le client (eth0, eth2)
Agrégat	LACP	100	400
Fixe	LACP	100	200
Fixe	Actif/sauvegarde	100	100
Agrégat	LACP	40	160
Fixe	LACP	40	80
Fixe	Actif/sauvegarde	40	40

b. Passez en revue la section communication réseau.

Les tableaux de réception et de transmission indiquent le nombre d'octets et de paquets reçus et envoyés sur chaque réseau ainsi que d'autres mesures de réception et de transmission.



Network communication							
Receive							
Interface	Data	Packets	Errors	Dropped	Frame overruns	Frames	
eth0	2.89 GB	19,421,503	0	24,032	0	0	
Transmit							
Interface	Data	Packets	Errors	Dropped	Collisions	Carrier	
eth0	3.64 GB	18,494,381	0	0	0	0	

5. Sélectionnez **Storage** pour afficher des informations sur les unités de disque et les volumes de l'appliance de services.

## Disk devices

Name <a href="#">?</a> <a href="#">↕</a>	World Wide Name <a href="#">?</a> <a href="#">↕</a>	I/O load <a href="#">?</a> <a href="#">↕</a>	Read rate <a href="#">?</a> <a href="#">↕</a>	Write rate <a href="#">?</a> <a href="#">↕</a>
croot(8:1,sda1)	N/A	0.02%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.03%	0 bytes/s	6 KB/s

## Volumes

Mount point <a href="#">?</a> <a href="#">↕</a>	Device <a href="#">?</a> <a href="#">↕</a>	Status <a href="#">?</a> <a href="#">↕</a>	Size <a href="#">?</a> <a href="#">↕</a>	Available <a href="#">?</a> <a href="#">↕</a>	Write cache status <a href="#">?</a> <a href="#">↕</a>
/	croot	Online	21.00 GB	14.73 GB 	Unknown
/var/local	cvloc	Online	85.86 GB	84.63 GB 	Unknown

## Afficher l'onglet réseau

L'onglet réseau affiche un graphique indiquant le trafic réseau reçu et envoyé sur toutes les interfaces réseau du nœud, du site ou de la grille.

L'onglet réseau s'affiche pour tous les nœuds, chaque site et la grille entière.

Pour afficher un intervalle de temps différent, sélectionnez l'une des commandes au-dessus du graphique ou du graphique. Vous pouvez afficher les informations disponibles pour les intervalles de 1 heure, 1 jour, 1 semaine ou 1 mois. Vous pouvez également définir un intervalle personnalisé, qui vous permet de spécifier des plages de date et d'heure.

Pour les nœuds, le tableau interfaces réseau fournit des informations sur les ports réseau physiques de chaque nœud. Le tableau des communications réseau fournit des détails sur les opérations de réception et de transmission de chaque nœud et sur tout compteur d'erreurs signalé par le pilote.

# DC1-S2 (Storage Node)

Overview

Hardware

Network

Storage

Objects

ILM

Tasks

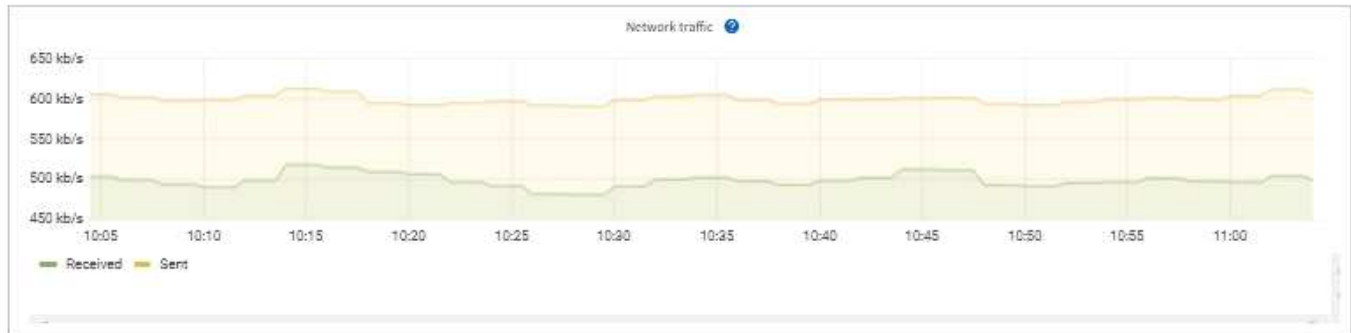
1 hour

1 day

1 week

1 month

Custom



## Network interfaces

Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status
eth0	00:50:56:A7:E8:1D	10 Gigabit	Full	Off	Up

## Network communication

### Receive

Interface	Data	Packets	Errors	Dropped	Frame overruns	Frames
eth0	3.04 GB	20,403,428	0	24,899	0	0

### Transmit

Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	3.65 GB	19,061,947	0	0	0	0

## Informations associées

["Contrôle des connexions réseau et des performances"](#)

## Afficher l'onglet stockage

L'onglet stockage récapitule la disponibilité du stockage et d'autres mesures de stockage.

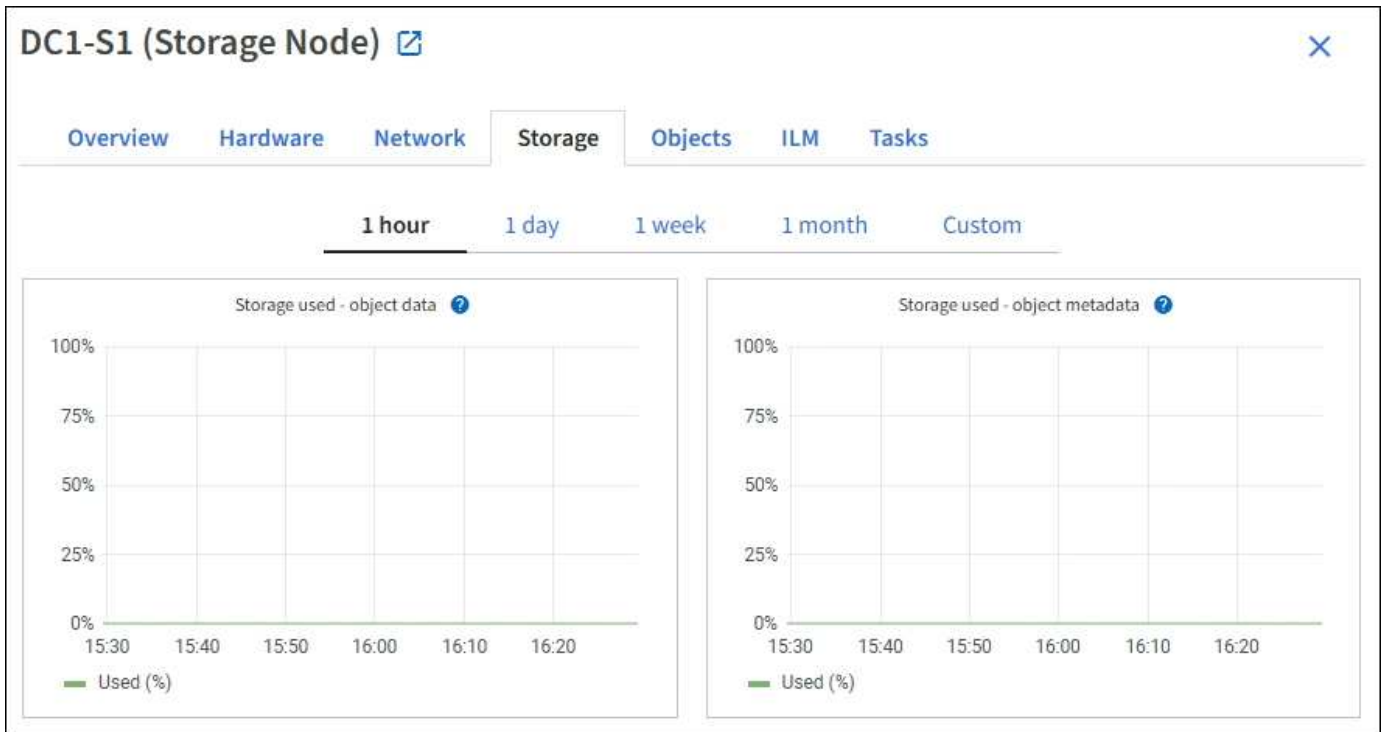
L'onglet stockage s'affiche pour tous les nœuds, chaque site et la grille complète.

## Graphiques utilisés pour le stockage

Pour les nœuds de stockage, chaque site et la grille dans son intégralité, l'onglet stockage contient des graphiques indiquant la quantité de stockage utilisée par les données d'objet et les métadonnées d'objet au fil du temps.



Lorsqu'un nœud n'est pas connecté à la grille, comme lors de la mise à niveau ou lorsqu'il est déconnecté, certains metrics peuvent être indisponibles ou exclus des totaux site et grid. Après qu'un nœud se reconnecte à la grille, attendez plusieurs minutes que les valeurs se stabilisent.



### Tables de stockage des périphériques de disque, des volumes et des objets

Pour tous les nœuds, l'onglet stockage contient des détails sur les unités de disque et les volumes du nœud. Pour les nœuds de stockage, le tableau magasins d'objets fournit des informations sur chaque volume de stockage.

## Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.67%	0 bytes/s	50 KB/s
sdc(8:16,sdb)	N/A	0.03%	0 bytes/s	4 KB/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s

## Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.75 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.05 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled

## Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	124.60 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

### Informations associées

["Surveiller la capacité de stockage"](#)

### Afficher l'onglet objets

L'onglet objets fournit des informations sur ["Taux d'ingestion et de récupération S3"](#).

L'onglet objets s'affiche pour chaque nœud de stockage, chaque site et la grille entière. Pour les nœuds de stockage, l'onglet objets fournit également le nombre d'objets et des informations sur les requêtes de métadonnées et la vérification en arrière-plan.

- Overview
- Hardware
- Network
- Storage
- Objects
- ILM
- Tasks

- 1 hour
- 1 day
- 1 week
- 1 month
- Custom



### Object counts

Total objects: <a href="#">?</a>	1,295	
Lost objects: <a href="#">?</a>	0	
S3 buckets and Swift containers: <a href="#">?</a>	161	

### Metadata store queries

Average latency: <a href="#">?</a>	10.00 milliseconds	
Queries - successful: <a href="#">?</a>	14,587	
Queries - failed (timed out): <a href="#">?</a>	0	
Queries - failed (consistency level unmet): <a href="#">?</a>	0	

### Verification

Status: <a href="#">?</a>	No errors	
Percent complete: <a href="#">?</a>	47.14%	
Average stat time: <a href="#">?</a>	0.00 microseconds	
Objects verified: <a href="#">?</a>	0	
Object verification rate: <a href="#">?</a>	0.00 objects / second	
Data verified: <a href="#">?</a>	0 bytes	
Data verification rate: <a href="#">?</a>	0.00 bytes / second	
Missing objects: <a href="#">?</a>	0	
Corrupt objects: <a href="#">?</a>	0	
Corrupt objects unidentified: <a href="#">?</a>	0	
Quarantined objects: <a href="#">?</a>	0	



## Afficher l'onglet ILM

L'onglet ILM fournit des informations sur les opérations de gestion du cycle de vie de l'information (ILM).

L'onglet ILM s'affiche pour chaque nœud de stockage, chaque site et la grille dans son ensemble. L'onglet ILM affiche un graphique de la file d'attente ILM sur la durée. Pour la grille, cet onglet indique également le temps estimé de l'analyse ILM complète de tous les objets.

Pour les nœuds de stockage, l'onglet ILM fournit des informations détaillées sur l'évaluation et la vérification en arrière-plan des objets avec code d'effacement.

### DC2-S1 (Storage Node) [🔗](#)

[Overview](#) [Hardware](#) [Network](#) [Storage](#) [Objects](#) **ILM** [Tasks](#)

#### Evaluation

Awaiting - all: <a href="#">?</a>	0 objects	
Awaiting - client: <a href="#">?</a>	0 objects	
Evaluation rate: <a href="#">?</a>	0.00 objects / second	
Scan rate: <a href="#">?</a>	0.00 objects / second	

#### Erasure coding verification

Status: <a href="#">?</a>	Idle	
Next scheduled: <a href="#">?</a>	2021-09-09 17:36:44 MDT	
Fragments verified: <a href="#">?</a>	0	
Data verified: <a href="#">?</a>	0 bytes	
Corrupt copies: <a href="#">?</a>	0	
Corrupt fragments: <a href="#">?</a>	0	
Missing fragments: <a href="#">?</a>	0	

### Informations associées

- ["Contrôle la gestion du cycle de vie des informations"](#)
- ["Administrer StorageGRID"](#)

## Utilisez l'onglet tâches

L'onglet tâches s'affiche pour tous les nœuds. Vous pouvez utiliser cet onglet pour renommer ou redémarrer un nœud ou pour mettre un nœud d'appliance en mode maintenance.

Pour connaître l'ensemble des exigences et des instructions relatives à chaque option de cet onglet, reportez-vous aux sections suivantes :

- ["Renommez la grille, les sites et les nœuds"](#)
- ["Redémarrez le nœud de la grille"](#)
- ["Mettez l'appareil en mode maintenance"](#)

## Afficher l'onglet équilibreur de charge

L'onglet Load Balancer contient des graphiques de performance et de diagnostic relatifs au fonctionnement du service Load Balancer.

L'onglet Load Balancer s'affiche pour les nœuds d'administration et les nœuds de passerelle, chaque site et la grille dans son ensemble. Pour chaque site, l'onglet Load Balancer fournit un récapitulatif global des statistiques pour tous les nœuds de ce site. Pour toute la grille, l'onglet Load Balancer fournit un récapitulatif global des statistiques pour tous les sites.

Si aucune E/S n'est exécutée via le service Load Balancer ou si aucun équilibreur de charge n'est configuré, les graphiques affichent « aucune donnée ».



### Trafic des demandes

Ce graphique fournit une moyenne mobile de 3 minutes du débit des données transmises entre les terminaux de l'équilibreur de charge et les clients effectuant les demandes, en bits par seconde.



Cette valeur est mise à jour à la fin de chaque demande. Par conséquent, cette valeur peut différer du débit en temps réel à des taux de demande faibles ou pour des demandes très longues. Vous pouvez consulter l'onglet réseau pour obtenir une vue plus réaliste du comportement actuel du réseau.

### Taux de demande entrante

Ce graphique fournit une moyenne mobile de 3 minutes du nombre de nouvelles demandes par seconde, ventilées par type de demande (OBTENIR, PLACER, TÊTE et SUPPRIMER). Cette valeur est mise à jour lorsque les en-têtes d'une nouvelle demande ont été validés.

### Durée moyenne de la demande (non-erreur)

Ce graphique fournit une moyenne mobile de 3 minutes des durées de requête, ventilées par type de demande (OBTENIR, PLACER, TÊTE et SUPPRIMER). Chaque durée de la demande commence lorsqu'un en-tête de requête est analysé par le service Load Balancer et se termine lorsque le corps de réponse complet

est renvoyé au client.

#### **Taux de réponse à l'erreur**

Ce graphique fournit une moyenne mobile de 3 minutes du nombre de réponses d'erreur renvoyées aux clients par seconde, ventilées par le code de réponse d'erreur.

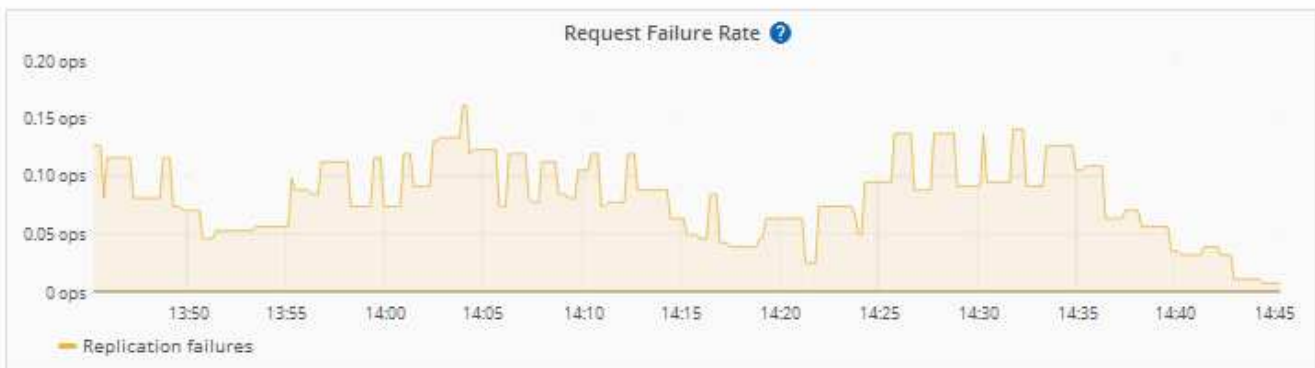
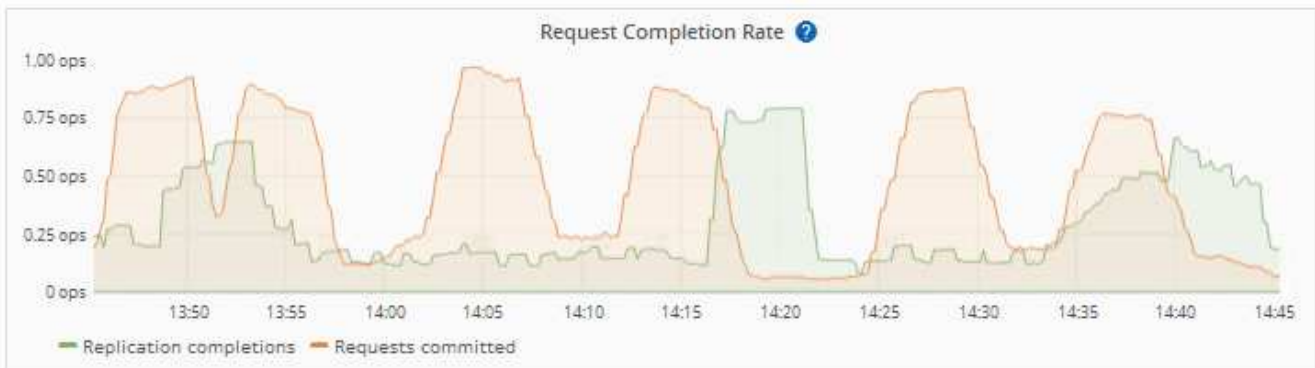
#### **Informations associées**

- ["Surveiller les opérations d'équilibrage de charge"](#)
- ["Administrer StorageGRID"](#)

#### **Afficher l'onglet Platform Services**

L'onglet Services de plateforme fournit des informations sur les opérations de service de la plateforme S3 sur un site.

L'onglet Platform Services s'affiche pour chaque site. Cet onglet fournit des informations sur les services de la plateforme S3, comme la réplication CloudMirror et le service d'intégration de la recherche. Les graphiques de cet onglet affichent des mesures telles que le nombre de requêtes en attente, le taux d'achèvement de la requête et le taux d'échec de la requête.



Pour plus d'informations sur les services de plateforme S3, notamment des détails de dépannage, consultez le ["Instructions d'administration de StorageGRID"](#).

### Affichez l'onglet gérer les lecteurs

L'onglet gérer les disques vous permet d'accéder aux détails et d'effectuer des tâches de dépannage et de maintenance sur les disques des appliances qui prennent en charge cette fonctionnalité.

L'onglet gérer les lecteurs vous permet d'effectuer les opérations suivantes :

- Afficher la disposition des disques de stockage des données du système
- Affichez un tableau répertoriant l'emplacement, le type, l'état, la version du micrologiciel et le numéro de série de chaque lecteur
- Exécutez les fonctions de dépannage et de maintenance sur chaque disque

Pour accéder à l'onglet gérer les lecteurs, vous devez disposer du ["Administrateur de l'appliance de stockage ou autorisation d'accès racine"](#).

Pour plus d'informations sur l'utilisation de l'onglet gérer les lecteurs, reportez-vous à la section ["Utilisez l'onglet gérer les lecteurs"](#).

### Afficher l'onglet SANtricity System Manager (E-Series uniquement)

L'onglet SANtricity System Manager vous permet d'accéder à SANtricity System Manager sans devoir configurer ni connecter le port de gestion de l'appliance de stockage. Cet onglet permet de consulter les informations de diagnostic du matériel et les informations environnementales, ainsi que les problèmes liés aux lecteurs.



L'accès à SANtricity System Manager à partir de Grid Manager se limite généralement à la surveillance du matériel de l'appliance et à la configuration des baies E-Series AutoSupport. De nombreuses fonctionnalités et opérations dans SANtricity System Manager, telles que la mise à niveau du firmware, ne s'appliquent pas à la surveillance de l'appliance StorageGRID. Pour éviter tout problème, suivez toujours les instructions de maintenance du matériel de votre appareil. Pour mettre à niveau le micrologiciel SANtricity, reportez-vous au ["Procédures de configuration de la maintenance"](#) pour votre appliance de stockage.



L'onglet SANtricity System Manager s'affiche uniquement pour les nœuds d'appliance de stockage qui utilisent le matériel E-Series.

Grâce à SANtricity System Manager, vous pouvez effectuer les opérations suivantes :

- Affichez des données sur les performances, telles que les performances au niveau des baies de stockage, la latence des E/S, l'utilisation du CPU du contrôleur de stockage et le débit.
- Vérifiez l'état des composants matériels.
- Exécutez des fonctions de support, notamment l'affichage des données de diagnostic et la configuration du système E-Series AutoSupport.



Pour utiliser SANtricity System Manager afin de configurer un proxy pour E-Series AutoSupport, reportez-vous à ["Envoyez des packages AutoSupport E-Series via StorageGRID"](#) la section .

Pour accéder au Gestionnaire système SANtricity via le Gestionnaire de grille, vous devez disposer du ["Administrateur de l'appliance de stockage ou autorisation d'accès racine"](#).



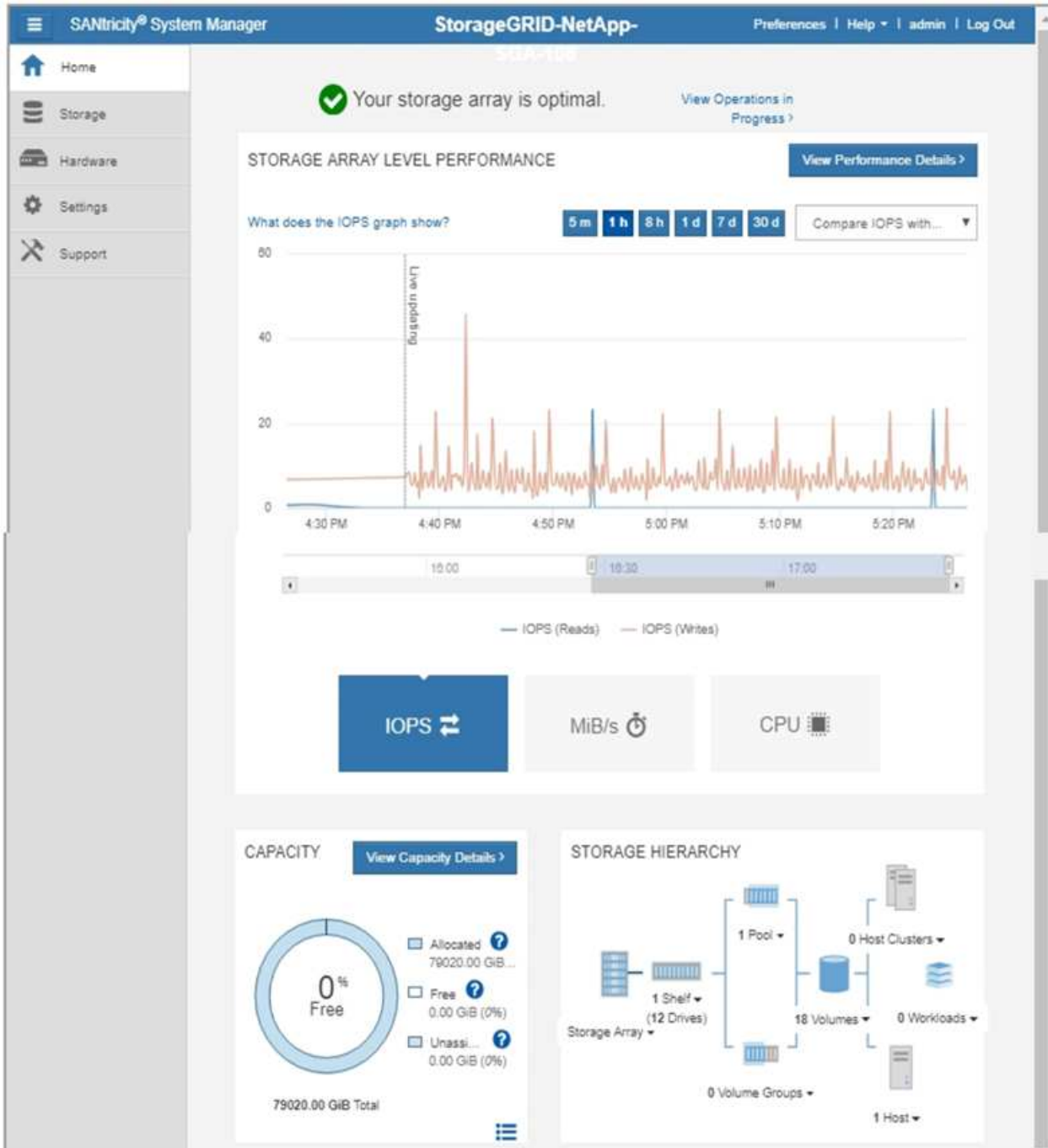
Vous devez disposer d'un firmware SANtricity 8.70 ou supérieur pour accéder à SANtricity System Manager à l'aide de Grid Manager.


L'onglet affiche la page d'accueil de SANtricity System Manager.

Use SANtricity System Manager to monitor and manage the hardware components in this storage appliance. From SANtricity System Manager, you can review hardware diagnostic and environmental information as well as issues related to the drives.

**Note:** Many features and operations within SANtricity Storage Manager do not apply to your StorageGRID appliance. To avoid issues, always follow the hardware installation and maintenance instructions for your appliance model.

Open SANtricity System Manager [in a new browser tab](#).



 Pour plus de facilité, vous pouvez utiliser le lien SANtricity System Manager pour ouvrir SANtricity System Manager dans une nouvelle fenêtre de navigateur.

Pour afficher des informations détaillées sur les performances au niveau de la baie de stockage et l'utilisation

de la capacité, positionnez le curseur sur chaque graphique.

Pour plus d'informations sur l'affichage des informations accessibles depuis l'onglet Gestionnaire système SANtricity, reportez-vous à la section "[Documentation sur les systèmes NetApp E-Series et SANtricity](#)".

## Informations à surveiller régulièrement

### Quoi et quand surveiller

Même si le système StorageGRID peut continuer à fonctionner lorsque des erreurs se produisent ou que des parties de la grille sont indisponibles, vous devez surveiller et résoudre les problèmes potentiels avant qu'ils n'affectent l'efficacité ou la disponibilité de la grille.

### Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur web pris en charge](#)".
- Vous avez "[autorisations d'accès spécifiques](#)".

### A propos des tâches de surveillance

Un système occupé génère de grandes quantités d'informations. La liste suivante fournit des conseils sur les informations les plus importantes à surveiller en permanence.

Quoi surveiller	Fréquence
" <a href="#">État de santé du système</a> "	Tous les jours
Taux de " <a href="#">Capacité des objets et des métadonnées du nœud de stockage</a> " consommation	Hebdomadaire
" <a href="#">Opérations de gestion du cycle de vie des informations</a> "	Hebdomadaire
" <a href="#">Ressources réseau et système</a> "	Hebdomadaire
" <a href="#">Activité des locataires</a> "	Hebdomadaire
" <a href="#">Opérations client S3</a> "	Hebdomadaire
" <a href="#">Opérations d'équilibrage de la charge</a> "	Après la configuration initiale et après toute modification de la configuration
" <a href="#">Connexions de fédération de grille</a> "	Hebdomadaire

### Contrôle de l'état des systèmes

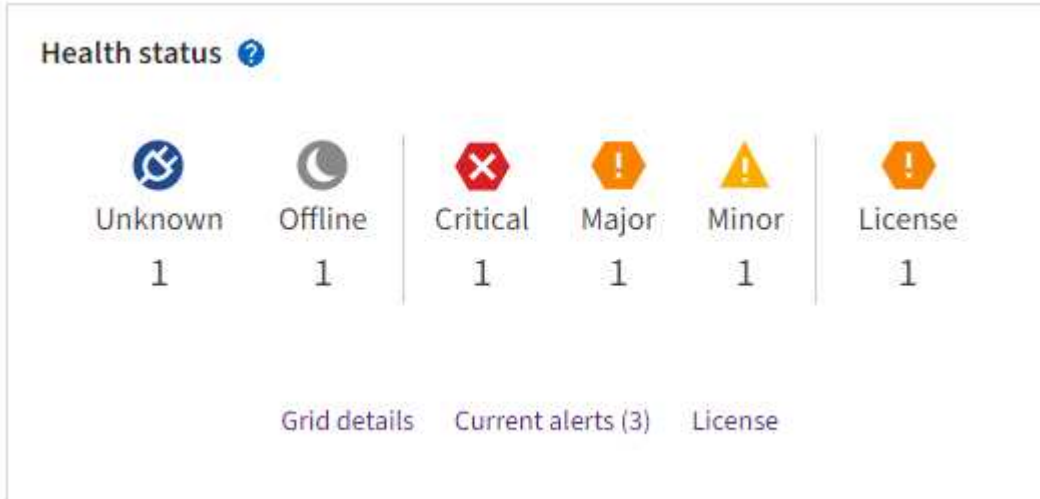
Surveillez quotidiennement l'état global de votre système StorageGRID.

### Description de la tâche



Le système StorageGRID peut continuer à fonctionner lorsque certaines parties de la grille ne sont pas disponibles. Les problèmes potentiels signalés par des alertes ne sont pas nécessairement des problèmes liés aux opérations du système. Examinez les problèmes résumés sur la carte d'état de santé du tableau de bord Grid Manager.

Pour être averti des alertes dès qu'elles sont déclenchées, vous pouvez ["configurez les notifications par e-mail pour les alertes"](#) ou ["Configurer les interruptions SNMP"](#).






Lorsque des problèmes existent, des liens s'affichent pour vous permettre d'afficher des détails supplémentaires :

Lien	Apparaît lorsque...
Détails de la grille	Tous les nœuds sont déconnectés (état de connexion inconnu ou arrêté administrativement).
Alertes actuelles (critique, majeure, mineure)	Les alertes sont <a href="#">actuellement actif</a> .
Alertes récemment résolues	Alertes déclenchées au cours de <a href="#">sont maintenant résolus</a> la semaine dernière .
Licence	Il y a un problème avec la licence logicielle de ce système StorageGRID. Vous pouvez <a href="#">"mettez à jour les informations de licence si nécessaire"</a> .

### Surveiller les États de connexion du nœud

Si un ou plusieurs nœuds sont déconnectés de la grille, les opérations StorageGRID stratégiques peuvent être affectées. Surveillez les États de connexion des nœuds et traitez tous les problèmes rapidement.

Icône	Description	Action requise
	<p><b>Non connecté - Inconnu</b></p> <p>Pour une raison inconnue, un nœud est déconnecté ou les services du nœud sont arrêtés de manière inattendue. Par exemple, un service du nœud peut être arrêté, ou le nœud a perdu sa connexion réseau en raison d'une panne de courant ou d'une panne imprévue.</p> <p>L'alerte <b>Impossible de communiquer avec le nœud</b> peut également être déclenchée. D'autres alertes peuvent également être actives.</p>	<p>Nécessite une attention immédiate. <a href="#">Sélectionnez chaque alerte</a> et suivre les actions recommandées.</p> <p>Par exemple, vous devrez peut-être redémarrer un service qui a arrêté ou redémarré l'hôte du nœud.</p> <p><b>Remarque</b> : un nœud peut apparaître comme inconnu pendant les opérations d'arrêt gérées. Dans ces cas, vous pouvez ignorer l'état Inconnu.</p>
	<p><b>Non connecté - Arrêt administratif</b></p> <p>Pour une raison prévue, le nœud n'est pas connecté au grid.</p> <p>Par exemple, le nœud ou les services du nœud ont été normalement arrêtés, le nœud est en cours de redémarrage ou le logiciel est mis à niveau. Une ou plusieurs alertes peuvent également être actives.</p> <p>En fonction du problème sous-jacent, ces nœuds sont souvent remis en ligne sans intervention.</p>	<p>Déterminez si des alertes affectent ce nœud.</p> <p>Si une ou plusieurs alertes sont actives <a href="#">sélectionnez chaque alerte</a> et suivez les actions recommandées.</p>
	<ul style="list-style-type: none"> <li>• Connecté*</li> </ul> <p>Le nœud est connecté à la grille.</p>	<p>Aucune action requise.</p>

#### Afficher les alertes actuelles et résolues




**Alertes actuelles** : lorsqu'une alerte est déclenchée, une icône d'alerte s'affiche sur le tableau de bord. Une icône d'alerte s'affiche également pour le nœud sur la page nœuds. Si "[les notifications par e-mail d'alerte sont configurées](#)", une notification par e-mail sera également envoyée, sauf si l'alerte a été neutralisée.

**Alertes résolues** : vous pouvez rechercher et afficher un historique des alertes qui ont été résolues.

Vous avez éventuellement regardé la vidéo : "[Vidéo : présentation des alertes](#)"



Le tableau suivant décrit les informations affichées dans Grid Manager pour les alertes en cours et résolues.

En-tête de colonne	Description
Nom ou titre	Le nom de l'alerte et sa description.
Gravité	<p>Gravité de l'alerte. Pour les alertes actuelles, si plusieurs alertes sont regroupées, la ligne de titre indique le nombre d'instances de cette alerte qui se produisent à chaque gravité.</p> <p> <b>Critique</b> : il existe une condition anormale qui a arrêté les opérations normales d'un noeud ou d'un service StorageGRID. Vous devez immédiatement résoudre le problème sous-jacent. Une interruption du service et une perte de données peuvent se produire si le problème n'est pas résolu.</p> <p> <b>Majeur</b> : il existe une condition anormale qui affecte les opérations en cours ou qui approche du seuil pour une alerte critique. Vous devez examiner les alertes majeures et résoudre tous les problèmes sous-jacents pour vérifier que leur condition anormale n'arrête pas le fonctionnement normal d'un nœud ou d'un service StorageGRID.</p> <p> <b>Mineur</b> : le système fonctionne normalement, mais il existe une condition anormale qui pourrait affecter la capacité de fonctionnement du système s'il continue. Vous devez surveiller et résoudre les alertes mineures qui ne sont pas claires par elles-mêmes pour vous assurer qu'elles n'entraînent pas de problème plus grave.</p>
Temps déclenché	<p><b>Alertes actuelles</b> : date et heure auxquelles l'alerte a été déclenchée à l'heure locale et en UTC. Si plusieurs alertes sont regroupées, la ligne de titre affiche les heures de l'instance la plus récente de l'alerte (<i>le plus récent</i>) et de l'instance la plus ancienne de l'alerte (<i>le plus ancien</i>).</p> <p><b>Alertes résolues</b> : il y a combien de temps l'alerte a été déclenchée.</p>
Site/nœud	Nom du site et du nœud où l'alerte a eu lieu ou s'est produite.

En-tête de colonne	Description
État	Indique si l’alerte est active, neutralisée ou résolue. Si plusieurs alertes sont regroupées et que <b>toutes les alertes</b> sont sélectionnées dans la liste déroulante, la ligne de titre indique le nombre d’instances de cette alerte actives et le nombre d’instances désactivées.
Temps résolu (alertes résolues uniquement)	Il y a combien de temps l’alerte a été résolue.
Valeurs actuelles ou <i>valeurs de données</i>	Valeur de la mesure à l’origine du déclenchement de l’alerte. Pour certaines alertes, des valeurs supplémentaires sont affichées pour vous aider à comprendre et à examiner l’alerte. Par exemple, les valeurs affichées pour une alerte <b>stockage de données d’objet bas</b> comprennent le pourcentage d’espace disque utilisé, la quantité totale d’espace disque et la quantité d’espace disque utilisée.  <b>Remarque</b> : si plusieurs alertes actuelles sont regroupées, les valeurs actuelles ne sont pas affichées dans la ligne de titre.
Valeurs déclenchées (alertes résolues uniquement)	Valeur de la mesure à l’origine du déclenchement de l’alerte. Pour certaines alertes, des valeurs supplémentaires sont affichées pour vous aider à comprendre et à examiner l’alerte. Par exemple, les valeurs affichées pour une alerte <b>stockage de données d’objet bas</b> comprennent le pourcentage d’espace disque utilisé, la quantité totale d’espace disque et la quantité d’espace disque utilisée.




## Étapes

1. Sélectionnez le lien **alertes actuelles** ou **alertes résolues** pour afficher la liste des alertes de ces catégories. Vous pouvez également afficher les détails d’une alerte en sélectionnant **nœuds > nœud > vue d’ensemble**, puis en sélectionnant l’alerte dans le tableau alertes.

Par défaut, les alertes actuelles s’affichent comme suit :

- Les alertes déclenchées les plus récemment sont affichées en premier.
- Plusieurs alertes du même type sont affichées sous la forme d’un groupe.
- Les alertes qui ont été neutralisées ne sont pas affichées.
- Pour une alerte spécifique sur un nœud spécifique, si les seuils sont atteints pour plus d’un niveau de gravité, seule l’alerte la plus grave est affichée. C’est-à-dire, si les seuils d’alerte sont atteints pour les niveaux de gravité mineur, majeur et critique, seule l’alerte critique s’affiche.

La page d’alertes en cours est actualisée toutes les deux minutes.

2. Pour développer des groupes d’alertes, sélectionnez la touche d’avertissement vers le bas . Pour réduire les alertes individuelles d’un groupe, sélectionnez la touche UP caret  ou sélectionnez le nom du groupe.
3. Pour afficher des alertes individuelles au lieu de groupes d’alertes, décochez la case **alertes de groupe**.
4. Pour trier les alertes ou les groupes d’alertes actuels, sélectionnez les flèches haut/bas  dans chaque en-tête de colonne.
  - Lorsque **alertes de groupe** est sélectionné, les groupes d’alertes et les alertes individuelles de chaque groupe sont triés. Par exemple, vous pouvez trier les alertes d’un groupe par **heure déclenchée** pour

trouver l'instance la plus récente d'une alerte spécifique.

- Lorsque **alertes de groupe** est effacé, la liste complète des alertes est triée. Par exemple, vous pouvez trier toutes les alertes par **nœud/site** pour voir toutes les alertes affectant un nœud spécifique.
5. Pour filtrer les alertes actuelles par état (**toutes les alertes**, **Active** ou **Silence**, utilisez le menu déroulant situé en haut du tableau.

Voir "[Notifications d'alerte de silence](#)".

6. Pour trier les alertes résolues :
- Sélectionnez une période dans le menu déroulant **lorsqu'elle est déclenchée**.
  - Sélectionnez une ou plusieurs gravité dans le menu déroulant **gravité**.
  - Sélectionnez une ou plusieurs règles d'alerte par défaut ou personnalisées dans le menu déroulant **règle d'alerte** pour filtrer les alertes résolues associées à une règle d'alerte spécifique.
  - Sélectionnez un ou plusieurs nœuds dans le menu déroulant **Node** pour filtrer les alertes résolues liées à un nœud spécifique.
7. Pour afficher les détails d'une alerte spécifique, sélectionnez l'alerte. Une boîte de dialogue fournit des détails et des actions recommandées pour l'alerte que vous avez sélectionnée.
8. (Facultatif) pour une alerte spécifique, sélectionnez silence cette alerte pour désactiver la règle d'alerte qui a déclenché cette alerte.

Vous devez avoir le "[Gérer les alertes ou l'autorisation d'accès racine](#)" pour désactiver une règle d'alerte.



Soyez prudent lorsque vous décidez de désactiver une règle d'alerte. Si une règle d'alerte est mise en mode silencieux, il est possible que vous ne détectiez pas un problème sous-jacent tant qu'elle n'empêche pas l'exécution d'une opération critique.

9. Pour afficher les conditions actuelles de la règle d'alerte :
- a. Dans les détails de l'alerte, sélectionnez **Afficher les conditions**.
- Une fenêtre contextuelle s'affiche, répertoriant l'expression Prometheus pour chaque gravité définie.
- b. Pour fermer la fenêtre contextuelle, cliquez n'importe où en dehors de la fenêtre contextuelle.
10. Vous pouvez également sélectionner **Modifier la règle** pour modifier la règle d'alerte qui a déclenché cette alerte.

Vous devez avoir le "[Gérer les alertes ou l'autorisation d'accès racine](#)" pour modifier une règle d'alerte.



Soyez prudent lorsque vous décidez de modifier une règle d'alerte. Si vous modifiez les valeurs de déclenchement, il est possible que vous ne détectiez pas de problème sous-jacent tant qu'elle n'empêche pas l'exécution d'une opération critique.

11. Pour fermer les détails de l'alerte, sélectionnez **Fermer**.

## Surveiller la capacité de stockage

Contrôlez l'espace total disponible pour vérifier que le système StorageGRID ne manque pas d'espace de stockage pour les objets ou les métadonnées d'objet.

StorageGRID stocke séparément les données d'objet et les métadonnées d'objet. Il réserve un espace

spécifique pour une base de données Cassandra distribuée qui contient les métadonnées d'objet. Surveiller la quantité totale d'espace consommée pour les objets et les métadonnées d'objet, ainsi que les tendances en matière de quantité d'espace consommée pour chaque. Vous pourrez ainsi planifier l'ajout de nœuds et éviter toute panne de service.

Vous pouvez "[affichez des informations sur la capacité de stockage](#)" couvrir l'ensemble de la grille, pour chaque site et pour chaque nœud de stockage du système StorageGRID.

### Surveiller la capacité de stockage pour l'ensemble de la grille

Surveillez la capacité de stockage globale de votre grid afin de vous assurer qu'il reste un espace libre adéquat pour les données d'objet et les métadonnées d'objet. Pour mieux comprendre les variations de capacité de stockage dans le temps, vous pouvez planifier l'ajout de nœuds de stockage ou de volumes avant de consommer la capacité de stockage utilisable de la grille.

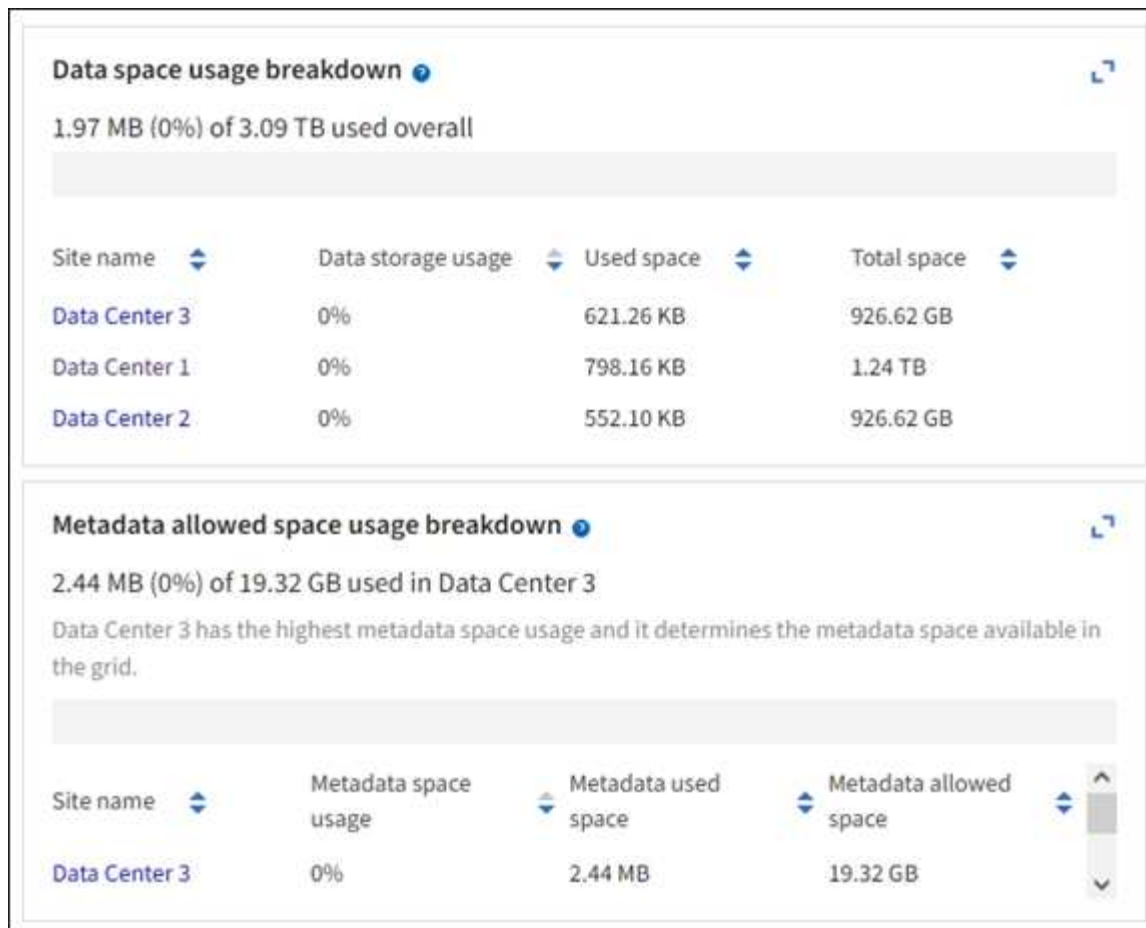
Le tableau de bord de Grid Manager vous permet d'évaluer rapidement la quantité de stockage disponible pour l'ensemble du grid et pour chaque data Center. La page nœuds fournit des valeurs plus détaillées pour les données d'objet et les métadonnées d'objet.

### Étapes

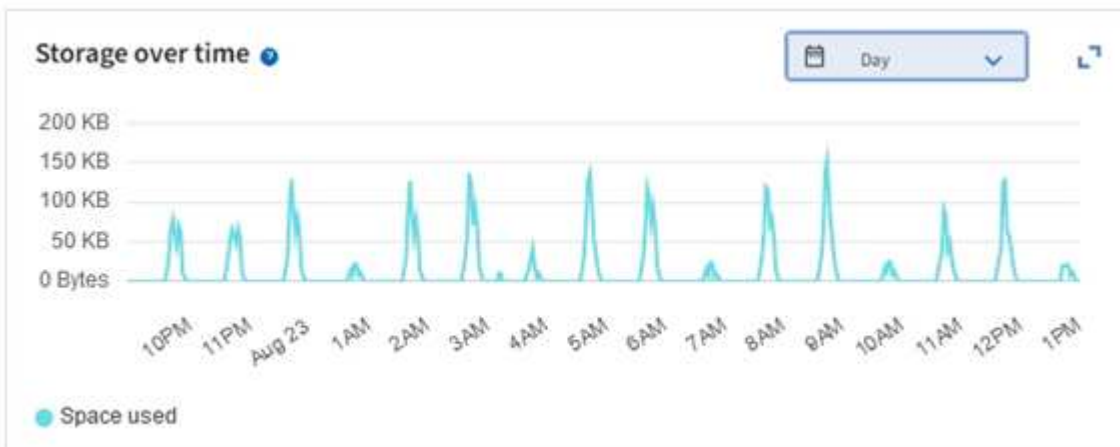
1. Évaluez la quantité de stockage disponible pour l'ensemble du grid et pour chaque data Center.
  - a. Sélectionnez **Tableau de bord > vue d'ensemble**.
  - b. Notez les valeurs de la répartition de l'utilisation de l'espace de données et les cartes de répartition de l'utilisation de l'espace autorisé dans les métadonnées. Chaque carte indique un pourcentage d'utilisation du stockage, la capacité de l'espace utilisé et l'espace total disponible ou autorisé par site.



Le résumé n'inclut pas les supports d'archivage.

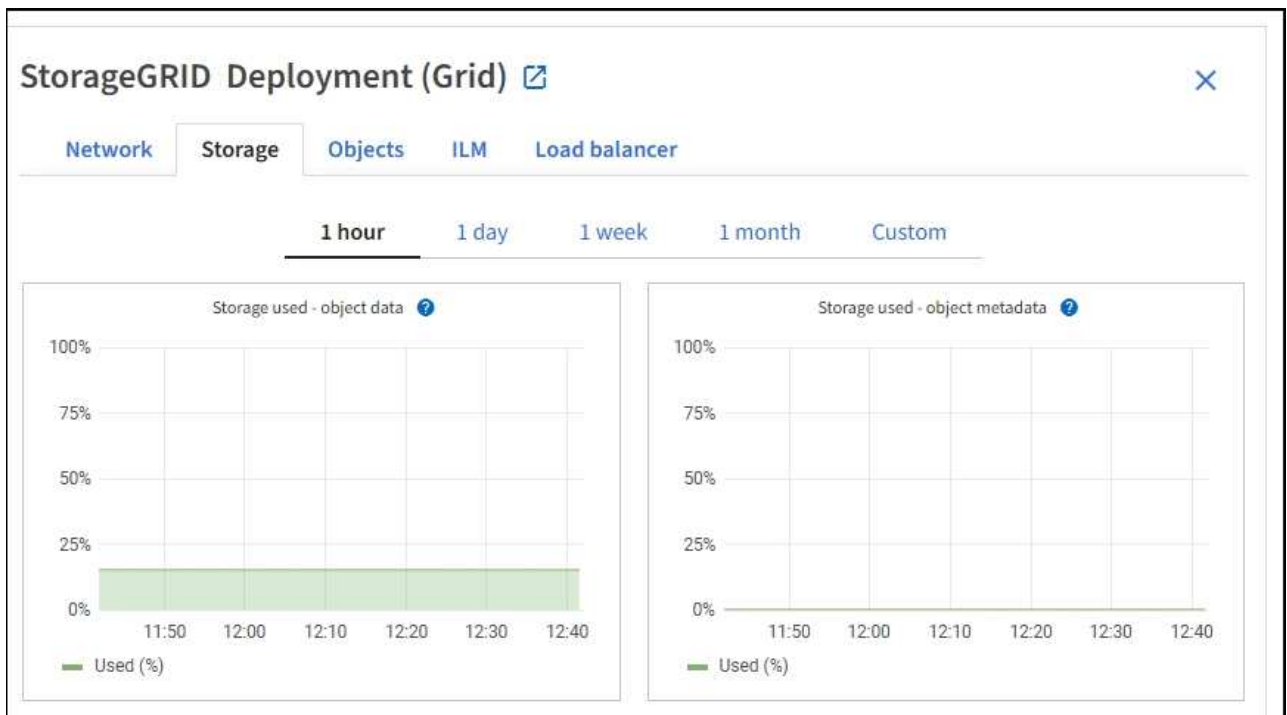


a. Notez le tableau sur la carte de stockage dans le temps. Utilisez la liste déroulante période pour vous aider à déterminer la rapidité de consommation du stockage.



2. Pour plus d'informations sur la quantité de stockage utilisée et la quantité de stockage restant disponible dans la grille pour les données d'objet et les métadonnées d'objet, consultez la page nœuds.

- a. Sélectionnez **NOEUDS**.
- b. Sélectionnez **GRID > stockage**.



- c. Placez votre curseur sur les graphiques **stockage utilisé - données d'objet** et **stockage utilisé - métadonnées d'objet** pour connaître la quantité de stockage d'objet et de métadonnées d'objet disponible pour l'ensemble de la grille, ainsi que la quantité utilisée au fil du temps.



Les valeurs totales d'un site ou de la grille n'incluent pas les nœuds qui n'ont pas signalé de mesures depuis au moins cinq minutes, comme les nœuds hors ligne.

3. Planifiez une extension permettant d'ajouter des nœuds de stockage ou des volumes de stockage avant l'utilisation de la capacité de stockage utilisable de la grille.

Lors de la planification d'une extension, réfléchissez au temps nécessaire pour approvisionner et installer du stockage supplémentaire.



Si votre règle ILM utilise le code d'effacement, vous pouvez préférer une extension lorsque les nœuds de stockage existants sont remplis à environ 70 % pour réduire le nombre de nœuds à ajouter.

Pour plus d'informations sur la planification d'une extension de stockage, reportez-vous au "[Instructions d'extension de StorageGRID](#)".

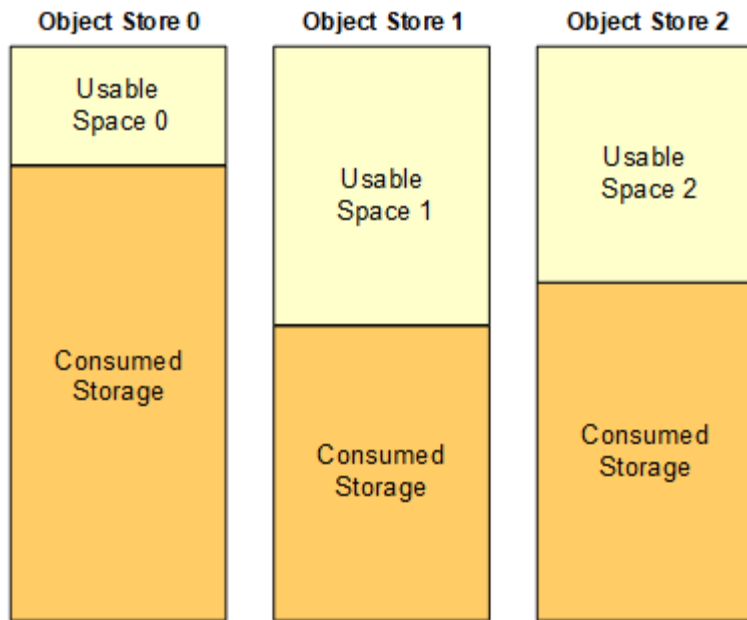
### Surveillez la capacité de stockage de chaque nœud de stockage

Surveillez l'espace total utilisable pour chaque nœud de stockage pour vous assurer que le nœud dispose de suffisamment d'espace pour les nouvelles données d'objet.

### Description de la tâche

L'espace utilisable correspond à la quantité d'espace de stockage disponible pour stocker des objets. L'espace total utilisable d'un nœud de stockage est calculé en ajoutant ensemble l'espace disponible sur tous les magasins d'objets du nœud.





**Total Usable Space = Usable Space 0 + Usable Space 1 + Usable Space 2**

### Étapes

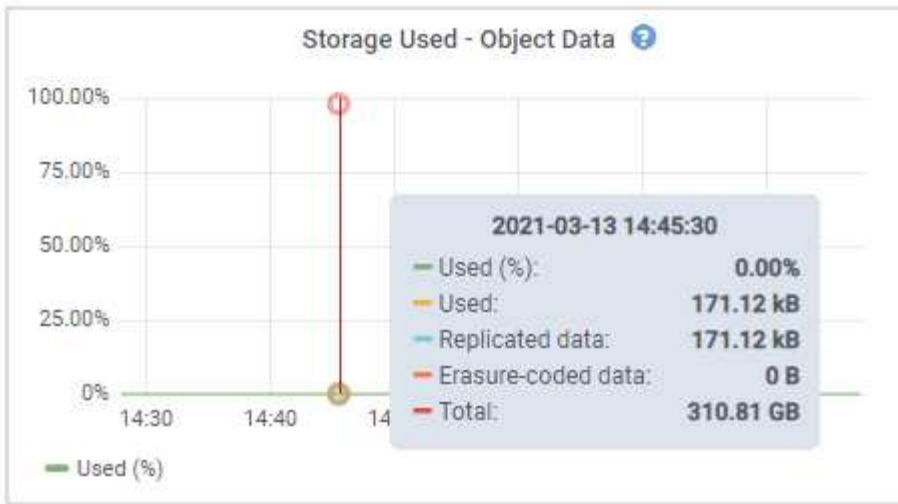
1. Sélectionnez **NODES > Storage Node > Storage**.

Les graphiques et les tableaux du nœud apparaissent.

2. Positionnez le curseur sur le graphique de données d'objet stockage utilisé -.


Les valeurs suivantes sont affichées :

- **Utilisé (%)** : pourcentage de l'espace utilisable total qui a été utilisé pour les données d'objet.
- **Used** : quantité de l'espace utilisable total qui a été utilisé pour les données d'objet.
- **Données répliquées** : estimation de la quantité de données d'objet répliqué sur ce nœud, site ou grille.
- **Données avec code d'effacement** : estimation de la quantité de données d'objet avec code d'effacement sur ce nœud, ce site ou ce grid.
- **Total** : la quantité totale d'espace utilisable sur ce nœud, site ou grille. La valeur utilisée est la `storagegrid_storage_utilization_data_bytes` mesure.



3. Passez en revue les valeurs disponibles dans les tableaux volumes et magasins d'objets, sous les graphiques.



Pour afficher les graphiques de ces valeurs, cliquez sur les icônes du graphique  dans les colonnes disponibles.

Disk devices					
Name	World Wide Name	I/O load	Read rate	Write rate	
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	3 KB/s	
cvloc(8:2,sda2)	N/A	0.67%	0 bytes/s	50 KB/s	
sdc(8:16,sdb)	N/A	0.03%	0 bytes/s	4 KB/s	
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s	
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s	

Volumes					
Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.75 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.05 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled

Object stores						
ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	124.60 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

- Surveillez les valeurs dans le temps pour estimer le taux de consommation de l'espace de stockage utilisable.
- Pour préserver le fonctionnement normal du système, ajoutez des nœuds de stockage, ajoutez des volumes de stockage ou archivez les données d'objet avant de consommer l'espace utilisable.

Lors de la planification d'une extension, réfléchissez au temps nécessaire pour approvisionner et installer du stockage supplémentaire.



Si votre règle ILM utilise le code d'effacement, vous pouvez préférer une extension lorsque les nœuds de stockage existants sont remplis à environ 70 % pour réduire le nombre de nœuds à ajouter.

Pour plus d'informations sur la planification d'une extension de stockage, reportez-vous au ["Instructions"](#)

d'extension de StorageGRID".

L'"Faible stockage des données objet"alerte est déclenchée lorsque l'espace restant est insuffisant pour stocker les données d'objet sur un nœud de stockage.

### Surveillez la capacité des métadonnées d'objet pour chaque nœud de stockage

Surveillez l'utilisation des métadonnées pour chaque nœud de stockage afin de garantir qu'un espace adéquat reste disponible pour les opérations essentielles de la base de données. Vous devez ajouter de nouveaux nœuds de stockage sur chaque site avant que les métadonnées d'objet dépassent 100 % de l'espace autorisé pour les métadonnées.

### Description de la tâche

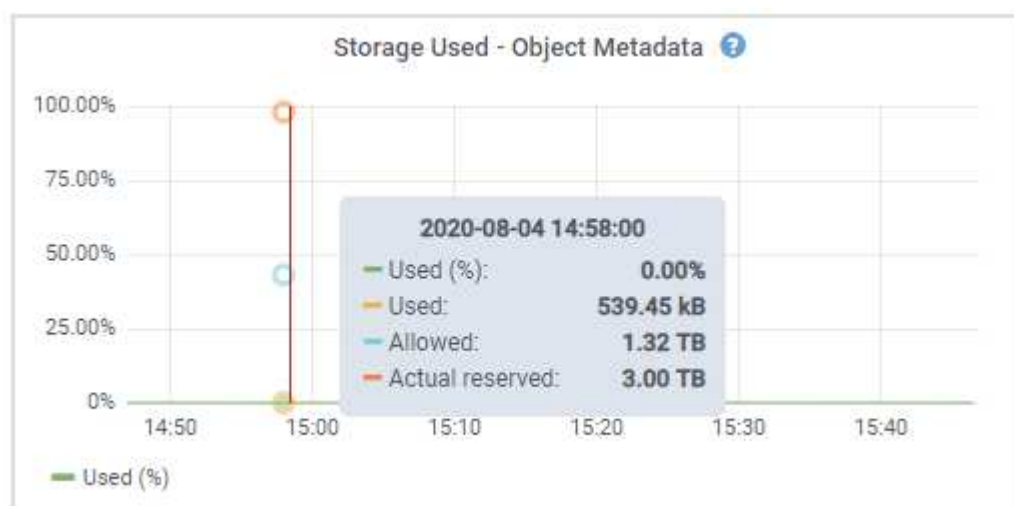
StorageGRID conserve trois copies des métadonnées d'objet sur chaque site pour assurer la redondance et protéger les métadonnées d'objet contre la perte. Les trois copies sont réparties de manière homogène sur tous les nœuds de stockage de chaque site, en utilisant l'espace réservé aux métadonnées sur le volume de stockage 0 de chaque nœud de stockage.

Dans certains cas, la capacité des métadonnées d'objet de la grille peut être utilisée plus rapidement que la capacité de stockage objet. Par exemple, si vous ingérez généralement un grand nombre d'objets de petite taille, vous devrez ajouter des nœuds de stockage pour augmenter la capacité des métadonnées, même si la capacité de stockage objet est suffisante.

L'utilisation des métadonnées peut notamment être augmentée, comme la taille et la quantité des métadonnées et du balisage, le nombre total d'éléments d'un téléchargement partitionné et la fréquence des modifications apportées aux emplacements de stockage ILM.

### Étapes

1. Sélectionnez **NODES > Storage Node > Storage**.
2. Positionnez le curseur sur le graphique de métadonnées de l'objet stockage utilisé - pour afficher les valeurs d'une heure spécifique.



### Utilisé (%)

Pourcentage de l'espace de métadonnées autorisé utilisé sur ce nœud de stockage.

Metrics Prometheus : `storagegrid_storage_utilization_metadata_bytes` et `storagegrid_storage_utilization_metadata_allowed_bytes`

## Utilisé

Les octets de l'espace de métadonnées autorisé qui ont été utilisés sur ce nœud de stockage.

Prometheus métrique : `storagegrid_storage_utilization_metadata_bytes`

## Autorisé

Espace autorisé pour les métadonnées d'objet sur ce nœud de stockage. Pour savoir comment cette valeur est déterminée pour chaque nœud de stockage, reportez-vous au ["Description complète de l'espace de métadonnées autorisé"](#).

Prometheus métrique : `storagegrid_storage_utilization_metadata_allowed_bytes`

## Réservé réelle

Espace réel réservé aux métadonnées sur ce nœud de stockage. Inclut l'espace autorisé et l'espace requis pour les opérations essentielles sur les métadonnées. Pour savoir comment cette valeur est calculée pour chaque nœud de stockage, reportez-vous au ["Description complète de l'espace réservé réel pour les métadonnées"](#).

*Prometheus métrique sera ajouté dans une prochaine version.*



Les valeurs totales d'un site ou de la grille n'incluent pas les nœuds qui n'ont pas signalé de mesures depuis au moins cinq minutes, comme les nœuds hors ligne.

3. Si la valeur **utilisée (%)** est de 70 % ou plus, développez votre système StorageGRID en ajoutant des nœuds de stockage à chaque site.



L'alerte **stockage de métadonnées faible** est déclenchée lorsque la valeur **utilisée (%)** atteint certains seuils. Les résultats indésirables peuvent se produire si les métadonnées de l'objet utilisent plus de 100 % de l'espace autorisé.

Lorsque vous ajoutez des nœuds, le système rééquilibre automatiquement les métadonnées d'objet sur tous les nœuds de stockage du site. Voir la ["Instructions d'extension d'un système StorageGRID"](#).

## Surveillez les prévisions d'utilisation de l'espace

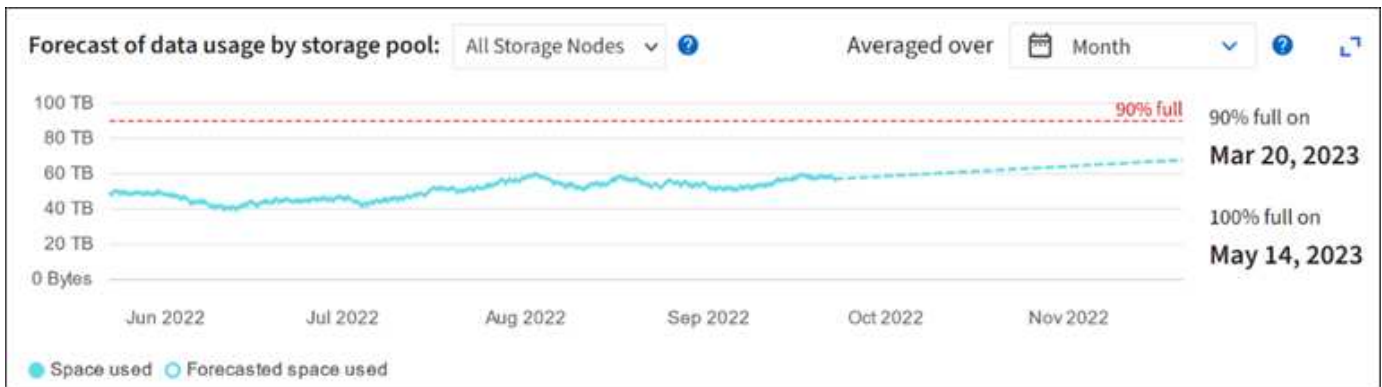
Surveillez les prévisions d'utilisation de l'espace pour les données utilisateur et les métadonnées afin d'estimer quand vous en aurez besoin ["développez une grille"](#).

Si vous remarquez que le taux de consommation change au fil du temps, sélectionnez une plage plus courte dans le menu déroulant **moyenne sur** pour refléter uniquement les modèles d'ingestion les plus récents. Si vous remarquez des motifs saisonniers, sélectionnez une plage plus longue.

Si vous disposez d'une nouvelle installation StorageGRID, autorisez l'accumulation de données et de métadonnées avant d'évaluer les prévisions d'utilisation de l'espace.

## Étapes

1. Sur le tableau de bord, sélectionnez **stockage**.
2. Affichez les cartes du tableau de bord, la prévision de l'utilisation des données par pool de stockage et la prévision de l'utilisation des métadonnées par site.
3. Utilisez ces valeurs pour déterminer quand ajouter de nouveaux nœuds de stockage pour le stockage des données et des métadonnées.



## Contrôle la gestion du cycle de vie des informations

Le système de gestion du cycle de vie des informations (ILM) assure la gestion des données de tous les objets stockés sur la grille. Vous devez contrôler les opérations ILM pour déterminer si la grille peut gérer la charge actuelle ou si des ressources supplémentaires sont nécessaires.

### Description de la tâche

Le système StorageGRID gère les objets en appliquant les règles ILM actives. Les règles ILM associées déterminent le nombre de copies effectuées, le type de copies créées, l'emplacement des copies et la durée de conservation de chaque copie.

L'ingestion d'objets et d'autres activités liées aux objets peuvent dépasser la vitesse à laquelle StorageGRID peut évaluer la gestion des règles ILM. Le système peut ainsi mettre en file d'attente des objets dont les instructions de placement des règles ILM ne peuvent pas être exécutées en temps quasi réel. Vous devez vérifier si StorageGRID est au fait des actions des clients.

### Utilisez l'onglet Tableau de bord de Grid Manager

#### Étapes

Pour contrôler les opérations ILM, utilisez l'onglet ILM du tableau de bord Grid Manager :

1. Connectez-vous au Grid Manager.
2. Dans le tableau de bord, sélectionnez l'onglet ILM et notez les valeurs sur la carte ILM queue (Objects) et la carte des taux d'évaluation ILM.

Des pics temporaires sont attendus dans la carte de la file d'attente ILM (objets) du tableau de bord. Toutefois, si la file d'attente continue d'augmenter ou de ne jamais diminuer, le grid a besoin de davantage de ressources pour fonctionner efficacement : plus de nœuds de stockage ou, si la règle ILM place des objets sur des sites distants, plus de bande passante réseau.

### Utilisez la page NŒUDS

#### Étapes

De plus, examinez les files d'attente ILM à l'aide de la page **NŒUDS** :



Les graphiques de la page **NŒUDS** seront remplacés par les cartes de tableau de bord correspondantes dans une future version de StorageGRID.

1. Sélectionnez **NOEUDS**.
2. Sélectionnez **grid name > ILM**.
3. Positionnez le curseur de votre souris sur le graphique de la file d'attente ILM pour voir la valeur des attributs suivants à un moment donné :
  - **Objets mis en file d'attente (à partir des opérations client)** : nombre total d'objets en attente d'évaluation ILM en raison des opérations client (par exemple, ingestion).
  - **Objets mis en file d'attente (de toutes les opérations)** : nombre total d'objets en attente d'évaluation ILM.
  - **Taux d'acquisition (objets/s)** : vitesse à laquelle les objets de la grille sont analysés et mis en file d'attente pour ILM.
  - **Taux d'évaluation (objets/s)** : taux actuel auquel les objets sont évalués par rapport à la politique ILM de la grille.
4. Dans la section ILM Queue, observez les attributs suivants.



La section de file d'attente ILM est incluse pour la grille uniquement. Ces informations ne s'affichent pas dans l'onglet ILM d'un site ou d'un nœud de stockage.

- **Période d'analyse - estimation** : temps estimé pour effectuer une analyse ILM complète de tous les objets.



Une analyse complète ne garantit pas l'application du ILM à tous les objets.

- **Tentatives de réparation** : nombre total d'opérations de réparation d'objets pour les données répliquées qui ont été tentées. Ce nombre est incrémenté chaque fois qu'un nœud de stockage tente de réparer un objet à haut risque. Les réparations ILM à haut risque sont hiérarchisées si le grid est occupé.



La réparation d'un même objet peut être de nouveau incrémentée si la réplication a échoué après la réparation.

Ces attributs peuvent être utiles lorsque vous surveillez la progression de la récupération de volume du nœud de stockage. Si le nombre de réparations tentées a cessé d'augmenter et qu'une analyse complète a été effectuée, la réparation est probablement terminée.

## Surveiller les ressources réseau et système

L'intégrité et la bande passante du réseau entre les nœuds et les sites, ainsi que l'utilisation des ressources par les nœuds de grid individuels, sont essentielles à l'efficacité des opérations.

### Contrôle des connexions réseau et des performances

La connectivité réseau et la bande passante sont d'autant plus importantes si votre stratégie de gestion du cycle de vie des informations (ILM) copie les objets répliqués entre des sites ou stocke des objets avec code d'effacement au moyen d'un système qui assure la protection contre la perte de site. Si le réseau entre les sites n'est pas disponible, que la latence du réseau est trop élevée ou que la bande passante du réseau est insuffisante, certaines règles ILM risquent de ne pas pouvoir placer les objets là où prévu. Cela peut entraîner des échecs d'ingestion (lorsque l'option d'ingestion stricte est sélectionnée pour les règles ILM) ou de mauvaises performances d'ingestion et de journalisation des règles ILM.

Utilisez le gestionnaire de grille pour surveiller la connectivité et les performances du réseau, afin de résoudre rapidement tout problème.

Vous pouvez également "création de stratégies de classification du trafic réseau" surveiller le trafic lié à des locataires, des compartiments, des sous-réseaux ou des terminaux d'équilibrage de la charge. Vous pouvez définir des règles de limitation du trafic selon vos besoins.

## Étapes

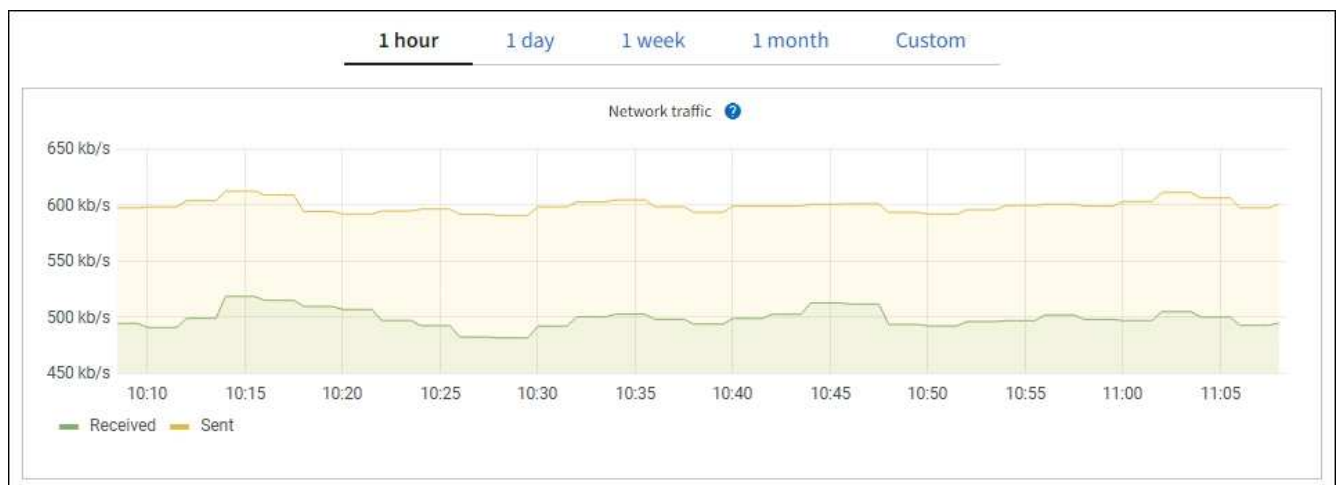
1. Sélectionnez **NOEUDS**.

La page nœuds s'affiche. Chaque nœud de la grille est répertorié au format de tableau.

Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID Deployment	Grid	0%	0%	—
Data Center 1	Site	0%	0%	—
DC1-ADM1	Primary Admin Node	—	—	21%
DC1-ARC1	Archive Node	—	—	8%
DC1-G1	Gateway Node	—	—	10%
DC1-S1	Storage Node	0%	0%	29%

2. Sélectionnez le nom de la grille, un site de centre de données spécifique ou un nœud de grille, puis sélectionnez l'onglet **réseau**.

Le graphique trafic réseau fournit un récapitulatif du trafic réseau global pour la grille dans son ensemble, le site du centre de données ou le nœud.



- a. Si vous avez sélectionné un nœud de grille, faites défiler vers le bas pour consulter la section



interfaces réseau de la page.

Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status
eth0	00:50:56:A7:66:75	10 Gigabit	Full	Off	Up

b. Pour les nœuds de grille, faites défiler vers le bas pour consulter la section **communication réseau** de la page.

Les tableaux de réception et de transmission indiquent le nombre d'octets et de paquets reçus et envoyés sur chaque réseau ainsi que d'autres mesures de réception et de transmission.

Network communication						
Receive						
Interface	Data	Packets	Errors	Dropped	Frame overruns	Frames
eth0	2.89 GB	19,421,503	0	24,032	0	0

Transmit						
Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	3.64 GB	18,494,381	0	0	0	0

3. Utilisez les indicateurs associés à vos stratégies de classification de trafic pour surveiller le trafic réseau.

a. Sélectionnez **CONFIGURATION > réseau > classification du trafic**.

La page règles de classification du trafic s'affiche et les stratégies existantes sont répertoriées dans le tableau.

#### Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

+ Create   Edit   Remove   Metrics		
Name	Description	ID
<input type="radio"/> ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
<input checked="" type="radio"/> Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bdbc894b

Displaying 2 traffic classification policies.

a. Pour afficher les graphiques présentant les mesures de réseau associées à une stratégie, sélectionnez le bouton radio à gauche de la stratégie, puis cliquez sur **métriques**.

b. Consultez les graphiques pour comprendre le trafic réseau associé à la stratégie.

Si une politique de classification du trafic est conçue pour limiter le trafic réseau, analysez la fréquence à laquelle le trafic est limité et déterminez si la politique continue de répondre à vos besoins. De temps en temps "ajustez chaque stratégie de classification du trafic au besoin", .

### Informations associées

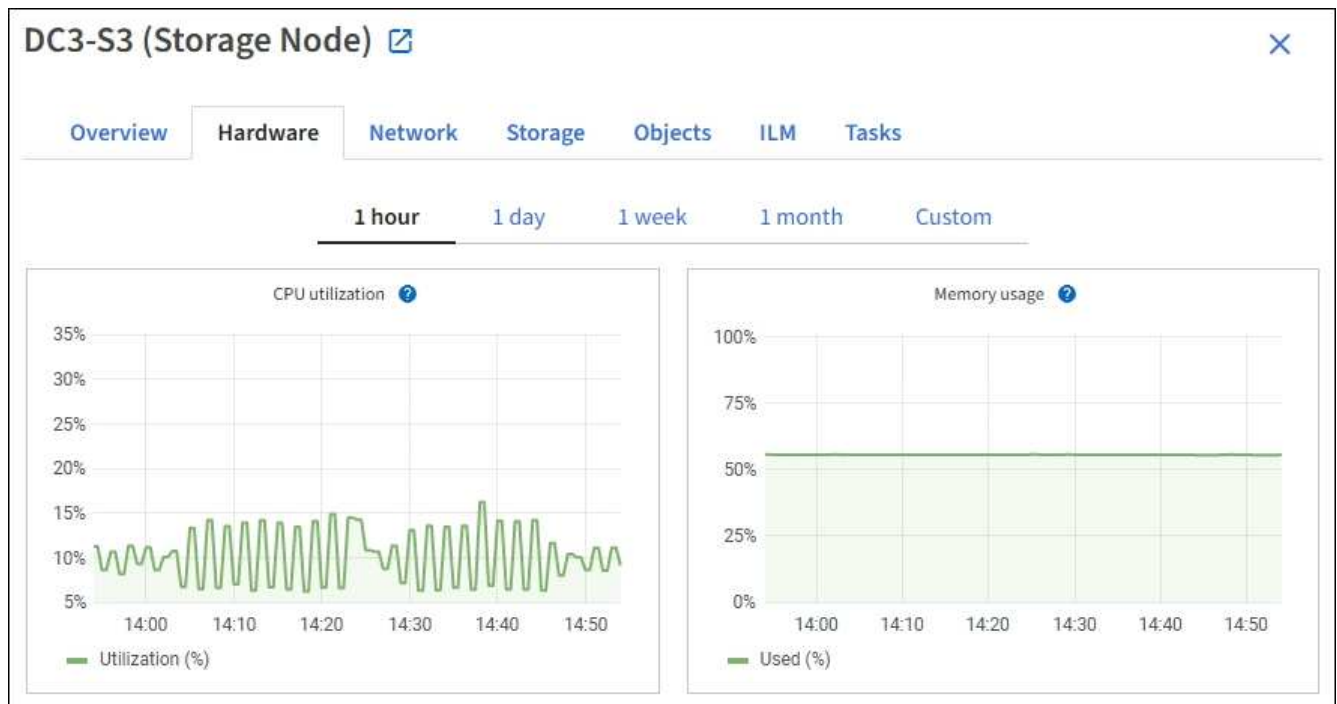
- ["Afficher l'onglet réseau"](#)
- ["Surveiller les États de connexion du nœud"](#)

### Contrôle des ressources au niveau des nœuds

Surveiller les nœuds de grid individuels pour vérifier leurs niveaux d'utilisation des ressources. Si les nœuds sont constamment surchargés, un nombre plus élevé de nœuds peut être requis pour une efficacité optimale des opérations.

### Étapes

1. Dans la page **NODES**, sélectionnez le nœud.
2. Sélectionnez l'onglet **matériel** pour afficher les graphiques de l'utilisation de l'UC et de la mémoire.



3. Pour afficher un intervalle de temps différent, sélectionnez l'une des commandes au-dessus du graphique ou du graphique. Vous pouvez afficher les informations disponibles pour les intervalles de 1 heure, 1 jour, 1 semaine ou 1 mois. Vous pouvez également définir un intervalle personnalisé, qui vous permet de spécifier des plages de date et d'heure.
4. Si le nœud est hébergé sur une appliance de stockage ou sur une appliance de services, faites défiler la page vers le bas pour afficher les tableaux des composants. L'état de tous les composants doit être « nominal ». Rechercher les composants ayant un autre état.

### Informations associées

- ["Afficher des informations sur les nœuds de stockage de l'appliance"](#)
- ["Affiche des informations sur les nœuds d'administration de l'appliance et les nœuds de passerelle"](#)

## Surveillez l'activité des locataires

Toutes les activités du client S3 sont associées aux comptes de locataires StorageGRID. Vous pouvez utiliser Grid Manager pour surveiller l'utilisation du stockage ou le trafic réseau de tous les locataires ou d'un locataire spécifique. Vous pouvez utiliser le journal des audits ou les tableaux de bord Grafana pour collecter des informations plus détaillées sur l'utilisation de StorageGRID par les locataires.

### Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".
- Vous avez le "Autorisation d'accès racine ou de comptes de locataires".

### Afficher tous les locataires

La page tenants affiche les informations de base pour tous les comptes de locataires actuels.

### Étapes

1. Sélectionnez **LOCATAIRES**.
2. Vérifiez les informations affichées sur les pages tenant.

L'espace logique utilisé, l'utilisation des quotas, le quota et le nombre d'objets sont indiqués pour chaque locataire. Si aucun quota n'est défini pour un locataire, les champs utilisation du quota et quota contiennent un tiret (—).



Les valeurs de l'espace utilisé sont des estimations. Ces estimations sont affectées par le moment de l'ingestion, la connectivité réseau et l'état des nœuds.

### Tenants

View information for each tenant account. Depending on the timing of ingests, network connectivity, and node status, the usage data shown might be out of date. To view more recent values, select the tenant name.

Create Export to CSV Actions Search tenants by name or ID Displaying 5 results

<input type="checkbox"/>	Name	Logical space used	Quota utilization	Quota	Object count	Sign in/Copy URL
<input type="checkbox"/>	Tenant 01	2.00 GB	<div style="width: 10%; background-color: green;"></div> 10%	20.00 GB	100	<a href="#">→</a> <a href="#">📄</a>
<input type="checkbox"/>	Tenant 02	85.00 GB	<div style="width: 85%; background-color: orange;"></div> 85%	100.00 GB	500	<a href="#">→</a> <a href="#">📄</a>
<input type="checkbox"/>	Tenant 03	500.00 TB	<div style="width: 50%; background-color: green;"></div> 50%	1.00 PB	10,000	<a href="#">→</a> <a href="#">📄</a>
<input type="checkbox"/>	Tenant 04	475.00 TB	<div style="width: 95%; background-color: red;"></div> 95%	500.00 TB	50,000	<a href="#">→</a> <a href="#">📄</a>
<input type="checkbox"/>	Tenant 05	5.00 GB	—	—	500	<a href="#">→</a> <a href="#">📄</a>

3. Vous pouvez également vous connecter à un compte locataire en sélectionnant le lien de connexion [→](#) dans la colonne **se connecter/Copier l'URL**.
4. Vous pouvez également copier l'URL de la page d'ouverture de session d'un locataire en sélectionnant le lien Copier l'URL [📄](#) dans la colonne **se connecter/Copier l'URL**.

- Si vous le souhaitez, sélectionnez **Exporter au format CSV** pour afficher et exporter un `.csv` fichier contenant les valeurs d'utilisation de tous les locataires.

Vous êtes invité à ouvrir ou enregistrer le `.csv` fichier.

Le contenu du `.csv` fichier ressemble à l'exemple suivant :

Tenant ID	Display Name	Space Used (Bytes)	Quota utilization (%)	Quota (Bytes)	Object Count	Protocol
12659822378459233654	Tenant 01	2000000000	10	20000000000	100	S3
99658234112547853685	Tenant 02	85000000000	85	110000000	500	S3
03521145586975586321	Tenant 03	60500000000	50	150000	10000	S3
44251365987569885632	Tenant 04	4750000000	95	140000000	50000	S3
36521587546689565123	Tenant 05	5000000000	Infinity		500	S3

Vous pouvez ouvrir `.csv` le fichier dans une feuille de calcul ou l'utiliser dans l'automatisation.

- Si aucun objet n'est répertorié, sélectionnez **actions** > **Supprimer** pour supprimer un ou plusieurs locataires. Voir "[Supprimer le compte de locataire](#)".

Vous ne pouvez pas supprimer un compte de locataire si le compte inclut des compartiments ou des conteneurs.

#### Afficher un locataire spécifique


Vous pouvez afficher les détails d'un locataire spécifique.

#### Étapes

- Sélectionnez le nom du locataire dans la page locataires.

La page des détails du locataire s'affiche.

## Tenant 02

Tenant ID: 4103 1879 2208 5551 2180  Quota utilization: 85%  
 Protocol: S3 Logical space used: 85.00 GB  
 Object count: 500 Quota: 100.00 GB


[Sign in](#) [Edit](#) [Actions](#) ▾

[Space breakdown](#) [Allowed features](#)

### Bucket space consumption

85.00 GB of 100.00 GB used


15.00 GB remaining (15%).







0 25% 50% 75% 100%

● bucket-01 ● bucket-02 ● bucket-03

### Bucket details

[Export to CSV](#)   Displaying 3 results

Name  ▾	Region  ▾	Space used  ▾	Object count  ▾
bucket-01		40.00 GB	250
bucket-02		30.00 GB	200
bucket-03		15.00 GB	50

2. Consultez la présentation du locataire en haut de la page.

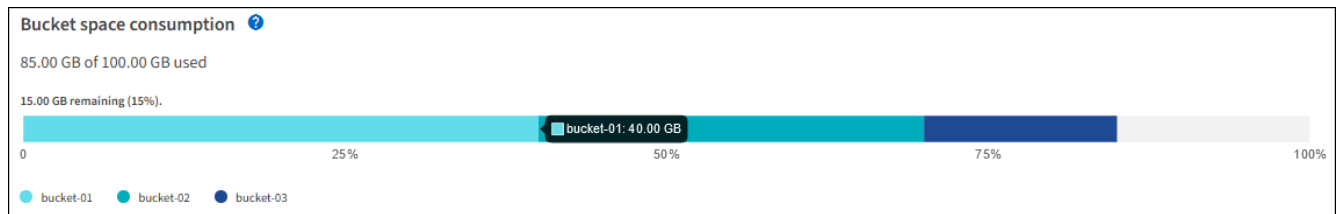
Cette section de la page de détails fournit des informations récapitulatives pour le locataire, notamment le nombre d'objets du locataire, l'utilisation du quota, l'espace logique utilisé et le paramètre de quota.

3. Dans l'onglet **Space Dclaquage**, consultez le graphique **Space Consumption**.

Ce tableau présente la consommation totale d'espace pour tous les compartiments S3 du locataire.

Si un quota a été défini pour ce tenant, le montant du quota utilisé et restant est affiché dans le texte (par exemple, 85.00 GB of 100 GB used). Si aucun quota n'a été défini, le locataire a un quota illimité et le texte ne contient qu'une quantité d'espace utilisée (par exemple, 85.00 GB used). Le graphique à barres indique le pourcentage de quota dans chaque compartiment ou conteneur. Si le locataire a dépassé le quota de stockage de plus de 1 % et d'au moins 1 Go, le graphique indique le quota total et le montant de l'excès.

Vous pouvez placer le curseur sur le graphique à barres pour voir le stockage utilisé par chaque compartiment ou conteneur. Vous pouvez placer votre curseur sur le segment de l'espace libre pour voir la quantité de quota de stockage restant.



L'utilisation des quotas est basée sur des estimations internes et peut être dépassée dans certains cas. Par exemple, StorageGRID vérifie le quota lorsqu'un locataire commence à charger des objets et rejette les nouvelles ingère si le locataire a dépassé le quota. Cependant, StorageGRID ne prend pas en compte la taille du téléchargement actuel lors de la détermination du dépassement du quota. Si des objets sont supprimés, un locataire peut temporairement empêcher le téléchargement de nouveaux objets jusqu'au recalcul de l'utilisation du quota. Le calcul de l'utilisation des quotas peut prendre 10 minutes ou plus.



L'utilisation du quota d'un locataire indique la quantité totale de données d'objet chargées par ce dernier sur StorageGRID (taille logique). L'utilisation du quota ne représente pas l'espace utilisé pour stocker des copies de ces objets et de leurs métadonnées (taille physique).



Vous pouvez activer la règle d'alerte **tenant quota usage high** pour déterminer si les locataires utilisent leurs quotas. Si elle est activée, cette alerte est déclenchée lorsqu'un locataire a utilisé 90 % de son quota. Pour obtenir des instructions, reportez-vous à la section "[Modifiez les règles d'alerte](#)".

4. Dans l'onglet **Space Dclaquage**, passez en revue les détails **Bucket Details**.

Ce tableau répertorie les compartiments S3 pour le locataire. L'espace utilisé correspond à la quantité totale de données d'objet dans le compartiment ou le conteneur. Cette valeur ne représente pas l'espace de stockage requis pour les copies ILM et les métadonnées d'objet.

5. Vous pouvez également sélectionner **Exporter au format CSV** pour afficher et exporter un fichier .csv contenant les valeurs d'utilisation de chaque compartiment ou conteneur.

Le contenu du fichier d'un locataire S3 .csv se présente comme suit :

Tenant ID	Bucket Name	Space Used (Bytes)	Number of Objects
64796966429038923647	bucket-01	88717711	14
64796966429038923647	bucket-02	21747507	11
64796966429038923647	bucket-03	15294070	3

Vous pouvez ouvrir .csv le fichier dans une feuille de calcul ou l'utiliser dans l'automatisation.

6. Vous pouvez également sélectionner l'onglet **fonctions autorisées** pour afficher la liste des autorisations et fonctionnalités activées pour le tenant. Vérifiez "[Modifiez le compte de tenant](#)" si vous avez besoin de modifier l'un de ces paramètres.

7. Si le locataire dispose de l'autorisation **utiliser la connexion de fédération de grille**, sélectionnez éventuellement l'onglet **fédération de grille** pour en savoir plus sur la connexion.

Voir "[Qu'est-ce que la fédération de grille ?](#)" et "[Gérer les locataires autorisés pour la fédération dans le grid](#)".

## Affichez le trafic réseau

Si des stratégies de classification du trafic sont en place pour un locataire, examinez le trafic réseau de ce locataire.

### Étapes

1. Sélectionnez **CONFIGURATION > réseau > classification du trafic**.

La page règles de classification du trafic s'affiche et les stratégies existantes sont répertoriées dans le tableau.

2. Consultez la liste des politiques pour identifier celles qui s'appliquent à un locataire spécifique.
3. Pour afficher les mesures associées à une stratégie, sélectionnez le bouton radio à gauche de la stratégie et sélectionnez **métriques**.
4. Analysez les graphiques pour déterminer à quelle fréquence la stratégie limite le trafic et si vous devez ajuster la stratégie.

Voir "[Gérer les stratégies de classification du trafic](#)" pour plus d'informations.

### Utilisez le journal d'audit

Vous pouvez également utiliser le journal des audits pour une surveillance plus granulaire des activités d'un locataire.

Par exemple, vous pouvez surveiller les types d'informations suivants :

- Des opérations client spécifiques, telles QUE METTRE, OBTENIR ou SUPPRIMER
- Tailles d'objet
- Règle ILM appliquée aux objets
- Adresse IP source des requêtes client

Les journaux d'audit sont écrits dans des fichiers texte que vous pouvez analyser à l'aide de l'outil d'analyse des journaux de votre choix. Vous pouvez ainsi mieux comprendre les activités des clients ou implémenter des modèles de facturation et de refacturation sophistiqués.

Voir "[Examiner les journaux d'audit](#)" pour plus d'informations.

### Utilisez des metrics Prometheus

Éventuellement, utilisez des metrics Prometheus pour générer des rapports sur l'activité des locataires.

- Dans le Gestionnaire de grille, sélectionnez **SUPPORT > Outils > métriques**. Vous pouvez utiliser les tableaux de bord existants, tels que S3 Overview, pour examiner les activités des clients.



Les outils disponibles sur la page métriques sont principalement destinés au support technique. Certaines fonctions et options de menu de ces outils ne sont intentionnellement pas fonctionnelles.

- En haut du Gestionnaire de grille, sélectionnez l'icône d'aide et sélectionnez **documentation API**. Vous pouvez utiliser les mesures de la section Metrics de l'API de gestion du grid pour créer des règles d'alerte et des tableaux de bord personnalisés pour l'activité des locataires.

Voir "[Examinez les metrics de support](#)" pour plus d'informations.

## Surveillez les opérations du client S3

Vous pouvez surveiller les taux d'entrée et de récupération des objets, ainsi que les mesures relatives au nombre d'objets, aux requêtes et à la vérification. Vous pouvez afficher le nombre de tentatives de lecture, d'écriture et de modification d'objets du système StorageGRID ayant échoué et réussies par les applications client.

### Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).

### Étapes

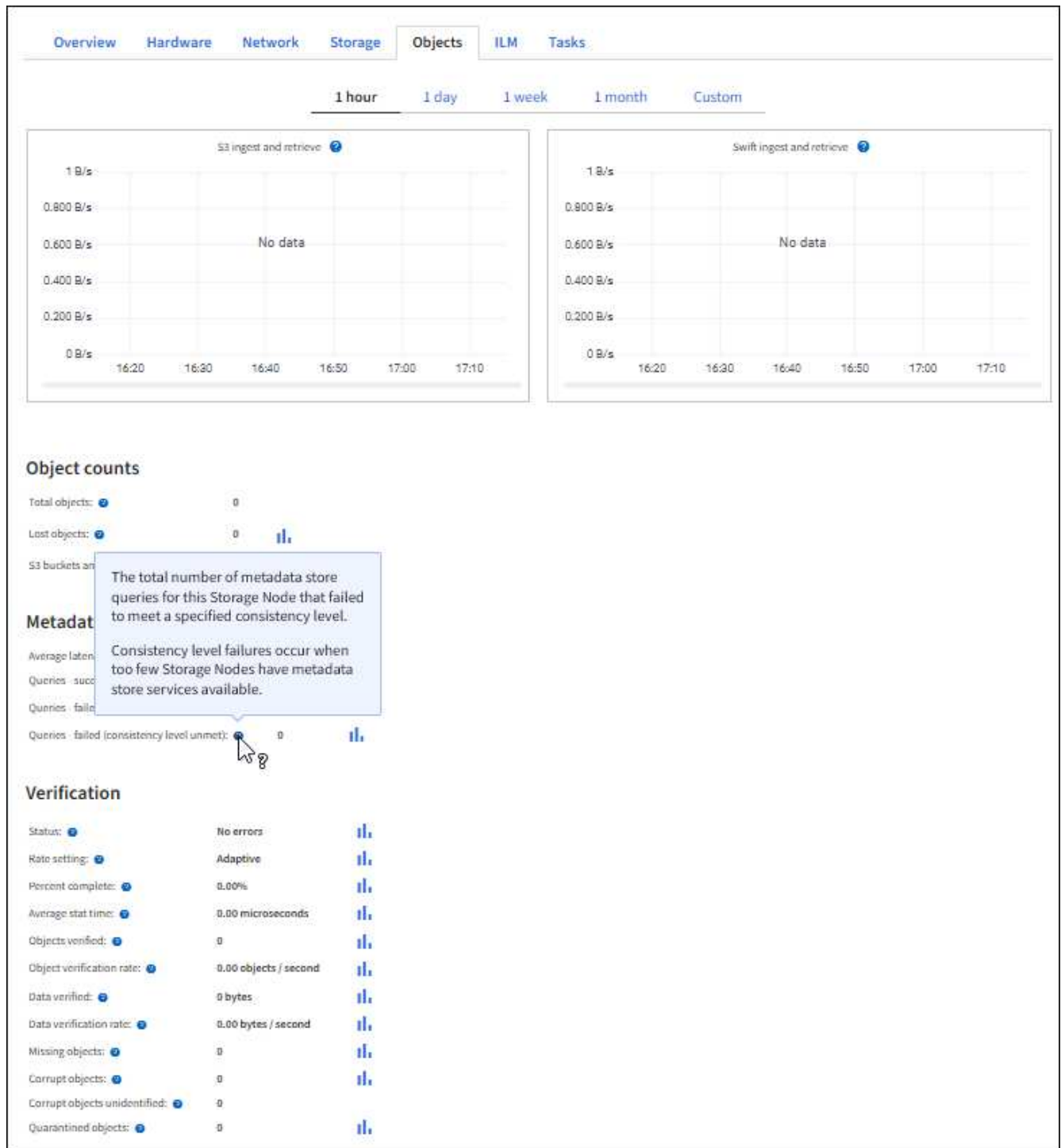
1. Dans le tableau de bord, sélectionnez l'onglet **Performance**.
2. Reportez-vous aux graphiques S3, qui résument le nombre d'opérations client effectuées par les nœuds de stockage et le nombre de requêtes d'API reçues par les nœuds de stockage au cours de la période sélectionnée.
3. Sélectionnez **NODES** pour accéder à la page noeuds.
4. Dans la page d'accueil noeuds (niveau grille), sélectionnez l'onglet **objets**.

Le graphique présente les taux d'ingestion et de récupération S3 pour l'ensemble de votre système StorageGRID, en octets par seconde, ainsi que la quantité de données ingérées ou récupérées. Vous pouvez sélectionner un intervalle de temps ou appliquer un intervalle personnalisé.

5. Pour afficher les informations relatives à un nœud de stockage particulier, sélectionnez-le dans la liste de gauche et sélectionnez l'onglet **objets**.

Le graphique présente les taux d'ingestion et de récupération du nœud. L'onglet inclut également des mesures pour le nombre d'objets, les requêtes de métadonnées et les opérations de vérification.





## Surveiller les opérations d'équilibrage de charge

Si vous utilisez un équilibreur de charge pour gérer les connexions client à StorageGRID, vous devez surveiller les opérations d'équilibrage de charge après avoir configuré le système initialement et après avoir effectué des modifications de configuration ou effectué une extension.

### Description de la tâche

Vous pouvez utiliser le service Load Balancer sur les nœuds d'administration ou les nœuds de passerelle, ou un équilibreur de charge tiers externe pour distribuer les requêtes client sur plusieurs nœuds de stockage.

Une fois l'équilibrage de la charge configuré, vérifiez que les opérations d'ingestion et de récupération des objets sont réparties de manière homogène entre les nœuds de stockage. La répartition homogène des demandes permet à StorageGRID de rester réactif aux demandes des clients sous charge et de maintenir les performances des clients.

Si vous avez configuré un groupe haute disponibilité de nœuds de passerelle ou de nœuds d'administration en mode de sauvegarde active/active, seul un nœud du groupe distribue activement les requêtes client.

Pour plus d'informations, voir "[Configurer les connexions client S3](#)".

## Étapes

1. Si les clients S3 se connectent à l'aide du service Load Balancer, vérifiez que les nœuds d'administration ou les nœuds de passerelle distribuent activement le trafic comme vous le souhaitez :
  - a. Sélectionnez **NOEUDS**.
  - b. Sélectionnez un nœud de passerelle ou un nœud d'administration.
  - c. Dans l'onglet **Overview**, vérifiez si une interface de nœud fait partie d'un groupe HA et si l'interface de nœud a le rôle Primary.

Les nœuds ayant le rôle de nœud principal et les nœuds qui ne font pas partie d'un groupe haute disponibilité doivent distribuer activement les demandes aux clients.

- d. Pour chaque nœud devant distribuer activement des demandes client, sélectionnez le "[Onglet Load Balancer](#)".
- e. Consultez le graphique du trafic des demandes d'équilibrage de charge pour la dernière semaine afin de vous assurer que le nœud distribue activement les demandes.

Les nœuds d'un groupe haute disponibilité à sauvegarde active peuvent parfois prendre le rôle de sauvegarde. Pendant ce temps, les nœuds ne distribuent pas les requêtes client.
- f. Consultez le graphique du taux de demande entrant de Load Balancer pour la dernière semaine afin de vérifier le débit d'objet du nœud.
- g. Répétez cette procédure pour chaque nœud d'administration ou de passerelle du système StorageGRID.
- h. Vous pouvez également utiliser les stratégies de classification du trafic pour afficher une analyse plus détaillée du trafic desservi par le service Load Balancer.

2. Vérifiez que ces demandes sont réparties de manière homogène vers les nœuds de stockage.
  - a. Sélectionnez **Storage Node > LDR > HTTP**.
  - b. Examiner le nombre de **sessions entrantes actuellement établies**.
  - c. Répétez l'opération pour chaque nœud de stockage de la grille.

Le nombre de sessions doit être approximativement égal sur tous les nœuds de stockage.

## Surveiller les connexions de fédération de grille

Vous pouvez surveiller des informations de base sur tous "[connexions de fédération de grille](#)", des informations détaillées sur une connexion spécifique ou des metrics Prometheus sur les opérations de réplication entre les grilles. Vous pouvez surveiller une connexion à partir de l'une ou l'autre des grilles.

## Avant de commencer

- Vous êtes connecté au Gestionnaire de grille sur l'une des grilles à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Autorisation d'accès racine"](#) pour la grille à laquelle vous êtes connecté.

## Afficher toutes les connexions

La page Grid federation affiche des informations de base sur toutes les connexions de fédération de grille et sur tous les comptes de locataire autorisés à utiliser les connexions de fédération de grille.

## Étapes

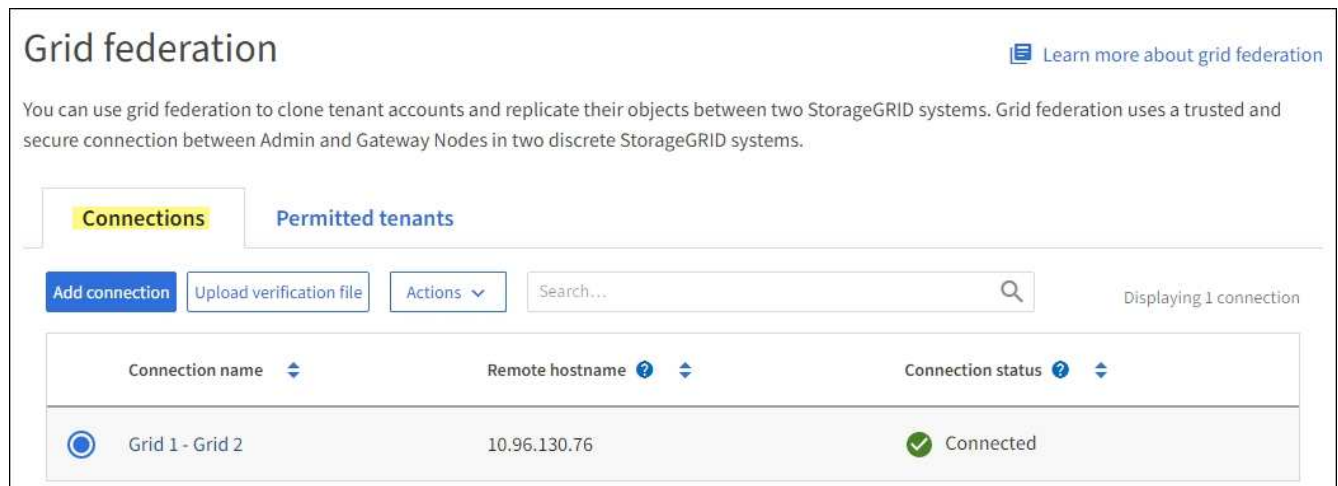
1. Sélectionnez **CONFIGURATION > système > fédération de grille**.

La page grid federation s'affiche.

2. Pour afficher des informations de base sur toutes les connexions de cette grille, sélectionnez l'onglet **connexions**.

À partir de cet onglet, vous pouvez :

- ["Créer une nouvelle connexion"](#).
- Sélectionnez une connexion existante à ["modifier ou tester"](#).



The screenshot shows the 'Grid federation' page. At the top, there's a title 'Grid federation' and a link 'Learn more about grid federation'. Below the title, a paragraph explains that grid federation is used to clone tenant accounts and replicate objects between two StorageGRID systems. The main content area has two tabs: 'Connections' (active) and 'Permitted tenants'. Below the tabs, there are buttons for 'Add connection', 'Upload verification file', and 'Actions', along with a search bar and a 'Displaying 1 connection' indicator. A table below displays the connection details:

Connection name	Remote hostname	Connection status
Grid 1 - Grid 2	10.96.130.76	Connected

3. Pour afficher les informations de base de tous les comptes de locataires de cette grille disposant de l'autorisation **utiliser la connexion de fédération de grille**, sélectionnez l'onglet **locataires autorisés**.

À partir de cet onglet, vous pouvez :

- ["Afficher la page de détails pour chaque locataire autorisé"](#).
- Afficher la page de détails de chaque connexion. Voir [Afficher une connexion spécifique](#).
- Sélectionnez un locataire autorisé et ["supprimez l'autorisation"](#).
- Vérifiez la présence d'erreurs de réplication inter-grille et effacez la dernière erreur, le cas échéant. Voir ["Dépanner les erreurs de fédération de grille"](#).

## Grid federation [Learn more about grid federation](#)

You can use grid federation to clone tenant accounts and replicate their objects between two StorageGRID systems. Grid federation uses a trusted and secure connection between Admin and Gateway Nodes in two discrete StorageGRID systems.

Connections
Permitted tenants

Remove permission
Clear error

Q

Displaying one result

Tenant name	Connection name	Connection status	Remote grid hostname	Last error
<span style="color: blue;">●</span> Tenant A	Grid 1 - Grid 2	<span style="color: green;">✔</span> Connected	10.96.130.76	<a href="#">Check for errors</a>

### permet d'afficher une connexion spécifique

Vous pouvez afficher les détails d'une connexion de fédération de grille spécifique.

### Étapes

1. Sélectionnez l'un des onglets de la page fédération de grille, puis sélectionnez le nom de la connexion dans le tableau.

Dans la page de détails de la connexion, vous pouvez :

- Consultez les informations d'état de base sur la connexion, y compris les noms d'hôtes locaux et distants, le port et l'état de la connexion.
  - Sélectionnez une connexion à "[modifier, tester ou supprimer](#)".
2. Lors de l'affichage d'une connexion spécifique, sélectionnez l'onglet **locataires autorisés** pour afficher des détails sur les locataires autorisés pour la connexion.

À partir de cet onglet, vous pouvez :

- "[Afficher la page de détails pour chaque locataire autorisé](#)".
- "[Supprimer l'autorisation d'un locataire](#)" pour utiliser la connexion.
- Recherchez les erreurs de réplication inter-grille et effacez la dernière erreur. Voir "[Dépanner les erreurs de fédération de grille](#)".

### Grid 1 - Grid 2

Local hostname (this grid): 10.96.130.64  
Port: 23000  
Remote hostname (other grid): 10.96.130.76  
Connection status: ✔ Connected

[Edit](#) [Download file](#) [Test connection](#) [Remove](#)

**Permitted tenants** [Certificates](#)

[Remove permission](#) [Clear error](#)  Displaying one result


Tenant name	Last error
<input checked="" type="radio"/> Tenant A	<a href="#">Check for errors</a>

3. Lors de l'affichage d'une connexion spécifique, sélectionnez l'onglet **certificats** pour afficher les certificats de serveur et de client générés par le système pour cette connexion.

À partir de cet onglet, vous pouvez :

- "[Faire pivoter les certificats de connexion](#)".
- Sélectionnez **Server** ou **client** pour afficher ou télécharger le certificat associé ou copier le certificat PEM.

## Grid A-Grid B

Local hostname (this grid): 10.96.106.230  
Port: 23000  
Remote hostname (other grid): 10.96.104.230  
Connection status:  Connected

Edit

Download file

Test connection

Remove

Permitted tenants

Certificates

Rotate certificates

Server

Client

Download certificate

Copy certificate PEM

### Metadata ?

Subject DN: /C=US/ST=California/L=Sunnyvale/O=NetApp Inc./OU=NetApp StorageGRID/CN=10.96.106.230  
Serial number: 30:81:B8:DD:AE:B2:86:0A  
Issuer DN: /C=US/ST=California/L=Sunnyvale/O=NetApp Inc./OU=NetApp StorageGRID/CN=GPT  
Issued on: 2022-10-04T02:21:18.000Z  
Expires on: 2024-10-03T19:05:13.000Z  
SHA-1 fingerprint: 92:7A:03:AF:6D:1C:94:8C:33:24:08:84:F9:2B:01:23:7D:BE:F2:DF  
SHA-256 fingerprint: 54:97:3E:77:EB:D3:6A:0F:8F:EE:72:83:D0:39:86:02:32:A5:60:9D:6F:C0:A2:3C:76:DA:3F:4D:FF:64:5D:60  
Alternative names: IP Address:10.96.106.230

### Certificate PEM ?

```
-----BEGIN CERTIFICATE-----
MIIGdTCCBF2gAwIBAgIIMIG43a6yhgowDQYJKoZIhvcNAQENBQAwzELMAkGA1UE
BhMCVVMxIjEzARBgNVBAgMCkNhbm91dG8wCzAJBgNVBAMTMT0.96.106.230
MB0YGA90CjA9AgQVAAQVAAQVAAQVAAQVAAQVAAQVAAQVAAQVAAQVAAQVAAQVAA
-----END CERTIFICATE-----
```

### Examinez les metrics de réplication entre les grilles

Vous pouvez utiliser le tableau de bord de réplication Cross-Grid de Grafana pour afficher les metrics Prometheus sur les opérations de réplication cross-grid sur votre grille.

### Étapes

1. Dans le Gestionnaire de grille, sélectionnez **SUPPORT > Outils > métriques**.



Les outils disponibles sur la page métriques sont destinés au support technique. Certaines fonctions et options de menu de ces outils sont intentionnellement non fonctionnelles et peuvent faire l'objet de modifications. Voir la liste de "[Metrics Prometheus couramment utilisés](#)".

2. Dans la section Grafana de la page, sélectionnez **Cross Grid Replication**.

Pour des instructions détaillées, voir "[Examinez les metrics de support](#)".

3. Pour réessayer la réplication d'objets qui n'ont pas pu être répliqués, reportez-vous à la section "[Identifier et réessayer les opérations de réplication ayant échoué](#)".

## Gérer les alertes

### Gérer les alertes

Le système d'alerte offre une interface facile à utiliser pour détecter, évaluer et résoudre les problèmes susceptibles de se produire lors du fonctionnement de StorageGRID.

Les alertes sont déclenchées à des niveaux de gravité spécifiques lorsque les conditions des règles d'alerte sont définies comme vrai. Lorsqu'une alerte est déclenchée, les actions suivantes se produisent :

- Une icône de gravité d'alerte s'affiche sur le tableau de bord dans le Gestionnaire de grille et le nombre d'alertes actuelles est incrémenté.
- L'alerte s'affiche sur la page de résumé **NODES** et sur l'onglet **NODES > node > Overview**.
- Une notification par e-mail est envoyée, en supposant que vous avez configuré un serveur SMTP et fourni des adresses e-mail aux destinataires.
- Une notification SNMP (simple Network Management Protocol) est envoyée, en supposant que vous avez configuré l'agent SNMP StorageGRID.

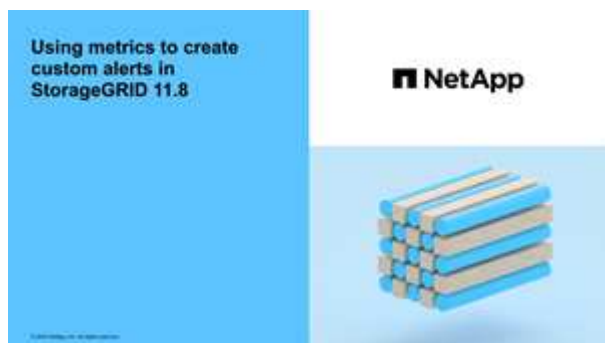
Vous pouvez créer des alertes personnalisées, modifier ou désactiver des alertes et gérer les notifications d'alerte.

Pour en savoir plus :

- Regardez la vidéo : "[Vidéo : présentation des alertes](#)"



- Regardez la vidéo : "[Vidéo : alertes personnalisées](#)"



- Voir la "[Référence des alertes](#)".

## Afficher les règles d'alerte

Les règles d'alerte définissent les conditions qui déclenchent "[alertes spécifiques](#)". StorageGRID inclut un ensemble de règles d'alerte par défaut que vous pouvez utiliser en l'état ou en modifier, ou vous pouvez créer des règles d'alerte personnalisées.

Vous pouvez afficher la liste de toutes les règles d'alerte par défaut et personnalisées pour savoir quelles conditions déclenchent chaque alerte et pour déterminer si les alertes sont désactivées.

### Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur web pris en charge](#)".
- Vous avez le "[Gérer les alertes ou l'autorisation d'accès racine](#)".
- Vous avez éventuellement regardé la vidéo : "[Vidéo : présentation des alertes](#)"



## Étapes

1. Sélectionnez **ALERTES > règles**.

La page règles d'alerte s'affiche.

Alert Rules [Learn more](#)

Alert rules define which conditions trigger specific alerts.




You can edit the conditions for default alert rules to better suit your environment, or create custom alert rules that use your own conditions for triggering alerts.

Name	Conditions	Type	Status
<input type="radio"/> <b>Appliance battery expired</b> The battery in the appliance's storage controller has expired.	storagegrid_appliance_component_failure(type="REC_EXPIRED_BATTERY") Major > 0	Default	Enabled
<input type="radio"/> <b>Appliance battery failed</b> The battery in the appliance's storage controller has failed.	storagegrid_appliance_component_failure(type="REC_FAILED_BATTERY") Major > 0	Default	Enabled
<input type="radio"/> <b>Appliance battery has insufficient learned capacity</b> The battery in the appliance's storage controller has insufficient learned capacity.	storagegrid_appliance_component_failure(type="REC_BATTERY_WARN") Major > 0	Default	Enabled
<input type="radio"/> <b>Appliance battery near expiration</b> The battery in the appliance's storage controller is nearing expiration.	storagegrid_appliance_component_failure(type="REC_BATTERY_NEAR_EXPIRATION") Major > 0	Default	Enabled
<input type="radio"/> <b>Appliance battery removed</b> The battery in the appliance's storage controller is missing.	storagegrid_appliance_component_failure(type="REC_REMOVED_BATTERY") Major > 0	Default	Enabled
<input type="radio"/> <b>Appliance battery too hot</b> The battery in the appliance's storage controller is overheated.	storagegrid_appliance_component_failure(type="REC_BATTERY_OVERTEMP") Major > 0	Default	Enabled
<input type="radio"/> <b>Appliance cache backup device failed</b> A persistent cache backup device has failed.	storagegrid_appliance_component_failure(type="REC_CACHE_BACKUP_DEVICE_FAILED") Major > 0	Default	Enabled
<input type="radio"/> <b>Appliance cache backup device insufficient capacity</b> There is insufficient cache backup device capacity.	storagegrid_appliance_component_failure(type="REC_CACHE_BACKUP_DEVICE_INSUFFICIENT_CAPACITY") Major > 0	Default	Enabled
<input type="radio"/> <b>Appliance cache backup device write-protected</b> A cache backup device is write-protected.	storagegrid_appliance_component_failure(type="REC_CACHE_BACKUP_DEVICE_WRITE_PROTECTED") Major > 0	Default	Enabled
<input type="radio"/> <b>Appliance cache memory size mismatch</b> The two controllers in the appliance have different cache sizes.	storagegrid_appliance_component_failure(type="REC_CACHE_MEM_SIZE_MISMATCH") Major > 0	Default	Enabled

Displaying 62 alert rules.



## 2. Vérifiez les informations du tableau des règles d'alerte :

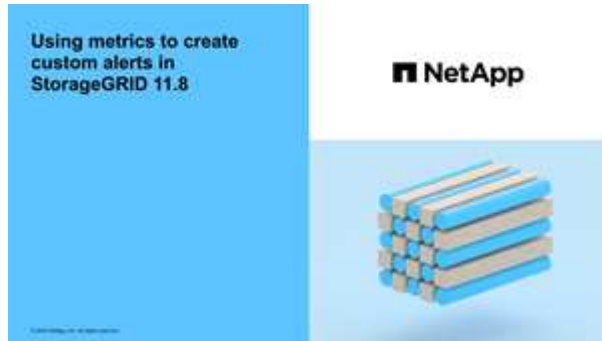
En-tête de colonne	Description
Nom	Nom et description uniques de la règle d'alerte. Les règles d'alerte personnalisées sont répertoriées en premier, suivies des règles d'alerte par défaut. Le nom de la règle d'alerte est l'objet des notifications par e-mail.
Conditions	<p>Expressions Prometheus qui déterminent le moment où cette alerte est déclenchée. Une alerte peut être déclenchée à un ou plusieurs des niveaux de sévérité suivants, mais une condition pour chaque gravité n'est pas requise.</p> <ul style="list-style-type: none"><li>• <b>Critique</b>  : il existe une condition anormale qui a arrêté les opérations normales d'un nœud ou d'un service StorageGRID. Vous devez immédiatement résoudre le problème sous-jacent. Une interruption du service et une perte de données peuvent se produire si le problème n'est pas résolu.</li><li>• <b>Majeur</b>  : il existe une condition anormale qui affecte les opérations en cours ou qui approche du seuil pour une alerte critique. Vous devez examiner les alertes majeures et résoudre tous les problèmes sous-jacents pour vérifier que leur condition anormale n'arrête pas le fonctionnement normal d'un nœud ou d'un service StorageGRID.</li><li>• <b>Mineur</b>  : le système fonctionne normalement, mais il existe une condition anormale qui pourrait affecter la capacité de fonctionnement du système s'il continue. Vous devez surveiller et résoudre les alertes mineures qui ne sont pas claires par elles-mêmes pour vous assurer qu'elles n'entraînent pas de problème plus grave.</li></ul>
Type	<p>Type de règle d'alerte :</p> <ul style="list-style-type: none"><li>• <b>Default</b> : règle d'alerte fournie avec le système. Vous pouvez désactiver une règle d'alerte par défaut ou modifier les conditions et la durée d'une règle d'alerte par défaut. Vous ne pouvez pas supprimer une règle d'alerte par défaut.</li><li>• <b>Par défaut*</b> : règle d'alerte par défaut qui inclut une condition ou une durée modifiée. Si nécessaire, vous pouvez facilement rétablir une condition modifiée par défaut.</li><li>• <b>Custom</b> : une règle d'alerte que vous avez créée. Vous pouvez désactiver, modifier et supprimer des règles d'alerte personnalisées.</li></ul>
État	Si cette règle d'alerte est actuellement activée ou désactivée. Les conditions des règles d'alerte désactivées ne sont pas évaluées et aucune alerte n'est déclenchée.

### Création de règles d'alerte personnalisées

Vous pouvez créer des règles d'alerte personnalisées afin de définir vos propres conditions pour déclencher des alertes.

## Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Gérer les alertes ou l'autorisation d'accès racine"](#).
- Vous connaissez le ["Metrics Prometheus couramment utilisés"](#).
- Vous comprenez le ["Syntaxe des requêtes Prometheus"](#).
- Si vous le souhaitez, vous avez regardé la vidéo : ["Vidéo : alertes personnalisées"](#).



## Description de la tâche

StorageGRID ne valide pas les alertes personnalisées. Si vous décidez de créer des règles d'alerte personnalisées, suivez les consignes générales suivantes :

- Consultez les conditions des règles d'alerte par défaut et utilisez-les comme exemples pour vos règles d'alerte personnalisées.
- Si vous définissez plusieurs conditions pour une règle d'alerte, utilisez la même expression pour toutes les conditions. Modifiez ensuite la valeur seuil pour chaque condition.
- Vérifier soigneusement chaque condition pour détecter les fautes de frappe et les erreurs logiques.
- Utilisez uniquement les metrics répertoriées dans l'API Grid Management.
- Lors du test d'une expression à l'aide de l'API de gestion de grille, sachez qu'une réponse « réussie » peut être un corps de réponse vide (aucune alerte déclenchée). Pour vérifier si l'alerte est déclenchée, vous pouvez définir temporairement une valeur de seuil sur laquelle vous vous attendez à ce que la valeur soit vraie actuellement.

Par exemple, pour tester l'expression `node_memory_MemTotal_bytes < 24000000000`, exécutez d'abord `node_memory_MemTotal_bytes >= 0` et assurez-vous d'obtenir les résultats attendus (tous les nœuds renvoient une valeur). Ensuite, remplacez l'opérateur et le seuil par les valeurs prévues et recommencez. Aucun résultat n'indique qu'il n'y a pas d'alerte en cours pour cette expression.

- Ne supposez pas qu'une alerte personnalisée fonctionne, sauf si vous avez validé que l'alerte est déclenchée quand vous le souhaitez.

## Étapes

1. Sélectionnez **ALERTES > règles**.

La page règles d'alerte s'affiche.

2. Sélectionnez **Créer règle personnalisée**.

La boîte de dialogue Créer une règle personnalisée s'affiche.

## Create Custom Rule

Enabled

Unique Name

Description

Recommended Actions  
(optional)

### Conditions ?

Minor

Major

Critical

Enter the amount of time a condition must continuously remain in effect before an alert is triggered.

Duration

5

minutes

Cancel

Save

3. Cochez ou décochez la case **activé** pour déterminer si cette règle d'alerte est actuellement activée.

Si une règle d'alerte est désactivée, ses expressions ne sont pas évaluées et aucune alerte n'est déclenchée.

4. Saisissez les informations suivantes :

Champ	Description
Nom unique	Un nom unique pour cette règle. Le nom de la règle d'alerte s'affiche sur la page alertes et est également l'objet des notifications par e-mail. Les noms des règles d'alerte peuvent comporter entre 1 et 64 caractères.

Champ	Description
Description	Description du problème. La description est le message d'alerte affiché sur la page alertes et dans les notifications par e-mail. Les descriptions des règles d'alerte peuvent comporter entre 1 et 128 caractères.
Actions recommandées	En option, les actions recommandées à effectuer lorsque cette alerte est déclenchée. Saisissez les actions recommandées en texte brut (aucun code de mise en forme). Les actions recommandées pour les règles d'alerte peuvent comporter entre 0 et 1,024 caractères.

5. Dans la section Conditions, entrez une expression Prometheus pour un ou plusieurs niveaux de gravité d'alerte.


Une expression de base est généralement de la forme :

```
[metric] [operator] [value]
```

Les expressions peuvent être de toute longueur, mais apparaissent sur une seule ligne dans l'interface utilisateur. Au moins une expression est requise.

Cette expression déclenche une alerte si la quantité de RAM installée pour un nœud est inférieure à 24,000,000,000 octets (24 Go).

```
node_memory_MemTotal_bytes < 24000000000
```

Pour afficher les metrics disponibles et tester les expressions Prometheus, sélectionnez l'icône d'aide  et suivez le lien vers la section Metrics de l'API de gestion de grille.

6. Dans le champ **durée**, entrez la durée pendant laquelle une condition doit rester en vigueur en continu avant le déclenchement de l'alerte et sélectionnez une unité de temps.

Pour déclencher une alerte immédiatement lorsqu'une condition devient vraie, entrez **0**. Augmentez cette valeur pour éviter que des conditions temporaires ne déclenchent des alertes.

La valeur par défaut est 5 minutes.

7. Sélectionnez **Enregistrer**.

La boîte de dialogue se ferme et la nouvelle règle d'alerte personnalisée apparaît dans le tableau règles d'alerte.

## Modifiez les règles d'alerte

Vous pouvez modifier une règle d'alerte pour modifier les conditions de déclenchement, pour une règle d'alerte personnalisée, vous pouvez également mettre à jour le nom de la règle, sa description et les actions recommandées.

### Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).

- Vous avez le "[Gérer les alertes ou l'autorisation d'accès racine](#)".

### Description de la tâche

Lorsque vous modifiez une règle d'alerte par défaut, vous pouvez modifier les conditions pour les alertes mineures, majeures et critiques, ainsi que la durée. Lorsque vous modifiez une règle d'alerte personnalisée, vous pouvez également modifier le nom, la description et les actions recommandées de la règle.



Soyez prudent lorsque vous décidez de modifier une règle d'alerte. Si vous modifiez les valeurs de déclenchement, il est possible que vous ne détéciez pas de problème sous-jacent tant qu'elle n'empêche pas l'exécution d'une opération critique.

### Étapes

1. Sélectionnez **ALERTES > règles**.

La page règles d'alerte s'affiche.

2. Sélectionnez le bouton radio correspondant à la règle d'alerte que vous souhaitez modifier.
3. Sélectionnez **Modifier la règle**.

La boîte de dialogue Modifier la règle s'affiche. Cet exemple montre une règle d'alerte par défaut, les champs Nom unique, Description et actions recommandées sont désactivés et ne peuvent pas être modifiés.

## Edit Rule - Low installed node memory

Enabled

Unique Name

Description

Recommended Actions (optional) VMware installation- [Red Hat Enterprise Linux or CentOS installation](#)
- [Ubuntu or Debian installation](#)
"/>

### Conditions

Minor

Major

Critical

Enter the amount of time a condition must continuously remain in effect before an alert is triggered.

Duration

Cancel

Save

4. Cochez ou décochez la case **activé** pour déterminer si cette règle d'alerte est actuellement activée.

Si une règle d'alerte est désactivée, ses expressions ne sont pas évaluées et aucune alerte n'est déclenchée.



Si vous désactivez la règle d'alerte pour une alerte en cours, vous devez attendre quelques minutes que l'alerte n'apparaisse plus comme une alerte active.



En général, la désactivation d'une règle d'alerte par défaut n'est pas recommandée. Si une règle d'alerte est désactivée, vous risquez de ne pas détecter un problème sous-jacent tant qu'elle n'empêche pas l'exécution d'une opération critique.

5. Pour les règles d'alerte personnalisées, mettez à jour les informations suivantes si nécessaire.



Vous ne pouvez pas modifier ces informations pour les règles d'alerte par défaut.

Champ	Description
Nom unique	Un nom unique pour cette règle. Le nom de la règle d'alerte s'affiche sur la page alertes et est également l'objet des notifications par e-mail. Les noms des règles d'alerte peuvent comporter entre 1 et 64 caractères.
Description	Description du problème. La description est le message d'alerte affiché sur la page alertes et dans les notifications par e-mail. Les descriptions des règles d'alerte peuvent comporter entre 1 et 128 caractères.
Actions recommandées	En option, les actions recommandées à effectuer lorsque cette alerte est déclenchée. Saisissez les actions recommandées en texte brut (aucun code de mise en forme). Les actions recommandées pour les règles d'alerte peuvent comporter entre 0 et 1,024 caractères.

6. Dans la section Conditions, entrez ou mettez à jour l'expression Prometheus pour un ou plusieurs niveaux de gravité d'alerte.



Si vous souhaitez restaurer une condition pour une règle d'alerte par défaut modifiée à sa valeur d'origine, sélectionnez les trois points à droite de la condition modifiée.

#### Conditions

Minor	<input type="text"/>
Major	<input type="text" value="node_memory_MemTotal_bytes &lt; 24000000000"/>
Critical	<input type="text" value="node_memory_MemTotal_bytes &lt;= 14000000000"/>



Si vous mettez à jour les conditions d'une alerte en cours, vos modifications risquent de ne pas être appliquées tant que la condition précédente n'est pas résolue. La prochaine fois que l'une des conditions de la règle est remplie, l'alerte reflète les valeurs mises à jour.

Une expression de base est généralement de la forme :

```
[metric] [operator] [value]
```

Les expressions peuvent être de toute longueur, mais apparaissent sur une seule ligne dans l'interface utilisateur. Au moins une expression est requise.

Cette expression déclenche une alerte si la quantité de RAM installée pour un nœud est inférieure à 24,000,000,000 octets (24 Go).

```
node_memory_MemTotal_bytes < 24000000000
```

7. Dans le champ **durée**, entrez la durée pendant laquelle une condition doit rester en vigueur en continu avant le déclenchement de l'alerte et sélectionnez l'unité de temps.

Pour déclencher une alerte immédiatement lorsqu'une condition devient vraie, entrez **0**. Augmentez cette

valeur pour éviter que des conditions temporaires ne déclenchent des alertes.

La valeur par défaut est 5 minutes.

#### 8. Sélectionnez **Enregistrer**.

Si vous avez modifié une règle d'alerte par défaut, **default\*** apparaît dans la colonne Type. Si vous avez désactivé une règle d'alerte par défaut ou personnalisée, **Disabled** apparaît dans la colonne **Status**.

### Désactiver les règles d'alerte

Vous pouvez modifier l'état activé/désactivé pour une règle d'alerte par défaut ou personnalisée.

#### Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur web pris en charge](#)".
- Vous avez le "[Gérer les alertes ou l'autorisation d'accès racine](#)".

#### Description de la tâche

Lorsqu'une règle d'alerte est désactivée, ses expressions ne sont pas évaluées et aucune alerte n'est déclenchée.



En général, la désactivation d'une règle d'alerte par défaut n'est pas recommandée. Si une règle d'alerte est désactivée, vous risquez de ne pas détecter un problème sous-jacent tant qu'elle n'empêche pas l'exécution d'une opération critique.

#### Étapes

##### 1. Sélectionnez **ALERTES > règles**.

La page règles d'alerte s'affiche.

##### 2. Sélectionnez le bouton radio de la règle d'alerte que vous souhaitez désactiver ou activer.

##### 3. Sélectionnez **Modifier la règle**.

La boîte de dialogue Modifier la règle s'affiche.

##### 4. Cochez ou décochez la case **activé** pour déterminer si cette règle d'alerte est actuellement activée.

Si une règle d'alerte est désactivée, ses expressions ne sont pas évaluées et aucune alerte n'est déclenchée.



Si vous désactivez la règle d'alerte pour une alerte en cours, vous devez attendre quelques minutes que l'alerte ne s'affiche plus comme alerte active.

##### 5. Sélectionnez **Enregistrer**.

**Disabled** apparaît dans la colonne **Status**.

### Supprimez les règles d'alerte personnalisées

Vous pouvez supprimer une règle d'alerte personnalisée si vous ne souhaitez plus



l'utiliser.

### Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Gérer les alertes ou l'autorisation d'accès racine"](#).

### Étapes

1. Sélectionnez **ALERTES > règles**.

La page règles d'alerte s'affiche.

2. Sélectionnez le bouton radio de la règle d'alerte personnalisée que vous souhaitez supprimer.

Vous ne pouvez pas supprimer une règle d'alerte par défaut.

3. Sélectionnez **Supprimer la règle personnalisée**.

Une boîte de dialogue de confirmation s'affiche.

4. Sélectionnez **OK** pour supprimer la règle d'alerte.

Toutes les instances actives de l'alerte seront résolues dans un délai de 10 minutes.

### Gérer les notifications d'alerte

#### Configurez les notifications SNMP pour les alertes

Si vous souhaitez que StorageGRID envoie des notifications SNMP lorsque des alertes se produisent, vous devez activer l'agent SNMP StorageGRID et configurer une ou plusieurs destinations d'interruption.

Vous pouvez utiliser l'option **CONFIGURATION > surveillance > agent SNMP** dans le Gestionnaire de grille ou les noeuds finaux SNMP pour l'API de gestion de grille pour activer et configurer l'agent SNMP StorageGRID. L'agent SNMP prend en charge les trois versions du protocole SNMP.

Pour savoir comment configurer l'agent SNMP, reportez-vous à ["Utiliser la surveillance SNMP"](#) la section .

Après avoir configuré l'agent SNMP StorageGRID, deux types de notifications basées sur les événements peuvent être envoyées :

- Les interruptions sont des notifications envoyées par l'agent SNMP qui ne nécessitent pas d'accusé de réception par le système de gestion. Les interruptions servent à signaler au système de gestion qu'une alerte s'est produite au sein de StorageGRID, par exemple. Les traps sont pris en charge dans les trois versions de SNMP.
- Les informations sont similaires aux pièges, mais elles nécessitent une reconnaissance par le système de gestion. Si l'agent SNMP ne reçoit pas d'accusé de réception dans un certain temps, il renvoie l'information jusqu'à ce qu'un accusé de réception soit reçu ou que la valeur de nouvelle tentative maximale ait été atteinte. Les informations sont prises en charge dans SNMPv2c et SNMPv3.

Des notifications d'interruption et d'information sont envoyées lorsqu'une alerte par défaut ou personnalisée est déclenchée à n'importe quel niveau de gravité. Pour supprimer les notifications SNMP pour une alerte, vous devez configurer un silence pour l'alerte. Voir ["Notifications d'alerte de silence"](#).

Si votre déploiement StorageGRID inclut plusieurs nœuds d'administration, le nœud d'administration principal est l'expéditeur préféré pour les notifications d'alerte, les packages AutoSupport, les traps et les notifications SNMP. Si le nœud d'administration principal n'est plus disponible, les notifications sont envoyées temporairement par d'autres nœuds d'administration. Voir "[Qu'est-ce qu'un nœud d'administration ?](#)".

### Configurez les notifications par e-mail pour les alertes

Si vous souhaitez que des notifications par e-mail soient envoyées lorsque des alertes se produisent, vous devez fournir des informations sur votre serveur SMTP. Vous devez également saisir des adresses e-mail pour les destinataires des notifications d'alerte.

#### Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur web pris en charge](#)".
- Vous avez le "[Gérer les alertes ou l'autorisation d'accès racine](#)".

#### Description de la tâche

La configuration des e-mails utilisée pour les notifications d'alerte n'est pas utilisée pour les packages AutoSupport. Cependant, vous pouvez utiliser le même serveur de messagerie pour toutes les notifications.

Si votre déploiement StorageGRID inclut plusieurs nœuds d'administration, le nœud d'administration principal est l'expéditeur préféré pour les notifications d'alerte, les packages AutoSupport, les traps et les notifications SNMP. Si le nœud d'administration principal n'est plus disponible, les notifications sont envoyées temporairement par d'autres nœuds d'administration. Voir "[Qu'est-ce qu'un nœud d'administration ?](#)".

#### Étapes

1. Sélectionnez **ALERTE** > **Configuration de la messagerie**.

La page Configuration de l'e-mail s'affiche.

2. Cochez la case **Activer les notifications par e-mail** pour indiquer que vous souhaitez que les e-mails de notification soient envoyés lorsque les alertes atteignent des seuils configurés.

Les sections serveur d'e-mail (SMTP), sécurité de la couche de transport (TLS), adresses e-mail et filtres s'affichent.

3. Dans la section serveur de messagerie (SMTP), entrez les informations dont StorageGRID a besoin pour accéder à votre serveur SMTP.

Si votre serveur SMTP nécessite une authentification, vous devez fournir à la fois un nom d'utilisateur et un mot de passe.

Champ	Entrez
Serveur de messagerie	Nom de domaine complet (FQDN) ou adresse IP du serveur SMTP.
Port	Port utilisé pour accéder au serveur SMTP. Doit être compris entre 1 et 65535.
Nom d'utilisateur (facultatif)	Si votre serveur SMTP nécessite une authentification, entrez le nom d'utilisateur à authentifier.

Champ	Entrez
Mot de passe (facultatif)	Si votre serveur SMTP nécessite une authentification, entrez le mot de passe à authentifier auprès de.

4. Dans la section adresses e-mail, entrez les adresses e-mail de l'expéditeur et de chaque destinataire.
- Pour l'adresse électronique **expéditeur**, spécifiez une adresse e-mail valide à utiliser comme adresse de pour les notifications d'alerte.

Par exemple : `storagegrid-alerts@example.com`

- Dans la section destinataires, entrez une adresse e-mail pour chaque liste d'e-mails ou personne devant recevoir un e-mail lorsqu'une alerte se produit.

Sélectionnez l'icône plus **+** pour ajouter des destinataires.

5. Si transport Layer Security (TLS) est requis pour les communications avec le serveur SMTP, sélectionnez **exiger TLS** dans la section transport Layer Security (TLS).

- Dans le champ **certificat CA**, indiquez le certificat CA qui sera utilisé pour vérifier l'identification du serveur SMTP.

Vous pouvez copier et coller le contenu dans ce champ ou sélectionner **Parcourir** et sélectionner le fichier.

Vous devez fournir un seul fichier contenant les certificats de chaque autorité de certification intermédiaire (AC). Le fichier doit contenir chacun des fichiers de certificat d'autorité de certification codés au PEM, concaténés dans l'ordre de la chaîne de certificats.


- Cochez la case **Envoyer le certificat client** si votre serveur de messagerie SMTP requiert que les expéditeurs de courrier électronique fournissent des certificats client pour l'authentification.
- Dans le champ **certificat client**, fournissez le certificat client codé PEM à envoyer au serveur SMTP.

Vous pouvez copier et coller le contenu dans ce champ ou sélectionner **Parcourir** et sélectionner le fichier.

- Dans le champ **Private Key**, saisissez la clé privée du certificat client dans le codage PEM non chiffré.

Vous pouvez copier et coller le contenu dans ce champ ou sélectionner **Parcourir** et sélectionner le fichier.



Si vous devez modifier la configuration de la messagerie, sélectionnez l'icône représentant un crayon  pour mettre à jour ce champ.

6. Dans la section filtres, sélectionnez les niveaux de gravité des alertes qui doivent donner lieu à des notifications par e-mail, sauf si la règle d'une alerte spécifique a été mise en silence.

Gravité	Description
Mineur, majeur, critique	Une notification par e-mail est envoyée lorsque la condition mineure, majeure ou critique d'une règle d'alerte est remplie.

Gravité	Description
Important, critique	Une notification par e-mail est envoyée lorsque la condition principale ou critique d'une règle d'alerte est remplie. Les notifications ne sont pas envoyées pour les alertes mineures.
Critique uniquement	Une notification par e-mail est envoyée uniquement lorsque la condition critique d'une règle d'alerte est remplie. Les notifications ne sont pas envoyées pour les alertes mineures ou majeures.

7. Lorsque vous êtes prêt à tester vos paramètres de messagerie, procédez comme suit :

a. Sélectionnez **Envoyer e-mail test**.

Un message de confirmation s'affiche, indiquant qu'un e-mail de test a été envoyé.

b. Cochez les cases de tous les destinataires d'e-mail et confirmez qu'un e-mail de test a été reçu.



Si l'e-mail n'est pas reçu dans quelques minutes ou si l'alerte **échec de notification par e-mail** est déclenchée, vérifiez vos paramètres et réessayez.

c. Connectez-vous à tout autre nœud d'administration et envoyez un e-mail de test pour vérifier la connectivité de tous les sites.



Lorsque vous testez les notifications d'alertes, vous devez vous connecter à chaque nœud d'administration pour vérifier la connectivité. Cela contraste avec les tests de packages AutoSupport, où tous les nœuds d'administration envoient l'e-mail de test.

8. Sélectionnez **Enregistrer**.

L'envoi d'un e-mail de test n'enregistre pas vos paramètres. Vous devez sélectionner **Enregistrer**.

Les paramètres de messagerie sont enregistrés.

### Informations incluses dans les notifications par e-mail d'alerte

Après avoir configuré le serveur de messagerie SMTP, des notifications par e-mail sont envoyées aux destinataires désignés lorsqu'une alerte est déclenchée, à moins que la règle d'alerte ne soit supprimée par un silence. Voir "[Notifications d'alerte de silence](#)".

Les notifications par e-mail incluent les informations suivantes :

## Low object data storage (6 alerts) 1

The space available for storing object data is low. 2

### Recommended actions 3

Perform an expansion procedure. You can add storage volumes (LUNs) to existing Storage Nodes, or you can add new Storage Nodes. See the instructions for expanding a StorageGRID system.

DC1-S1-226

**Node** DC1-S1-226 4  
**Site** DC1 225-230  
**Severity** Minor  
**Time triggered** Fri Jun 28 14:43:27 UTC 2019  
**Job** storagegrid  
**Service** ldr

DC1-S2-227

**Node** DC1-S2-227  
**Site** DC1 225-230  
**Severity** Minor  
**Time triggered** Fri Jun 28 14:43:27 UTC 2019  
**Job** storagegrid  
**Service** ldr

Sent from: DC1-ADM1-225 5

Légende	Description
1	Nom de l'alerte, suivi du nombre d'instances actives de cette alerte.
2	Description de l'alerte.
3	Toutes les actions recommandées pour l'alerte.
4	Détails sur chaque instance active de l'alerte, y compris le nœud et le site affectés, la gravité de l'alerte, l'heure UTC au moment où la règle d'alerte a été déclenchée, ainsi que le nom du travail et du service affectés.
5	Nom d'hôte du nœud d'administration qui a envoyé la notification.

### Mode de regroupement des alertes

Pour empêcher l'envoi d'un nombre excessif de notifications par e-mail lorsque des alertes sont déclenchées, StorageGRID tente de regrouper plusieurs alertes dans la même notification.

Reportez-vous au tableau suivant pour obtenir des exemples de la manière dont StorageGRID regroupe plusieurs alertes dans les notifications par e-mail.

Comportement	Exemple
<p>Chaque notification d'alerte s'applique uniquement aux alertes portant le même nom. Si deux alertes avec des noms différents sont déclenchées en même temps, deux notifications par e-mail sont envoyées.</p>	<ul style="list-style-type: none"> <li>• L'alerte A est déclenchée en même temps sur deux nœuds. Une seule notification est envoyée.</li> <li>• L'alerte A est déclenchée sur le nœud 1 et l'alerte B est déclenchée simultanément sur le nœud 2. Deux notifications sont envoyées : une pour chaque alerte.</li> </ul>
<p>Pour une alerte spécifique sur un nœud spécifique, si les seuils sont atteints pour plus d'un degré de sévérité, une notification est envoyée uniquement pour l'alerte la plus grave.</p>	<ul style="list-style-type: none"> <li>• L'alerte A est déclenchée et le seuil d'alerte secondaire, majeur et critique est atteint. Une notification est envoyée pour l'alerte critique.</li> </ul>
<p>La première fois qu'une alerte est déclenchée, StorageGRID attend 2 minutes avant d'envoyer une notification. Si d'autres alertes du même nom sont déclenchées pendant ce temps, StorageGRID regroupe toutes les alertes de la notification initiale.</p>	<ol style="list-style-type: none"> <li>1. L'alerte A est déclenchée sur le nœud 1 à 08:00. Aucune notification n'a été envoyée.</li> <li>2. L'alerte A est déclenchée sur le nœud 2 à 08:01. Aucune notification n'a été envoyée.</li> <li>3. À 08 h 02, une notification est envoyée pour signaler les deux instances de l'alerte.</li> </ol>
<p>Si une autre alerte du même nom est déclenchée, StorageGRID attend 10 minutes avant d'envoyer une nouvelle notification. La nouvelle notification signale toutes les alertes actives (alertes en cours qui n'ont pas été désactivées), même si elles ont été signalées précédemment.</p>	<ol style="list-style-type: none"> <li>1. L'alerte A est déclenchée sur le nœud 1 à 08:00. Une notification est envoyée à 08:02.</li> <li>2. L'alerte A est déclenchée sur le nœud 2 à 08:05. Une seconde notification est envoyée à 08:15 (10 minutes plus tard). Les deux nœuds sont signalés.</li> </ol>
<p>Si plusieurs alertes en cours portent le même nom et que l'une de ces alertes est résolue, une nouvelle notification n'est pas envoyée si l'alerte se reproduit sur le nœud pour lequel l'alerte a été résolue.</p>	<ol style="list-style-type: none"> <li>1. L'alerte A est déclenchée pour le nœud 1. Une notification est envoyée.</li> <li>2. L'alerte A est déclenchée pour le nœud 2. Une seconde notification est envoyée.</li> <li>3. L'alerte A est résolue pour le nœud 2, mais elle reste active pour le nœud 1.</li> <li>4. L'alerte A est à nouveau déclenchée pour le nœud 2. Aucune nouvelle notification n'est envoyée, car l'alerte est toujours active pour le nœud 1.</li> </ol>
<p>StorageGRID continue à envoyer des notifications par e-mail tous les 7 jours jusqu'à ce que toutes les instances de l'alerte soient résolues ou que la règle d'alerte soit désactivée.</p>	<ol style="list-style-type: none"> <li>1. L'alerte A est déclenchée pour le nœud 1 le 8 mars. Une notification est envoyée.</li> <li>2. L'alerte A n'est pas résolue ou arrêtée. Des notifications supplémentaires sont envoyées le 15 mars, le 22 mars, le 29 mars, etc.</li> </ol>

## Dépanner les notifications d'alerte par e-mail

Si l'alerte **échec de notification par e-mail** est déclenchée ou si vous ne parvenez pas à recevoir la notification par e-mail d'alerte de test, procédez comme suit pour résoudre le problème.

### Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Gérer les alertes ou l'autorisation d'accès racine"](#).

### Étapes

1. Vérifiez vos paramètres.
  - a. Sélectionnez **ALERTES > Configuration de la messagerie**.
  - b. Vérifiez que les paramètres du serveur de messagerie (SMTP) sont corrects.
  - c. Vérifiez que vous avez spécifié des adresses e-mail valides pour les destinataires.
2. Vérifiez votre filtre de spam et assurez-vous que l'e-mail n'a pas été envoyé à un dossier indésirable.
3. Demandez à votre administrateur de messagerie de confirmer que les e-mails de l'adresse de l'expéditeur ne sont pas bloqués.
4. Collectez un fichier journal pour le nœud d'administration, puis contactez le support technique.

Le support technique peut utiliser les informations contenues dans les journaux pour vous aider à déterminer ce qui s'est mal passé. Par exemple, le fichier prometheus.log peut afficher une erreur lors de la connexion au serveur spécifié.

Voir ["Collecte de fichiers journaux et de données système"](#).

### Notifications d'alerte de silence

Si vous le souhaitez, vous pouvez configurer des silences pour supprimer temporairement les notifications d'alerte.

### Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Gérer les alertes ou l'autorisation d'accès racine"](#).

### Description de la tâche

Vous pouvez désactiver les règles d'alerte sur toute la grille, sur un seul site ou sur un seul nœud et pour une ou plusieurs niveaux de gravité. Chaque silence supprime toutes les notifications d'une règle d'alerte unique ou de toutes les règles d'alerte.

Si vous avez activé l'agent SNMP, les silences suppriment également les interruptions SNMP et informent.



Soyez prudent lorsque vous décidez de désactiver une règle d'alerte. Si vous neutralisez une alerte, il est possible que vous ne détectez pas un problème sous-jacent tant qu'elle n'empêche pas l'exécution d'une opération critique.

### Étapes

1. Sélectionnez **ALERTES > silences**.

La page silences s'affiche.

## Silences

You can configure silences to temporarily suppress alert notifications. Each silence suppresses the notifications for an alert rule at one or more severities. You can suppress an alert rule on the entire grid, a single site, or a single node.

+ Create Edit Remove

Alert Rule	Description	Severity	Time Remaining	Nodes
<i>No results found.</i>				

### 2. Sélectionnez **Créer**.

La boîte de dialogue Créer une Silence s'affiche.

### Create Silence

Alert Rule

Description (optional)

Duration

Severity  Minor only  Minor, major  Minor, major, critical

Nodes

- StorageGRID Deployment
  - Data Center 1
    - DC1-ADM1
    - DC1-G1
    - DC1-S1
    - DC1-S2
    - DC1-S3

### 3. Sélectionnez ou entrez les informations suivantes :

Champ	Description
Règle d'alerte	<p>Le nom de la règle d'alerte que vous souhaitez désactiver. Vous pouvez sélectionner n'importe quelle règle d'alerte par défaut ou personnalisée, même si la règle d'alerte est désactivée.</p> <p><b>Remarque :</b> sélectionnez <b>toutes les règles</b> si vous voulez désactiver toutes les règles d'alerte en utilisant les critères spécifiés dans cette boîte de dialogue.</p>



Champ	Description
Description	Éventuellement, une description du silence. Par exemple, décrivez le but de ce silence.
Durée	Combien de temps vous voulez que ce silence reste en vigueur, en minutes, heures ou jours. Un silence peut être en vigueur de 5 minutes à 1,825 jours (5 ans).  <b>Remarque:</b> vous ne devez pas désactiver une règle d'alerte pour une durée prolongée. Si une règle d'alerte est mise en mode silencieux, il est possible que vous ne détectiez pas un problème sous-jacent tant qu'elle n'empêche pas l'exécution d'une opération critique. Cependant, vous devrez peut-être utiliser un silence étendu si une alerte est déclenchée par une configuration intentionnelle spécifique, par exemple pour les alertes <b>liaison appliance Services Down</b> et les alertes <b>liaison appliance Storage Down</b> .
Gravité	Quelle alerte de gravité ou de gravité doit être neutralisée. Si l'alerte est déclenchée à l'un des niveaux de gravité sélectionnés, aucune notification n'est envoyée.
Nœuds	À quel nœud ou nœud vous souhaitez que ce silence s'applique. Vous pouvez supprimer une règle d'alerte ou toutes les règles de la grille dans son ensemble, un seul site ou un seul nœud. Si vous sélectionnez l'ensemble de la grille, le silence s'applique à tous les sites et à tous les nœuds. Si vous sélectionnez un site, le silence s'applique uniquement aux nœuds de ce site.  <b>Note:</b> vous ne pouvez pas sélectionner plus d'un nœud ou plus d'un site pour chaque silence. Vous devez créer des silences supplémentaires si vous souhaitez supprimer la même règle d'alerte sur plusieurs nœuds ou plusieurs sites à la fois.

4. Sélectionnez **Enregistrer**.

5. Si vous souhaitez modifier ou mettre fin à un silence avant son expiration, vous pouvez le modifier ou le supprimer.

Option	Description
Modifier un silence	<ol style="list-style-type: none"> <li>Sélectionnez <b>ALERTE &gt; silences</b>.</li> <li>Dans le tableau, sélectionnez le bouton radio correspondant au silence que vous souhaitez modifier.</li> <li>Sélectionnez <b>Modifier</b>.</li> <li>Modifiez la description, le temps restant, les niveaux de gravité sélectionnés ou le nœud affecté.</li> <li>Sélectionnez <b>Enregistrer</b>.</li> </ol>

Option	Description
Supprimer un silence	<p>a. Sélectionnez <b>ALERTE</b> &gt; <b>silences</b>.</p> <p>b. Dans le tableau, sélectionnez le bouton radio correspondant au silence que vous souhaitez supprimer.</p> <p>c. Sélectionnez <b>Supprimer</b>.</p> <p>d. Sélectionnez <b>OK</b> pour confirmer que vous souhaitez supprimer ce silence.</p> <p><b>Remarque</b> : les notifications sont maintenant envoyées lorsque cette alerte est déclenchée (sauf si elle est supprimée par un autre silence). Si cette alerte est déclenchée, l'envoi de notifications par e-mail ou SNMP peut prendre quelques minutes et la mise à jour de la page alertes.</p>

### Informations associées

["Configurez l'agent SNMP"](#)

### Référence des alertes

Cette référence répertorie les alertes par défaut qui apparaissent dans le Gestionnaire de grille. Les actions recommandées sont dans le message d'alerte que vous recevez.

Si nécessaire, vous pouvez créer des règles d'alerte personnalisées en fonction de votre approche de gestion du système.

Certaines alertes par défaut utilisent ["Metrics Prometheus"](#).

### Alertes de l'appliance

Nom de l'alerte	Description
Batterie de l'appareil expirée	La batterie du contrôleur de stockage de l'appareil a expiré.
La batterie de l'appareil est défectueuse	La batterie du contrôleur de stockage de l'appareil est défectueuse.
La capacité de la batterie de l'appareil est insuffisante	La capacité de la batterie du contrôleur de stockage de l'appareil est insuffisante.
La batterie de l'appareil est presque déchargée	La batterie du contrôleur de stockage de l'appliance arrive à expiration.
Batterie de l'appareil retirée	La batterie du contrôleur de stockage de l'appareil est manquante.
Batterie de l'appareil trop chaude	La batterie du contrôleur de stockage de l'appareil est en surchauffe.
Erreur de communication du BMC de l'appliance	La communication avec le contrôleur de gestion de la carte mère (BMC) a été perdue.

Nom de l'alerte	Description
Erreur de périphérique d'amorçage de l'apppliance détectée	Un problème a été détecté au niveau du périphérique d'amorçage de l'appareil.
Échec du périphérique de sauvegarde du cache de l'apppliance	Échec d'un périphérique de sauvegarde de cache persistant.
Capacité insuffisante du périphérique de sauvegarde en cache de l'apppliance	La capacité du périphérique de sauvegarde du cache est insuffisante.
Dispositif de sauvegarde cache de l'apppliance protégé en écriture	Un périphérique de sauvegarde de cache est protégé en écriture.
La taille de la mémoire cache de l'apppliance ne correspond pas	Le cache des deux contrôleurs de l'apppliance est de différentes tailles.
Défaillance de la pile CMOS de l'appareil	Un problème a été détecté au niveau de la pile CMOS de l'appareil.
La température du châssis du contrôleur de calcul de l'apppliance est trop élevée	La température du contrôleur de calcul d'une appliance StorageGRID a dépassé le seuil nominal.
Température trop élevée du processeur du contrôleur de calcul de l'apppliance	La température du processeur dans le contrôleur de calcul d'une appliance StorageGRID a dépassé le seuil nominal.
Le contrôleur de calcul de l'apppliance doit faire attention	Une défaillance matérielle a été détectée dans le contrôleur de calcul d'une appliance StorageGRID.
L'alimentation A du contrôleur de calcul de l'apppliance présente un problème	L'alimentation A du contrôleur de calcul présente un problème.
L'alimentation B du contrôleur de calcul de l'apppliance présente un problème	L'alimentation B du contrôleur de calcul présente un problème.
Service de surveillance du matériel de calcul de l'apppliance bloqué	Le service qui surveille l'état du matériel de stockage est bloqué.
Disques DAS du dispositif dépassant la limite pour les données écrites par jour	Une quantité excessive de données est écrite sur un disque chaque jour, ce qui pourrait annuler sa garantie.

<b>Nom de l'alerte</b>	<b>Description</b>
Panne du lecteur DAS de l'appliance détectée	Un problème a été détecté au niveau d'un disque DAS (Direct-Attached Storage) dans l'appliance.
Le voyant de localisation du dispositif DAS est allumé	Le voyant de localisation de lecteur d'un ou plusieurs disques DAS (Direct-Attached Storage Node) d'un nœud de stockage d'appliance est allumé.
Reconstruction des disques DAS du dispositif	Un disque DAS (Direct-Attached Storage) est en cours de reconstruction. Ceci est attendu s'il a été récemment remplacé ou supprimé/réinséré.
Panne du ventilateur de l'appareil détectée	Un problème de ventilateur dans l'appareil a été détecté.
Panne Fibre Channel de l'appliance détectée	Un problème de liaison Fibre Channel a été détecté entre le contrôleur de stockage de l'appliance et le contrôleur de calcul
Défaillance du port HBA Fibre Channel de l'appliance	Un port HBA Fibre Channel est défectueux ou est défectueux.
Flash cache de l'appliance ne sont pas optimaux	Les disques utilisés pour la mise en cache SSD ne sont pas optimaux.
Interconnexion de l'appareil/boîtier de la batterie retiré	Le boîtier d'interconnexion/de batterie est manquant.
Port d'appliance LACP manquant	Aucun port d'une appliance StorageGRID ne participe au lien LACP.
Défaillance de la carte réseau de l'appareil détectée	Un problème de carte d'interface réseau (NIC) a été détecté sur le serveur.
L'alimentation générale de l'appareil est dégradée	La puissance d'un dispositif StorageGRID s'est déviée de la tension de fonctionnement recommandée.
Avertissement critique sur les disques SSD de l'appliance	Un SSD d'appliance signale un avertissement critique.
Défaillance Du contrôleur de stockage De l'appliance	Le contrôleur de stockage A d'une appliance StorageGRID est en panne.
Défaillance du contrôleur B de stockage de l'appliance	Le contrôleur de stockage B d'une appliance StorageGRID est en panne.
Panne de disque du contrôleur de stockage de l'appliance	Un ou plusieurs disques d'une appliance StorageGRID sont défectueux ou non optimaux.

Nom de l'alerte	Description
Problème matériel du contrôleur de stockage de l'appliance	Le logiciel SANtricity signale les besoins d'attention d'un composant d'une appliance StorageGRID.
Panne de l'alimentation Du contrôleur de stockage de l'appliance	L'alimentation A d'un dispositif StorageGRID s'est déviée de la tension de fonctionnement recommandée.
Panne de l'alimentation B du contrôleur de stockage de l'appliance	L'alimentation B d'un dispositif StorageGRID s'est déviée de la tension de fonctionnement recommandée.
Entretien du moniteur matériel de stockage de l'appliance bloqué	Le service qui surveille l'état du matériel de stockage est bloqué.
Dégradation des tiroirs de stockage de l'appliance	L'état de l'un des composants du tiroir de stockage d'une appliance de stockage est dégradé.
Température de l'appareil dépassée	La température nominale ou maximale du contrôleur de stockage de l'appareil a été dépassée.
Capteur de température de l'appareil retiré	Un capteur de température a été déposé.
Erreur d'amorçage sécurisé UEFI de l'appliance	Un appareil n'a pas été correctement démarré.
Les E/S du disque sont très lentes	Les E/S de disque très lentes peuvent affecter les performances du grid.
Panne du ventilateur du dispositif de stockage détectée	Un problème de ventilateur dans le contrôleur de stockage d'un dispositif a été détecté.
Dégradation de la connectivité du stockage de l'appliance de stockage	Un problème se produit au niveau d'une ou plusieurs connexions entre le contrôleur de calcul et le contrôleur de stockage.
Périphérique de stockage inaccessible	Impossible d'accéder à un périphérique de stockage.

#### Alertes d'audit et syslog

Nom de l'alerte	Description
Des journaux d'audit sont ajoutés à la file d'attente en mémoire	Le nœud ne peut pas envoyer de journaux au serveur syslog local et la file d'attente in-memory est en cours de remplissage.

Nom de l'alerte	Description
Erreur de transfert du serveur syslog externe	Le nœud ne peut pas transférer les journaux vers le serveur syslog externe.
Grande file d'attente d'audit	La file d'attente des messages d'audit est pleine. Si cette condition n'est pas résolue, les opérations S3 ou Swift risquent d'échouer.
Des journaux sont ajoutés à la file d'attente sur disque	Le nœud ne peut pas transférer les journaux vers le serveur syslog externe et la file d'attente sur disque est en cours de chargement.

#### Alertes de compartiment

Nom de l'alerte	Description
Le paramètre de cohérence du compartiment FabricPool n'est pas pris en charge	Un compartiment FabricPool utilise le niveau de cohérence disponible ou élevé des sites, ce qui n'est pas pris en charge.
Le compartiment FabricPool possède un paramètre de gestion des versions non pris en charge	La gestion des versions ou le verrouillage d'objet S3 d'un compartiment FabricPool est activé, ce qui n'est pas pris en charge.

#### Alertes Cassandra

Nom de l'alerte	Description
Erreur du compacteur automatique Cassandra	Le compacteur automatique Cassandra a rencontré une erreur.
Indicateurs du compacteur automatique Cassandra obsolètes	Les mesures qui décrivent le compacteur automatique Cassandra sont obsolètes.
Erreur de communication Cassandra	Les nœuds qui exécutent le service Cassandra rencontrent des problèmes.
Compression Cassandra surchargée	Le processus de compactage Cassandra est surchargé.
Erreur d'écriture surdimensionnée Cassandra	Un processus StorageGRID interne a envoyé à Cassandra une demande d'écriture trop volumineuse.
Les metrics de réparation de Cassandra sont obsolètes	Les mesures qui décrivent les tâches de réparation de Cassandra sont obsolètes.
La progression de la réparation de Cassandra est lente	La progression des réparations des bases de données Cassandra est lente.

Nom de l'alerte	Description
Le service de réparation Cassandra n'est pas disponible	Le service de réparation Cassandra n'est pas disponible.
La corruption des tables Cassandra	Cassandra a détecté une corruption de table. Cassandra redémarre automatiquement si elle détecte une corruption de la table.

#### Alertes de pool de stockage cloud

Nom de l'alerte	Description
Erreur de connectivité de Cloud Storage Pool	Le contrôle de l'état des pools de stockage cloud a détecté une ou plusieurs nouvelles erreurs.
IAM Roles Anywhere expiration de la certification d'entité finale	Le certificat d'entité finale IAM Roles Anywhere va expirer.

#### Alertes de réplication intergrid

Nom de l'alerte	Description
Défaillance permanente de la réplication entre les grilles	Une erreur de réplication inter-grille s'est produite et nécessite une intervention de l'utilisateur pour la résoudre.
Ressources de réplication intergrid indisponibles	Les demandes de réplication multigrille sont en attente car une ressource n'est pas disponible.

#### Alertes DHCP

Nom de l'alerte	Description
Bail DHCP expiré	Le bail DHCP sur une interface réseau a expiré.
La location DHCP expire bientôt	Le bail DHCP sur une interface réseau expire bientôt.
Serveur DHCP indisponible	Le serveur DHCP n'est pas disponible.

#### Alertes de débogage et de suivi

Nom de l'alerte	Description
Impact sur les performances de débogage	Lorsque le mode débogage est activé, les performances du système peuvent être affectées négativement.
Configuration de trace activée	Lorsque la configuration de trace est activée, les performances du système peuvent être affectées de façon négative.

## Alertes par e-mail et AutoSupport

Nom de l'alerte	Description
Échec de l'envoi du message AutoSupport	L'envoi du message AutoSupport le plus récent a échoué.
Échec de la résolution du nom de domaine	Le nœud StorageGRID n'a pas pu résoudre les noms de domaine.
Échec de la notification par e-mail	Impossible d'envoyer la notification par e-mail pour une alerte.
Erreurs d'information SNMP	Erreurs lors de l'envoi de notifications d'information SNMP à une destination d'interruption.
Connexion SSH ou console détectée	Au cours des 24 dernières heures, un utilisateur s'est connecté à la console Web ou à SSH.

## Alertes de code d'effacement (EC)

Nom de l'alerte	Description
Défaillance du rééquilibrage EC	La procédure de rééquilibrage EC a échoué ou a été arrêtée.
Échec de réparation EC	Une tâche de réparation pour les données EC a échoué ou a été arrêtée.
Réparation EC bloquée	Un travail de réparation pour les données EC est bloqué.
Erreur de vérification de fragment avec code d'effacement	Les fragments avec code d'effacement ne peuvent plus être vérifiés. Des fragments corrompus peuvent ne pas être réparés.

## Expiration des alertes de certificats

Nom de l'alerte	Description
Expiration du certificat de l'autorité de certification du proxy d'administration	Un ou plusieurs certificats du paquet CA du serveur proxy d'administration sont sur le point d'expirer.
Expiration du certificat client	Un ou plusieurs certificats client sont sur le point d'expirer.
Expiration du certificat de serveur global pour S3 et Swift	Le certificat de serveur global pour S3 et Swift est sur le point d'expirer.
Expiration du certificat de point final de l'équilibreur de charge	Un ou plusieurs certificats de nœud final de l'équilibreur de charge vont expirer.



Nom de l'alerte	Description
Expiration du certificat de serveur pour l'interface de gestion	Le certificat de serveur utilisé pour l'interface de gestion est sur le point d'expirer.
Expiration du certificat d'autorité de certification syslog externe	Le certificat d'autorité de certification (CA) utilisé pour signer le certificat de serveur syslog externe est sur le point d'expirer.
Expiration du certificat du client syslog externe	Le certificat client d'un serveur syslog externe est sur le point d'expirer.
Expiration du certificat du serveur syslog externe	Le certificat de serveur présenté par le serveur syslog externe arrive à expiration.

#### Alertes réseau Grid

Nom de l'alerte	Description
Non-concordance de MTU du réseau de grid	Le paramètre MTU de l'interface réseau Grid (eth0) diffère de manière significative sur tous les nœuds de la grille.

#### Alertes de fédération du grid

Nom de l'alerte	Description
Expiration du certificat de fédération GRID	Un ou plusieurs certificats de fédération de grille sont sur le point d'expirer.
Échec de la connexion de fédération de grille	La connexion de fédération de grille entre la grille locale et la grille distante ne fonctionne pas.

#### Alertes d'utilisation élevée ou de latence élevée

Nom de l'alerte	Description
Utilisation du segment de mémoire Java élevée	Un pourcentage élevé d'espace de tas Java est utilisé.
Latence élevée pour les requêtes de métadonnées	La durée moyenne des requêtes de métadonnées Cassandra est trop longue.

#### Alertes de fédération des identités

Nom de l'alerte	Description
Échec de synchronisation de la fédération d'identités	Impossible de synchroniser des groupes fédérés et des utilisateurs à partir du référentiel d'identité.

Nom de l'alerte	Description
Échec de la synchronisation de la fédération des identités pour un locataire	Impossible de synchroniser les groupes fédérés et les utilisateurs à partir du référentiel d'identité configuré par un locataire.

#### Alertes de gestion du cycle de vie des informations (ILM)

Nom de l'alerte	Description
Placement ILM impossible à atteindre	Une instruction de placement dans une règle ILM ne peut pas être obtenue pour certains objets.
Taux d'analyse ILM faible	La vitesse d'analyse ILM est définie sur moins de 100 objets/seconde.

#### Alertes du serveur de gestion des clés (KMS)

Nom de l'alerte	Description
Expiration du certificat CA KMS	Le certificat de l'autorité de certification (CA) utilisé pour signer le certificat du serveur de gestion des clés (KMS) est sur le point d'expirer.
Expiration du certificat client KMS	Le certificat client d'un serveur de gestion des clés est sur le point d'expirer
Echec du chargement de la configuration DES KMS	La configuration du serveur de gestion des clés existe mais n'a pas pu être chargée.
Erreur de connectivité KMS	Un nœud d'appliance n'a pas pu se connecter au serveur de gestion des clés de son site.
Nom de la clé de cryptage KMS introuvable	Le serveur de gestion des clés configuré ne dispose pas d'une clé de chiffrement correspondant au nom fourni.
Echec de la rotation de la clé de chiffrement KMS	Tous les volumes de l'appliance ont été déchiffrés avec succès, mais un ou plusieurs volumes n'ont pas pu tourner vers la clé la plus récente.
LES KMS ne sont pas configurés	Aucun serveur de gestion des clés n'existe pour ce site.
La clé KMS n'a pas réussi à déchiffrer un volume d'appliance	Impossible de déchiffrer un ou plusieurs volumes sur une appliance dont le chiffrement de nœud est activé avec la clé KMS actuelle.
Expiration du certificat du serveur KMS	Le certificat de serveur utilisé par le serveur de gestion des clés (KMS) est sur le point d'expirer.
Echec de la connectivité du serveur KM	Un nœud d'appliance n'a pas pu se connecter à un ou plusieurs serveurs du cluster de serveurs de gestion des clés pour son site.

## Alertes d'équilibrage de la charge

Nom de l'alerte	Description
Des connexions élevées d'équilibreur de charge sans demande	Pourcentage élevé de connexions aux terminaux de l'équilibreur de charge déconnectés sans effectuer de requêtes.

## Alertes de décalage d'horloge locale

Nom de l'alerte	Description
Décalage horaire grand horloge locale	Le décalage entre l'horloge locale et l'heure NTP (Network Time Protocol) est trop important.

## Alertes de mémoire insuffisante ou d'espace insuffisant

Nom de l'alerte	Description
Capacité du disque du journal d'audit faible	L'espace disponible pour les journaux d'audit est faible. Si cette condition n'est pas résolue, les opérations S3 ou Swift risquent d'échouer.
Mémoire de nœud faible disponibilité	La quantité de RAM disponible sur un nœud est faible.
Faible espace libre pour le pool de stockage	L'espace disponible pour le stockage des données d'objet dans le nœud de stockage est faible.
Mémoire insuffisante sur les nœuds installés	La quantité de mémoire installée sur un nœud est faible.
Faibles capacités de stockage de métadonnées	L'espace disponible pour le stockage des métadonnées d'objet est faible.
Capacité disque de metrics faible	L'espace disponible pour la base de données de metrics est faible.
Faible stockage des données objet	L'espace disponible pour le stockage des données d'objet est faible.
Remplacement du filigrane en lecture seule faible	Le remplacement du filigrane en lecture seule souple du volume de stockage est inférieur au filigrane optimisé minimum pour un nœud de stockage.
Capacité du disque racine faible	L'espace disponible sur le disque racine est faible.
Faible capacité des données système	L'espace disponible pour /var/local est faible. Si cette condition n'est pas résolue, les opérations S3 ou Swift risquent d'échouer.

Nom de l'alerte	Description
Petit répertoire tmp espace libre	L'espace disponible dans le répertoire /tmp est faible.

#### Alertes de réseau de nœuds ou de nœuds

Nom de l'alerte	Description
Utilisation de la réception du réseau d'administration	L'utilisation de la réception sur le réseau d'administration est élevée.
Admin utilisation de la transmission réseau	L'utilisation de la transmission sur le réseau d'administration est élevée.
Échec de la configuration du pare-feu	Impossible d'appliquer la configuration du pare-feu.
Noeuds finaux de l'interface de gestion en mode de secours	Tous les terminaux de l'interface de gestion reviennent aux ports par défaut depuis trop longtemps.
Erreur de connectivité réseau du nœud	Des erreurs se sont produites lors du transfert des données entre les nœuds.
Erreur de trame de réception du réseau du nœud	Un pourcentage élevé des trames réseau reçues par un nœud a rencontré des erreurs.
Nœud non synchronisé avec le serveur NTP	Le nœud n'est pas synchronisé avec le serveur NTP (Network Time Protocol).
Nœud non verrouillé avec le serveur NTP	Le nœud n'est pas verrouillé sur un serveur NTP (Network Time Protocol).
Réseau de nœuds non appliances arrêté	Un ou plusieurs périphériques réseau sont en panne ou déconnectés.
Liaison de l'appliance de services vers le réseau d'administration	L'interface de l'appliance vers le réseau d'administration (eth1) est en panne ou déconnectée.
Interruption de la liaison de l'appliance de services sur le port réseau d'administration 1	Le port réseau Admin 1 de l'appliance est arrêté ou déconnecté.
Liaison de l'appliance de services vers le réseau client	L'interface de l'appliance vers le réseau client (eth2) est en panne ou déconnectée.
La liaison de l'appliance de services est inactive sur le port réseau 1	Le port réseau 1 de l'appliance est en panne ou déconnecté.

Nom de l'alerte	Description
La liaison de l'appliance de services est inactive sur le port réseau 2	Le port réseau 2 de l'appliance est en panne ou déconnecté.
La liaison de l'appliance de services est inactive sur le port réseau 3	Le port réseau 3 de l'appliance est en panne ou déconnecté.
La liaison de l'appliance de services est inactive sur le port réseau 4	Le port réseau 4 de l'appliance est en panne ou déconnecté.
Liaison de l'appliance de stockage indisponible sur le réseau d'administration	L'interface de l'appliance vers le réseau d'administration (eth1) est en panne ou déconnectée.
Liaison du dispositif de stockage inactive sur le port réseau d'administration 1	Le port réseau Admin 1 de l'appliance est arrêté ou déconnecté.
La liaison de l'appliance de stockage sur le réseau client est inactive	L'interface de l'appliance vers le réseau client (eth2) est en panne ou déconnectée.
La liaison du dispositif de stockage est inactive sur le port réseau 1	Le port réseau 1 de l'appliance est en panne ou déconnecté.
La liaison du dispositif de stockage est inactive sur le port réseau 2	Le port réseau 2 de l'appliance est en panne ou déconnecté.
La liaison du dispositif de stockage est inactive sur le port réseau 3	Le port réseau 3 de l'appliance est en panne ou déconnecté.
La liaison du dispositif de stockage est inactive sur le port réseau 4	Le port réseau 4 de l'appliance est en panne ou déconnecté.
Le nœud de stockage n'est pas dans l'état de stockage souhaité	Le service LDR d'un nœud de stockage ne peut pas passer à l'état souhaité en raison d'une erreur interne ou d'un problème lié au volume
Utilisation de la connexion TCP	Le nombre de connexions TCP sur ce nœud est proche du nombre maximal de connexions pouvant être suivies.
Impossible de communiquer avec le nœud	Un ou plusieurs services ne répondent pas, ou le nœud ne peut pas être atteint.

Nom de l'alerte	Description
Redémarrage de nœud inattendu	Un nœud a été redémarré de manière inattendue au cours des 24 dernières heures.

#### Alertes sur les objets

Nom de l'alerte	Description
Échec de la vérification de l'existence de l'objet	Le travail de vérification de l'existence de l'objet a échoué.
La vérification de l'existence d'objet est bloquée	Le travail de vérification de l'existence de l'objet est bloqué.
Objets perdus	Un ou plusieurs objets ont été perdus de la grille.
S3 PLACEZ la taille de l'objet trop grande	Un client tente une opération PUT Object qui dépasse les limites de taille S3.
Objet corrompu non identifié détecté	Un fichier a été trouvé dans le stockage objet répliqué qui n'a pas pu être identifié en tant qu'objet répliqué.

#### Alertes de services de plateforme

Nom de l'alerte	Description
Capacité des demandes en attente des services de plateforme faible	Le nombre de demandes de services de plateforme en attente approche de la capacité.
Services de plateforme non disponibles	Trop peu de nœuds de stockage avec le service RSM sont en cours d'exécution ou disponibles sur un site.

#### Alertes de volume de stockage

Nom de l'alerte	Description
Le volume de stockage nécessite votre attention	Un volume de stockage est hors ligne et nécessite votre attention.
Le volume de stockage doit être restauré	Un volume de stockage a été restauré et doit être restauré.
Volume de stockage hors ligne	Un volume de stockage est hors ligne depuis plus de 5 minutes.
Tentative de remontage du volume de stockage	Un volume de stockage a été hors ligne et a déclenché un remontage automatique. Cela peut indiquer un problème de lecteur ou des erreurs de système de fichiers.

Nom de l'alerte	Description
La restauration de volume n'a pas pu démarrer la réparation des données répliquées	La réparation des données répliquées pour un volume réparé n'a pas pu être démarrée automatiquement.

#### Alertes des services StorageGRID

Nom de l'alerte	Description
service nginx utilisant la configuration de sauvegarde	La configuration du service nginx n'est pas valide. La configuration précédente est maintenant utilisée.
le service nginx-gw utilise la configuration de sauvegarde	La configuration du service nginx-gw n'est pas valide. La configuration précédente est maintenant utilisée.
Redémarrage requis pour désactiver FIPS	La stratégie de sécurité ne nécessite pas le mode FIPS, mais le module de sécurité cryptographique NetApp est activé.
Redémarrage requis pour activer FIPS	La stratégie de sécurité nécessite le mode FIPS, mais le module de sécurité cryptographique NetApp est désactivé.
Service SSH utilisant la configuration de sauvegarde	La configuration du service SSH n'est pas valide. La configuration précédente est maintenant utilisée.

#### Alertes aux locataires

Nom de l'alerte	Description
Utilisation élevée du quota par les locataires	Un pourcentage élevé de l'espace de quota est utilisé. Cette règle est désactivée par défaut car elle peut entraîner un trop grand nombre de notifications.

#### Metrics Prometheus couramment utilisés

Consultez cette liste de metrics Prometheus les plus utilisés pour mieux comprendre les conditions des règles d'alerte par défaut ou pour construire les conditions des règles d'alerte personnalisées.

Vous pouvez également [obtenez une liste complète de toutes les mesures](#).

Pour plus de détails sur la syntaxe des requêtes Prometheus, voir "[Interrogation de Prometheus](#)".

#### Quels sont les metrics Prometheus ?

Les metrics Prometheus sont des mesures de séries chronologiques. Le service Prometheus sur les nœuds d'administration collecte ces metrics à partir des services sur tous les nœuds. Des metrics sont stockés sur chaque nœud d'administration jusqu'à ce que l'espace réservé aux données Prometheus soit plein. Lorsque le `/var/local/mysql_ibdata/` volume atteint sa capacité, les mesures les plus anciennes sont supprimées en premier.

## Où sont utilisés les metrics Prometheus ?

Les metrics collectées par Prometheus sont utilisées à plusieurs endroits dans Grid Manager :

- **Page noeuds** : les graphiques et graphiques des onglets disponibles sur la page noeuds utilisent l'outil de visualisation Grafana pour afficher les metrics de séries chronologiques recueillies par Prometheus. Grafana affiche les données de séries chronologiques aux formats graphique et graphique, tandis que Prometheus sert de source de données back-end.



- **Alertes** : les alertes sont déclenchées à des niveaux de gravité spécifiques lorsque les conditions de règle d'alerte qui utilisent des metrics Prometheus sont définies comme vraies.
- **Grid Management API** : vous pouvez utiliser des metrics Prometheus dans des règles d'alerte personnalisées ou avec des outils d'automatisation externes pour surveiller votre système StorageGRID. La liste complète des metrics de Prometheus est disponible via l'API Grid Management. (En haut de Grid Manager, sélectionnez l'icône d'aide et sélectionnez **documentation API > metrics**.) Bien que plus d'un millier de mesures soient disponibles, seul un nombre relativement faible est requis pour surveiller les opérations StorageGRID les plus stratégiques.



Les indicateurs qui incluent *private* dans leurs noms sont destinés à un usage interne uniquement et peuvent être modifiés sans préavis entre les versions de StorageGRID.

- La page **SUPPORT > Tools > Diagnostics** et la page **SUPPORT > Tools > Metrics** : ces pages, qui sont principalement destinées au support technique, fournissent plusieurs outils et graphiques qui utilisent les valeurs des mesures Prometheus.



Certaines fonctions et options de menu de la page métriques sont intentionnellement non fonctionnelles et peuvent faire l'objet de modifications.

## Liste des mesures les plus courantes

La liste suivante répertorie les metrics Prometheus les plus utilisés.



Les indicateurs incluant *private* dans leur nom sont destinés à un usage interne uniquement et sont susceptibles d'être modifiés sans préavis entre les versions de StorageGRID.

### **alertmanager\_notifications\_failed\_total**

Nombre total de notifications d'alerte ayant échoué.



**node\_filesystem\_dispo\_octets**

Espace système de fichiers disponible pour les utilisateurs non root en octets.

**Node\_Memory\_MemAvailable\_Bytes**

Champ informations mémoire MemAvailable\_Bytes.

**node\_network\_carrier**

Valeur porteuse de `/sys/class/net/iface`.

**node\_network\_recy\_errs\_total**

Statistiques du périphérique réseau `receive_errs`.

**node\_network\_transmit\_errs\_total**

Statistiques du périphérique réseau `transmit_errs`.

**storagegrid\_panne\_administrative**

Le nœud n'est pas connecté à la grille pour une raison attendue. Par exemple, le nœud ou les services du nœud ont été normalement arrêtés, le nœud est en cours de redémarrage ou le logiciel est mis à niveau.

**storagegrid\_appliance\_compute\_controller\_status**

L'état du matériel du contrôleur de calcul d'une appliance.

**disques\_défaillants\_appliance\_storagegrid**

Pour le contrôleur de stockage d'une appliance, le nombre de disques qui ne sont pas optimaux.

**état\_matériel\_contrôleur\_stockage\_appliance\_storagegrid**

État global du matériel du contrôleur de stockage d'une appliance.

**conteneurs\_contenu\_seaux\_et\_conteneurs\_storagegrid**

Le nombre total de compartiments S3 et de conteneurs Swift connus par ce nœud de stockage.

**objets\_contenu\_storagegrid**

Le nombre total d'objets de données S3 et Swift connus de ce nœud de stockage. Count est valide uniquement pour les objets de données créés par des applications client qui communiquent avec le système via S3.

**objet\_contenu\_storagegrid\_perdu**

Le nombre total d'objets détectés par ce service est manquant dans le système StorageGRID. Des mesures doivent être prises pour déterminer la cause de la perte et si la récupération est possible.

["Dépanner les données d'objet perdues ou manquantes"](#)

**storagegrid\_http\_sessions\_entrant\_tenté**

Nombre total de sessions HTTP ayant été tentées vers un noeud de stockage.

**storagegrid\_http\_sessions\_entrant\_actuellement\_établi**

Nombre de sessions HTTP actuellement actives (ouvertes) sur le nœud de stockage.

**storagegrid\_http\_sessions\_incoming\_failed**

Nombre total de sessions HTTP qui n'ont pas réussi à se terminer correctement, soit en raison d'une requête HTTP mal formée, soit en cas d'échec du traitement d'une opération.

**storagegrid\_http\_sessions\_entrant\_réussi**

Nombre total de sessions HTTP terminées avec succès.

**objets\_ilm\_en\_attente\_arrière-plan**

Le nombre total d'objets sur ce nœud en attente d'évaluation ILM à partir de l'analyse.

**storagegrid\_ilm\_en\_attente\_client\_évaluation\_objets\_par\_seconde**

Vitesse actuelle d'évaluation des objets par rapport à la règle ILM de ce nœud.

**objet\_client\_attente\_ilm\_en\_attente**

Le nombre total d'objets de ce nœud attend l'évaluation ILM des opérations client (par exemple, ingestion).

**objets\_ilm\_en\_attente\_total\_storagegrid**

Le nombre total d'objets en attente d'évaluation ILM.

**ilm\_scan\_objets\_par\_seconde**

Vitesse à laquelle les objets appartenant à ce nœud sont analysés et mis en file d'attente d'ILM.

**storagegrid\_ilm\_scan\_perce\_estimé\_minutes**

Durée estimée d'une analyse ILM complète sur ce nœud.

**Remarque :** Une analyse complète ne garantit pas que ILM a été appliquée à tous les objets appartenant à ce nœud.

**storagegrid\_load\_balancer\_cert\_exexpiration\_time**

Le temps d'expiration du certificat de nœud final de l'équilibreur de charge en secondes depuis l'époque.

**storagegrid\_metadata\_requêtes\_moyenne\_latence\_millisecondes**

Temps moyen requis pour exécuter une requête sur le magasin de métadonnées via ce service.

**storagegrid\_réseau\_reçu\_octets**

Quantité totale de données reçues depuis l'installation.

**octets\_réseau\_transmis\_storagegrid**

Quantité totale de données envoyées depuis l'installation.

**pourcentage\_utilisation\_cpu\_storagegrid\_nœud\_nœud**

Pourcentage de temps CPU disponible actuellement utilisé par ce service. Indique le niveau d'occupation du service. Le temps CPU disponible dépend du nombre de CPU du serveur.

**storagegrid\_ntp\_choisi\_source\_temps\_offset\_millisecondes**

Décalage systématique du temps fourni par une source de temps choisie. Le décalage est introduit lorsque le délai d'accès à une source de temps n'est pas égal au temps requis pour que la source de temps atteigne le client NTP.

**storagegrid\_ntp\_verrouillé**

Le nœud n'est pas verrouillé sur un serveur NTP (Network Time Protocol).

**storagegrid\_s3\_data\_transfers\_bytes\_ingested**

Quantité totale de données ingérées à partir des clients S3 pour ce nœud de stockage, depuis la dernière réinitialisation de l'attribut.

**storagegrid\_s3\_data\_transfers\_bytes\_retrieved**

Quantité totale de données récupérées par les clients S3 à partir de ce noeud de stockage depuis la dernière réinitialisation de l'attribut.

**storagegrid\_s3\_operations\_failed**

Le nombre total d'opérations S3 ayant échoué (codes d'état HTTP 4xx et 5xx), à l'exclusion des opérations causées par l'échec d'autorisation S3.

**storagegrid\_s3\_operations\_successful**

Nombre total d'opérations S3 réussies (code d'état HTTP 2xx).

**storagegrid\_s3\_operations\_unauthorized**

Nombre total d'opérations S3 ayant échoué à la suite d'un échec d'autorisation.

**storagegrid\_servercertificate\_management\_interface\_cert\_expiration\_days**

Nombre de jours avant l'expiration du certificat de l'interface de gestion.

**storagegrid\_servercertificate\_storage\_api\_endpoints\_cert\_expiration\_days**

Nombre de jours avant l'expiration du certificat de l'API de stockage objet.

**storagegrid\_service\_cpu\_secondes**

Durée cumulée pendant laquelle le CPU a été utilisé par ce service depuis l'installation.

**octets\_usage\_mémoire\_service\_storagegrid**

La quantité de mémoire (RAM) actuellement utilisée par ce service. Cette valeur est identique à celle affichée par l'utilitaire Linux TOP sous RES.

**octets\_réseau\_service\_storagegrid\_reçus\_netapp**

Quantité totale de données reçues par ce service depuis l'installation.

**octets\_réseau\_service\_storagegrid\_transmis\_netapp**

Quantité totale de données envoyées par ce service.

**redémarrages\_service\_storagegrid**

Nombre total de fois où le service a été redémarré.

**storagegrid\_service\_runtime\_seconds**

Durée totale d'exécution du service depuis l'installation.

**temps\_disponibilité\_service\_storagegrid\_secondes**

Durée totale d'exécution du service depuis son dernier redémarrage.

**storage\_state\_current\_storagegrid**

État actuel des services de stockage. Les valeurs d'attribut sont :

- 10 = hors ligne
- 15 = entretien
- 20 = lecture seule
- 30 = en ligne

### **état\_stockage\_storage\_storagegrid**

État actuel des services de stockage. Les valeurs d'attribut sont :

- 0 = aucune erreur
- 10 = en transition
- 20 = espace libre insuffisant
- 30 = Volume(s) indisponible
- 40 = erreur

### **storagegrid\_utilisation\_données\_octets**

Estimation de la taille totale des données d'objet répliquées et codées d'effacement sur le nœud de stockage.

### **storage\_utilisation\_métadonnées\_autorisés\_storagegrid\_octets**

Espace total sur le volume 0 de chaque nœud de stockage autorisé pour les métadonnées d'objet. Cette valeur est toujours inférieure à l'espace réel réservé aux métadonnées sur un nœud, car une partie de l'espace réservé est requise pour les opérations essentielles de base de données (telles que la compaction et la réparation) et les futures mises à niveau matérielles et logicielles. l'espace autorisé pour les métadonnées de l'objet contrôle la capacité globale des objets.

### **octets\_métadonnées\_utilisation\_stockage\_storagegrid**

Volume des métadonnées d'objet sur le volume de stockage 0, en octets.

### **storage\_usage\_total\_octets\_espace\_stockage\_storagegrid**

Quantité totale d'espace de stockage alloué à tous les magasins d'objets.

### **octets\_stockage\_utilisation\_de\_stockage\_utilisables\_storagegrid**

Quantité totale d'espace de stockage objet restant. Calculé en ajoutant ensemble la quantité d'espace disponible pour tous les magasins d'objets du nœud de stockage.

### **storagegrid\_swift\_data\_transfère\_octets\_ingérés**

Quantité totale de données ingérées à partir des clients Swift vers ce nœud de stockage depuis la dernière réinitialisation de l'attribut.

### **storagegrid\_swift\_data\_transferts\_octets\_récupéré**

Quantité totale de données récupérées par les clients Swift à partir de ce nœud de stockage depuis la dernière réinitialisation de l'attribut.

### **storagegrid\_swift\_operations\_failed**

Nombre total d'opérations Swift ayant échoué (codes d'état HTTP 4xx et 5xx), à l'exclusion des opérations causées par l'échec de l'autorisation Swift.

### **storagegrid\_swift\_operations\_successful**

Nombre total d'opérations Swift réussies (code d'état HTTP 2xx).

### **storagegrid\_swift\_operations\_non autorisé**

Nombre total d'opérations Swift ayant échoué à la suite d'une erreur d'autorisation (codes d'état HTTP 401, 403, 405).

## octets\_données\_utilisation\_storagegrid\_tenant

Taille logique de tous les objets pour le locataire.

## nombre\_d'objets\_usage\_storagegrid\_tenant\_storagegrid

Le nombre d'objets pour le locataire.

## octets\_quota\_utilisation\_storagegrid\_tenant\_octets

Quantité maximale d'espace logique disponible pour les objets du locataire. Si aucune mesure de quota n'est fournie, une quantité illimitée d'espace est disponible.

### Obtenez une liste de toutes les mesures

pour obtenir la liste complète des mesures, utilisez l'API de gestion de grille.

1. En haut du Gestionnaire de grille, sélectionnez l'icône d'aide et sélectionnez **documentation API**.
2. Localisez les opérations **métriques**.
3. Exécutez `GET /grid/metric-names` l'opération.
4. Téléchargez les résultats.

## Référence des fichiers journaux

### Référence des fichiers journaux

StorageGRID fournit des journaux utilisés pour capturer les événements, les messages de diagnostic et les conditions d'erreur. Il se peut que vous soyez invité à collecter les fichiers journaux et à les transférer au support technique pour faciliter le dépannage.

Les journaux sont classés comme suit :

- ["Journaux du logiciel StorageGRID"](#)
- ["Journaux de déploiement et de maintenance"](#)
- ["Sur le bycast.log"](#)



Les détails fournis pour chaque type de journal sont fournis à titre de référence uniquement. Les journaux sont destinés au dépannage avancé par le support technique. Les techniques avancées qui impliquent la reconstruction de l'historique des problèmes à l'aide des journaux d'audit et des fichiers journaux de l'application sont hors de portée de ces instructions.

### Accéder aux journaux

Pour accéder aux journaux, vous pouvez ["collectez les fichiers journaux et les données système"](#) utiliser un ou plusieurs nœuds en tant qu'archive de fichier journal unique. Si le nœud d'administration principal n'est pas disponible ou ne parvient pas à atteindre un nœud spécifique, vous pouvez accéder à des fichiers journaux individuels pour chaque nœud de la grille comme suit :

1. Entrez la commande suivante : `ssh admin@grid_node_IP`
2. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
3. Entrez la commande suivante pour basculer en root : `su -`

4. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

### Exportez les journaux vers le serveur syslog

L'exportation des journaux vers le serveur syslog offre les fonctionnalités suivantes :

- Recevez la liste de toutes les demandes Grid Manager et tenant Manager, en plus des demandes S3 et Swift.
- Meilleure visibilité sur les requêtes S3 qui renvoient des erreurs, sans l'impact sur les performances que provoquent les méthodes de journalisation des audits.
- Accès aux requêtes de couche HTTP et aux codes d'erreur faciles à analyser.
- Meilleure visibilité sur les demandes bloquées par les classificateurs du trafic au niveau de l'équilibreur de charge.

Pour exporter les journaux, reportez-vous "[Configurez les messages d'audit et les destinations des journaux](#)" à la section .

### Catégories de fichiers journaux

L'archive du fichier journal StorageGRID contient les journaux décrits pour chaque catégorie et les fichiers supplémentaires contenant des mesures et la sortie de la commande debug.

Emplacement d'archivage	Description
audit	Messages d'audit générés pendant le fonctionnement normal du système.
base-os-logs	Informations sur le système d'exploitation de base, notamment les versions d'images StorageGRID.
packs	Informations de configuration globale (bundles).
cassandra	Informations sur la base de données Cassandra et journaux de réparation de couches.
d'europe	Informations VCS sur le nœud actuel et les informations de groupe EC par ID de profil.
grille	Journaux de grille généraux, y compris débogage ( <code>bypass.log</code> ) et <code>servermanager</code> journaux.
grid.json	Le fichier de configuration du grid est partagé sur tous les nœuds. En outre, <code>node.json</code> est spécifique au nœud actuel.
hagroups	Metrics et journaux pour les groupes de haute disponibilité.
installer	<code>Gdu-server</code> et installez les journaux.

Emplacement d'archivage	Description
Lambda-arbitre	Journaux associés à la demande de proxy S3 Select.
lumberjack.log	Messages de débogage liés à la collecte de journaux.
Métriques	Journaux de service pour Grafana, Jaeger, node exportateur et Prometheus.
etcd	Journaux d'accès divers et d'erreurs.
mysql	La configuration de la base de données MariaDB et les journaux associés.
nette	Journaux générés par des scripts de mise en réseau et le service Dynap.
nginx	Fichiers et journaux de configuration de l'équilibreur de charge et de la fédération du grid. Inclut également les journaux de trafic Grid Manager et tenant Manager.
nginx-gw	<ul style="list-style-type: none"> <li>• <code>access.log</code>: Le gestionnaire de grille et le gestionnaire de locataires demandent des messages de journal. <ul style="list-style-type: none"> <li>◦ Ces messages sont préfixés avec lorsqu'ils sont <code>mgmt</code> : exportés à l'aide de syslog.</li> <li>◦ Le format de ces messages de journal est <code>[\$time_iso8601] \$remote_addr \$status \$bytes_sent \$request_length \$request_time "\$endpointId" "\$request" "\$http_host" "\$http_user_agent" "\$http_referer"</code></li> </ul> </li> <li>• <code>cgr-access.log.gz</code>: Demandes de réplication entrantes de la grille transversale. <ul style="list-style-type: none"> <li>◦ Ces messages sont préfixés avec lorsqu'ils sont <code>cgr</code> : exportés à l'aide de syslog.</li> <li>◦ Le format de ces messages de journal est <code>[\$time_iso8601] \$remote_addr \$status \$bytes_sent \$request_length \$request_time "\$endpointId" "\$upstream_addr" "\$request" "\$http_host"</code></li> </ul> </li> <li>• <code>endpoint-access.log.gz</code>: Requêtes S3 et Swift pour l'équilibrage de la charge des terminaux. <ul style="list-style-type: none"> <li>◦ Ces messages sont préfixés avec lorsqu'ils sont <code>endpoint</code> : exportés à l'aide de syslog.</li> <li>◦ Le format de ces messages de journal est <code>[\$time_iso8601] \$remote_addr \$status \$bytes_sent \$request_length \$request_time "\$endpointId" "\$upstream_addr" "\$request" "\$http_host"</code></li> </ul> </li> <li>• <code>nginx-gw-dns-check.log</code>: Lié à la nouvelle alerte de vérification DNS.</li> </ul>
ntp	Fichier de configuration et journaux NTP.

Emplacement d'archivage	Description
Objets orphelins	Journaux relatifs aux objets orphelins.
os	Fichier d'état de nœud et de grille, y compris les services <code>pid</code> .
autre	Les fichiers journaux sous <code>/var/local/log</code> qui ne sont pas collectés dans d'autres dossiers.
diminution des	Informations de performances pour le CPU, la mise en réseau et les E/S de disque
données prometheus	Metrics Prometheus actuels si la collecte des journaux inclut des données Prometheus.
provisionnement	Journaux relatifs au processus de provisionnement de la grille.
radeau	Journaux de grappe raft utilisés dans les services de plate-forme.
ssh	Journaux liés à la configuration et au service SSH.
snmp	Configuration de l'agent SNMP utilisée pour l'envoi de notifications SNMP.
sockets-données	Données des sockets pour le débogage réseau.
system-commands.txt	Résultat des commandes du conteneur StorageGRID. Contient des informations sur le système, telles que la mise en réseau et l'utilisation du disque.
synchroniser-package-récupération	Lié au maintien de la cohérence du dernier package de récupération sur tous les nœuds d'administration et les nœuds de stockage qui hébergent le service ADC.

## Journaux du logiciel StorageGRID

Les journaux StorageGRID vous permettent de résoudre les problèmes.



Si vous souhaitez envoyer vos journaux à un serveur syslog externe ou modifier la destination des informations d'audit telles que `bycast.log` et `nms.log`, reportez-vous à la section "[Configurez les messages d'audit et les destinations des journaux](#)".

### Journaux StorageGRID généraux



Nom du fichier	Remarques	Ci-après
/var/local/log/bycast.log	Fichier de dépannage StorageGRID principal. Sélectionnez <b>SUPPORT &gt; Outils &gt; topologie de grille</b> . Sélectionnez ensuite <b>site &gt; Node &gt; SSM &gt; Events</b> .	Tous les nœuds
/var/local/log/bycast-err.log	Contient un sous-ensemble de <code>bycast.log</code> (messages avec ERREUR DE gravité et CRITIQUE). Des messages CRITIQUES sont également affichés dans le système. Sélectionnez <b>SUPPORT &gt; Outils &gt; topologie de grille</b> . Sélectionnez ensuite <b>site &gt; Node &gt; SSM &gt; Events</b> .	Tous les nœuds
/var/local/core/	Contient tous les fichiers core dump créés si le programme se termine anormalement. Les causes possibles sont les échecs d'assertion, les violations ou les retards de thread.  <b>Remarque</b> : le fichier <code>`/var/local/core/kexec_cmd</code> existe généralement sur les nœuds de l'appliance et n'indique pas d'erreur.	Tous les nœuds

#### Journaux liés au chiffrement

Nom du fichier	Remarques	Ci-après
/var/local/log/ssh-config-generation.log	Contient des journaux relatifs à la génération de configurations SSH et au rechargement de services SSH.	Tous les nœuds
/var/local/log/nginx/config-generation.log	Contient les journaux relatifs à la génération des configurations nginx et au rechargement des services nginx.	Tous les nœuds
/var/local/log/nginx-gw/config-generation.log	Contient les journaux relatifs à la génération des configurations nginx-gw (et au rechargement des services nginx-gw).	Nœuds d'administration et de passerelle
/var/local/log/update-cipher-configurations.log	Contient des journaux relatifs à la configuration des règles TLS et SSH.	Tous les nœuds

## Journaux de fédération du grid

Nom du fichier	Remarques	Ci-après
/var/local/log/update_grid_federation_config.log	Contient les journaux relatifs à la génération des configurations nginx et nginx-gw pour les connexions de fédération de grille.	Tous les nœuds

## Journaux NMS

Nom du fichier	Remarques	Ci-après
/var/local/log/nms.log	<ul style="list-style-type: none"><li>• Capture des notifications à partir du Grid Manager et du tenant Manager.</li><li>• Capture les événements liés au fonctionnement du service NMS. Par exemple, les notifications par e-mail et les modifications de configuration.</li><li>• Contient des mises à jour de bundle XML résultant des modifications de configuration effectuées dans le système.</li><li>• Contient des messages d'erreur liés au sous-échantillonnage de l'attribut effectué une fois par jour.</li><li>• Contient les messages d'erreur du serveur Web Java, par exemple les erreurs de génération de page et les erreurs HTTP Status 500.</li></ul>	Nœuds d'administration
/var/local/log/nms.errlog	<p>Contient des messages d'erreur relatifs aux mises à niveau de la base de données MySQL.</p> <p>Contient le flux erreur standard (stderr) des services correspondants. Il y a un fichier journal par service. Ces fichiers sont généralement vides, sauf en cas de problème avec le service.</p>	Nœuds d'administration
/var/local/log/nms.requestlog	Contient des informations sur les connexions sortantes de l'API de gestion vers les services StorageGRID internes.	Nœuds d'administration

## Journaux Server Manager

Nom du fichier	Remarques	Ci-après
/var/local/log/servermanager.log	Fichier journal de l'application Server Manager exécutée sur le serveur.	Tous les nœuds
/Var/local/log/GridstatBackend.errlog	Fichier journal de l'application back-end de l'interface utilisateur graphique de Server Manager.	Tous les nœuds
/var/local/log/gridstat.errlog	Fichier journal de l'interface graphique de Server Manager.	Tous les nœuds

#### Journaux des services StorageGRID

Nom du fichier	Remarques	Ci-après
/var/local/log/acct.errlog		Nœuds de stockage exécutant le service ADC
/var/local/log/adc.errlog	Contient le flux erreur standard (stderr) des services correspondants. Il y a un fichier journal par service. Ces fichiers sont généralement vides, sauf en cas de problème avec le service.	Nœuds de stockage exécutant le service ADC
/var/local/log/ams.errlog		Nœuds d'administration
/var/local/log/cassandra/system.log	Informations pour le magasin de métadonnées (base de données Cassandra) pouvant être utilisées en cas de problème lors de l'ajout de nouveaux nœuds de stockage ou si la tâche de réparation nodetool cale.	Nœuds de stockage
/var/local/log/cassandra-reaper.log	Informations concernant le service Cassandra Reaper, qui répare les données de la base de données Cassandra.	Nœuds de stockage
/var/local/log/cassandra-reaper.errlog	Informations d'erreur pour le service Cassandra Reaper.	Nœuds de stockage
/var/local/log/chunk.errlog		Nœuds de stockage
/var/local/log/cmn.errlog		Nœuds d'administration

Nom du fichier	Remarques	Ci-après
/var/local/log/cms.errlog	Ce fichier journal peut être présent sur les systèmes qui ont été mis à niveau à partir d'une ancienne version de StorageGRID. Il contient des informations héritées.	Nœuds de stockage
/var/local/log/dds.errlog		Nœuds de stockage
/var/local/log/dmv.errlog		Nœuds de stockage
/var/local/log/dylib*	Contient des journaux liés au service dynap, qui surveille la grille pour les modifications IP dynamiques et met à jour la configuration locale.	Tous les nœuds
/var/local/log/grafana.log	Journal associé au service Grafana, utilisé pour la visualisation des metrics dans Grid Manager.	Nœuds d'administration
/var/local/log/hagroups.log	Journal associé aux groupes haute disponibilité.	Nœuds d'administration et nœuds de passerelle
/var/local/log/hagroups_events.log	Suivi des changements d'état, tels que la transition de LA SAUVEGARDE vers LE MAÎTRE ou LE DÉFAUT.	Nœuds d'administration et nœuds de passerelle
/var/local/log/idnt.errlog		Nœuds de stockage exécutant le service ADC
/var/local/log/jaeger.log	Journal associé au service jaeger, qui est utilisé pour la collecte de traces.	Tous les nœuds
/var/local/log/kstn.errlog		Nœuds de stockage exécutant le service ADC
/var/local/log/lambda*	Contient les journaux du service S3 Select.	Nœuds d'administration et de passerelle  Seuls certains nœuds d'administration et de passerelle contiennent ce journal. Voir la <a href="#">"Exigences et limitations de S3 Select pour les nœuds d'administration et de passerelle"</a> .

Nom du fichier	Remarques	Ci-après
/var/local/log/ldr.errlog		Nœuds de stockage
/var/local/log/miscd/*.log	Contient des journaux pour le service MISCd (démon de contrôle du service d'information), qui fournit une interface pour interroger et gérer les services sur d'autres nœuds et pour gérer les configurations environnementales sur le nœud, comme interroger l'état des services s'exécutant sur d'autres nœuds.	Tous les nœuds
/var/local/log/nginx/*.log	Contient des journaux pour le service nginx, qui agit comme un mécanisme d'authentification et de communication sécurisée pour divers services de réseau (comme Prometheus et Dynap) pour pouvoir communiquer avec les services sur d'autres nœuds via des API HTTPS.	Tous les nœuds
/var/local/log/nginx-gw/*.log	Contient les journaux généraux relatifs au service nginx-gw, y compris les journaux d'erreurs et les journaux des ports d'administration restreints sur les nœuds d'administration.	Nœuds d'administration et nœuds de passerelle
/var/local/log/nginx-gw/cgr-access.log.gz	Contient des journaux d'accès relatifs au trafic de réplication inter-grid.	Nœuds d'administration, nœuds de passerelle ou les deux, en fonction de la configuration de fédération grid. Uniquement disponible sur la grille de destination pour la réplication inter-grid.
/var/local/log/nginx-gw/endpoint-access.log.gz	Contient les journaux d'accès du service Load Balancer, qui assure l'équilibrage de la charge du trafic S3 entre les clients et les nœuds de stockage.	Nœuds d'administration et nœuds de passerelle
/var/local/log/persistence*	Contient les journaux du service Persistence, qui gère les fichiers sur le disque racine qui doivent persister au cours d'un redémarrage.	Tous les nœuds

Nom du fichier	Remarques	Ci-après
/var/local/log/prometheus.log	<p>Pour tous les nœuds, il contient le journal de service de l'exportateur de nœuds et le journal des services de metrics de l'outil d'exportation de nœuds.</p> <p>Pour les nœuds d'administration, contient également les journaux des services Prometheus et Alert Manager.</p>	Tous les nœuds
/var/local/log/raft.log	Contient la sortie de la bibliothèque utilisée par le service RSM pour le protocole de radeau.	Nœuds de stockage avec service RSM
/var/local/log/rms.errlog	Contient les journaux du service RSM (State machine Service) répliqué, qui est utilisé pour les services de plateforme S3.	Nœuds de stockage avec service RSM
/var/local/log/ssm.errlog		Tous les nœuds
/var/local/log/update-s3vs-domains.log	Contient des journaux relatifs aux mises à jour de traitement pour la configuration des noms de domaine hébergés sur des serveurs virtuels S3. consultez les instructions d'implémentation des applications client S3.	Nœuds d'administration et de passerelle
/var/local/log/update-snmp-firewall.*	Contiennent des journaux relatifs aux ports de pare-feu gérés pour SNMP.	Tous les nœuds
/var/local/log/update-sysl.log	Contient des journaux relatifs aux modifications apportées à la configuration syslog du système.	Tous les nœuds
/var/local/log/update-traffic-classes.log	Contient des journaux relatifs aux modifications apportées à la configuration des classificateurs de trafic.	Nœuds d'administration et de passerelle
/var/local/log/update-utcn.log	Contient des journaux liés au mode réseau client non fiable sur ce nœud.	Tous les nœuds

#### Informations associées

- ["Sur le bycast.log"](#)
- ["UTILISEZ L'API REST S3"](#)

## Journaux de déploiement et de maintenance

Vous pouvez utiliser les journaux de déploiement et de maintenance pour résoudre les problèmes.

Nom du fichier	Remarques	Ci-après
<code>/var/local/log/install.log</code>	Créé lors de l'installation du logiciel. Contient un enregistrement des événements d'installation.	Tous les nœuds
<code>/var/local/log/expansion-progress.log</code>	Créé pendant les opérations d'extension. Contient un enregistrement des événements d'extension.	Nœuds de stockage
<code>/var/local/log/pa-move.log</code>	Créé lors de l'exécution <code>pa-move.sh</code> du script.	Nœud d'administration principal
<code>/var/local/log/pa-move-new_pa.log</code>	Créé lors de l'exécution <code>pa-move.sh</code> du script.	Nœud d'administration principal
<code>/var/local/log/pa-move-old_pa.log</code>	Créé lors de l'exécution <code>pa-move.sh</code> du script.	Nœud d'administration principal
<code>/var/local/log/gdu-server.log</code>	Créé par le service GDU. Contient les événements liés aux procédures d'approvisionnement et de maintenance gérées par le nœud d'administration principal.	Nœud d'administration principal
<code>/var/local/log/send_admin_hw.log</code>	Créé lors de l'installation. Contient des informations de débogage liées aux communications d'un nœud avec le nœud d'administration principal.	Tous les nœuds
<code>/var/local/log/upgrade.log</code>	Créé lors de la mise à niveau logicielle. Contient un enregistrement des événements de mise à jour du logiciel.	Tous les nœuds

### Sur le `bycast.log`

Le fichier est le fichier `/var/local/log/bycast.log` de dépannage principal du logiciel StorageGRID. Il existe un `bycast.log` fichier pour chaque nœud de grille. Le fichier contient des messages spécifiques à ce nœud de grille.

Le fichier `/var/local/log/bycast-err.log` est un sous-ensemble de `bycast.log`. Il contient des messages D'ERREUR de gravité et D'ERREUR CRITIQUE.

Vous pouvez également modifier la destination des journaux d'audit et envoyer des informations d'audit à un serveur syslog externe. Les journaux locaux des enregistrements d'audit continuent à être générés et stockés lorsqu'un serveur syslog externe est configuré. Voir "[Configurez les messages d'audit et les destinations des journaux](#)".

## Rotation des fichiers pour bycast.log

Lorsque le `bycast.log` fichier atteint 1 Go, le fichier existant est enregistré et un nouveau fichier journal démarre.

Le fichier enregistré est renommé `bycast.log.1` et le nouveau fichier est nommé `bycast.log`. Lorsque le nouveau `bycast.log` atteint 1 Go, `bycast.log.1` est renommé et compressé pour devenir `bycast.log.2.gz`, et `bycast.log` est renommé `bycast.log.1`.

La limite de rotation pour `bycast.log` est de 21 fichiers. Lorsque la 22e version du `bycast.log` fichier est créée, le fichier le plus ancien est supprimé.

La limite de rotation pour `bycast-err.log` est de sept fichiers.



Si un fichier journal a été compressé, vous ne devez pas le décompresser au même emplacement que celui dans lequel il a été écrit. La décompression du fichier au même emplacement peut interférer avec les scripts de rotation du journal.

Vous pouvez également modifier la destination des journaux d'audit et envoyer des informations d'audit à un serveur syslog externe. Les journaux locaux des enregistrements d'audit continuent à être générés et stockés lorsqu'un serveur syslog externe est configuré. Voir "[Configurez les messages d'audit et les destinations des journaux](#)".

### Informations associées

["Collecte de fichiers journaux et de données système"](#)

### Messages en bycast.log

Les messages dans `bycast.log` sont écrits par l'ADE (Asynchronous Distributed Environment). ADE est l'environnement d'exécution utilisé par les services de chaque nœud de la grille.

Exemple de message ADE :

```
May 15 14:07:11 um-sec-rg1-agn3 ADE: |12455685      0357819531
SVMR EVHR 2019-05-05T27T17:10:29.784677| ERROR 0906 SVMR: Health
check on volume 3 has failed with reason 'TOUT'
```

Les messages ADE contiennent les informations suivantes :

Segment de message	Valeur dans l'exemple
ID du nœud	12455685
ID processus ADE	0357819531
Nom du module	SVMR
Identifiant du message	EVHR



Segment de message	Valeur dans l'exemple
Heure système UTC	2019-05-05T27T17:10:29.784677 (AAAA-MM-DDTHH:MM:SS.UUUUUUUU)
Niveau de gravité	ERREUR
Numéro de suivi interne	0906
Messagerie	SVMR : le bilan de santé du volume 3 a échoué avec la raison « tout »

### Gravité des messages en bycast.log

Des niveaux de sévérité sont attribués aux messages `bycast.log` de la section.

Par exemple :

- **AVIS** — un événement qui devrait être enregistré s'est produit. La plupart des messages du journal sont à ce niveau.
- **AVERTISSEMENT** — une condition inattendue s'est produite.
- **ERREUR** — Une erreur majeure s'est produite qui aura une incidence sur les opérations.
- **CRITIQUE** — une condition anormale s'est produite qui a arrêté les opérations normales. Vous devez immédiatement corriger la condition sous-jacente.

### Codes d'erreur dans `bycast.log`

La plupart des messages d'erreur de la `bycast.log` contiennent des codes d'erreur.

Le tableau suivant répertorie les codes non numériques courants dans la `bycast.log` signification exacte d'un code non numérique dépend du contexte dans lequel il est signalé.

Code d'erreur	Signification
CAN	Pas d'erreur
GERR	Inconnu
ANNUL	Annulée
ABRT	Abandonné
TOUT	Délai dépassé
INVL	Non valide
NFND	Introuvable

Code d'erreur	Signification
VERS	Version
CONF	Configuration
ECHEC	Échec
CIPD	Incomplet
L'A FAIT	L'a fait
SUNV	Service indisponible

Le tableau suivant répertorie les codes d'erreur numériques dans `bycast.log`.

Numéro de l'erreur	Code d'erreur	Signification
001	EPERM	Opération non autorisée
002	RÉF	Ce fichier ou répertoire n'est pas disponible
003	ESRCH	Pas de tel processus
004	EINTA	Appel système interrompu
005	EIO	Erreur d'E/S.
006	ENXIO	Ce périphérique ou cette adresse n'est pas disponible
007	E2BIG	Liste d'arguments trop longue
008	ENOEXEC	Erreur de format Exec
009	EBADF	Numéro de fichier incorrect
010	ECHILD	Aucun processus enfant
011	EAGAIN	Réessayez
012	ENOMEM	Mémoire insuffisante
013	EACCES	Autorisation refusée

<b>Numéro de l'erreur</b>	<b>Code d'erreur</b>	<b>Signification</b>
014	PAR DÉFAUT	Adresse incorrecte
015	ENOTBLK	Dispositif de blocage requis
016	EBUSY	Périphérique ou ressource occupé
017	EEXIST	Le fichier existe déjà
018	EXDEV	Liaison interpériphérique
019	ENV	Aucun appareil de ce type
020	ENOTDIR	Pas un répertoire
021	EISDIR	Est un répertoire
022	EINVAL	Argument non valide
023	PAGE D'ACCUEIL	Dépassement de la table de fichiers
024	EMFILE	Trop de fichiers ouverts
025	EN COURS	Pas une machine à écrire
026	ETXTBBS	Fichier texte occupé
027	EFBIG	Fichier trop volumineux
028	ENOSPC	Il n'y a plus d'espace sur l'appareil
029	ESPIPE	Recherche illégale
030	EROFS	Système de fichiers en lecture seule
031	ALINK	Trop de liens
032	EPIPE	Tuyau cassé
033	ÉDOM	Argument mathématique hors domaine de la fonction
034	ERANGE	Résultat mathématique non représentativité

<b>Numéro de l'erreur</b>	<b>Code d'erreur</b>	<b>Signification</b>
035	EDEADLE	L'impasse de la ressource se produirait
036	ENAMETOOLONG	Nom de fichier trop long
037	ENOLCK	Aucun verrouillage d'enregistrement disponible
038	ENOSYS	Fonction non implémentée
039	ENOTEMPTY	Répertoire non vide
040	ELOP	Trop de liens symboliques rencontrés
041		
042	ENOMSG	Aucun message du type souhaité
043	EIDRM	Identificateur supprimé
044	ECHNG	Numéro de canal hors plage
045	EL2NSYNC	Niveau 2 non synchronisé
046	EL3HLT	Niveau 3 arrêté
047	EL3RST	Remise à zéro du niveau 3
048	ELNRNG	Numéro de liaison hors plage
049	EUNATCH	Pilote de protocole non connecté
050	ENOCSI	Aucune structure CSI disponible
051	EL2HLT	Niveau 2 arrêté
052	EBADE	Échange non valide
053	ADR	Descripteur de demande non valide
054	EXFULL	Exchange complet
055	ENOANO	Pas d'anode

<b>Numéro de l'erreur</b>	<b>Code d'erreur</b>	<b>Signification</b>
056	EBADRQC	Code de demande non valide
057	EBADSLT	Emplacement non valide
058		
059	EBFONT	Format de fichier de police incorrect
060	ENOSTR	Le périphérique n'est pas un flux
061	ENODATA	Aucune donnée disponible
062	ETIME	Temporisation expirée
063	ENOSR	Ressources hors flux
064	ENONET	La machine n'est pas sur le réseau
065	ENOPKG	Package non installé
066	EREMOTE	L'objet est distant
067	LIAISON	Le lien a été rompu
068	EADV	Erreur de publicité
069	ESRMNT	Erreur Srmount
070	ECOMM	Erreur de communication sur l'envoi
071	EPROTO	Erreur de protocole
072	EMULTIHOP	Multihop tenté
073	EDOTTDOT	Erreur spécifique RFS
074	EBADMSG	Pas un message de données
075	EOVERFLOW	Valeur trop élevée pour le type de données défini
076	ENOTUNIQ	Nom non unique sur le réseau

<b>Numéro de l'erreur</b>	<b>Code d'erreur</b>	<b>Signification</b>
077	EDFD	Descripteur de fichier dans un état incorrect
078	SOUS-GROUPE	Adresse distante modifiée
079	ELIBACC	Impossible d'accéder à une bibliothèque partagée nécessaire
080	ELIBBAD	Accès à une bibliothèque partagée endommagée
081	ELIBSCN	
082	ELIBMAX	Tentative de liaison dans trop de bibliothèques partagées
083	ELIBEXEC	impossible d'exécuter directement une bibliothèque partagée
084	EILSEQ	Séquence d'octets non autorisée
085	SYSTÈME	L'appel système interrompu doit être redémarré
086	ESTRPIPE	Erreur de tuyau de flux
087	EUSERS	Trop d'utilisateurs
088	ENOTSOCK	Fonctionnement de la prise femelle sur non prise femelle
089	EDESTADDRREQ	Adresse de destination requise
090	EMSGSIZE	Message trop long
091	EPROTOTYPE	Type de protocole incorrect pour le socket
092	EN OPTION	Protocole non disponible
093	EPROTONOSUPPORT	Protocole non pris en charge
094	ESOCKNOSUPPORT	Type de socket non pris en charge
095	EOPNOTSUPP	Opération non prise en charge sur le terminal de transport

<b>Numéro de l'erreur</b>	<b>Code d'erreur</b>	<b>Signification</b>
096	EPFNOSUPPORT	Famille de protocoles non prise en charge
097	EAFNOSUPPORT	Famille d'adresses non prise en charge par le protocole
098	EADDRINUSE	Adresse déjà utilisée
099	EADDRNOTAVAIL	Impossible d'attribuer l'adresse demandée
100	EN-TÊTE	Le réseau ne fonctionne pas
101	ENETUNREACH	Le réseau est inaccessible
102	ENETRESET	La connexion au réseau a été interrompue en raison d'une réinitialisation
103	ECONNABORTED	Le logiciel a provoqué l'arrêt de la connexion
104	ECONRESET	Réinitialisation de la connexion par poste
105	ENOBUFS	Aucun espace tampon disponible
106	EISCONN	Terminal de transport déjà connecté
107	ENOTCONN	Le terminal de transport n'est pas connecté
108	ESHUTDOWN	Impossible d'envoyer après l'arrêt du terminal de transport
109	ETOONYREFS	Trop de références : impossible d'épisser
110	ETIMDOUT	La connexion a expiré
111	ECONREFUSED	Connexion refusée
112	EHOSTDOWN	L'hôte n'est pas en panne
113	EHOSTUNREACH	Aucune route vers l'hôte
114	EALREADY	Opération déjà en cours
115	EINPROGRESS	Opération en cours

Numéro de l'erreur	Code d'erreur	Signification
116		
117	EUCLEAN	La structure doit être nettoyée
118	ENOTNAM	Pas un fichier de type nommé XENIX
119	ENAVAIL	Aucun sémaphores XENIX n'est disponible
120	EISNAM	Est un fichier de type nommé
121	EREMOTIO	Erreur d'E/S distante
122	EDUQUOT	Quota dépassé
123	ENOMEDIUM	Aucun support trouvé
124	EMEDIUMTYPE	Type de support incorrect
125	ECANCELED	Opération annulée
126	ENOKAY	Clé requise non disponible
127	EKEYEXPIRED	La clé a expiré
128	EKEYREVOKED	La clé a été révoquée
129	EKEYREJECTED	La clé a été rejetée par le service
130	EOWNERDEAD	Pour des mutexes robustes : le propriétaire est mort
131	ENOTRECOVERABLE	Pour les mutexes robustes : état non récupérable

## Configurer les destinations des messages d'audit et des journaux

### Considérations relatives à l'utilisation d'un serveur syslog externe

Un serveur syslog externe est un serveur hors de StorageGRID que vous pouvez utiliser pour collecter les informations d'audit système sur un emplacement unique. L'utilisation d'un serveur syslog externe vous permet de réduire le trafic réseau sur vos nœuds d'administration et de gérer les informations plus efficacement. Pour StorageGRID, le format de paquet de messages syslog sortants est conforme à la norme RFC 3164.

Les types d'informations d'audit que vous pouvez envoyer au serveur syslog externe sont les suivants :



- Journaux d'audit contenant les messages d'audit générés pendant le fonctionnement normal du système
- Événements liés à la sécurité tels que les connexions et la remontée à la racine
- Fichiers journaux d'application pouvant être demandés s'il est nécessaire d'ouvrir un dossier d'assistance pour résoudre un problème rencontré

### Quand utiliser un serveur syslog externe

Un serveur syslog externe est particulièrement utile si vous disposez d'une grande grille, utilisez plusieurs types d'applications S3 ou souhaitez conserver toutes les données d'audit. L'envoi d'informations d'audit à un serveur syslog externe vous permet de :

- Collectez et gérez plus efficacement les informations d'audit telles que les messages d'audit, les journaux d'applications et les événements de sécurité.
- Réduisez le trafic réseau sur vos nœuds d'administration, car les informations d'audit sont transférées directement depuis les différents nœuds de stockage vers le serveur syslog externe, sans devoir passer par un nœud d'administration.



Lorsque les journaux sont envoyés à un serveur syslog externe, les journaux uniques supérieurs à 8,192 octets sont tronqués à la fin du message pour se conformer aux limitations communes des implémentations de serveur syslog externe.



Pour optimiser les options de restauration complète des données en cas de défaillance du serveur syslog externe, jusqu'à 20 Go de journaux locaux d'enregistrements d'audit (`localaudit.log`) sont conservés sur chaque nœud.

### Comment configurer un serveur syslog externe

Pour savoir comment configurer un serveur syslog externe, reportez-vous à la section "[Configurer les messages d'audit et le serveur syslog externe](#)".

Si vous prévoyez de configurer l'utilisation du protocole TLS ou RELP/TLS, vous devez disposer des certificats suivants :

- **Certificats d'autorité de certification du serveur** : un ou plusieurs certificats d'autorité de certification de confiance pour vérifier le serveur syslog externe dans le codage PEM. Si omis, le certificat d'autorité de certification de la grille par défaut sera utilisé.
- **Certificat client** : certificat client pour l'authentification au serveur syslog externe dans le codage PEM.
- **Clé privée client** : clé privée pour le certificat client dans le codage PEM.



Si vous utilisez un certificat client, vous devez également utiliser une clé privée client. Si vous fournissez une clé privée chiffrée, vous devez également fournir la phrase de passe. L'utilisation d'une clé privée chiffrée n'est pas un avantage majeur en matière de sécurité, car la clé et la phrase de passe doivent être stockées. Si elles sont disponibles, il est recommandé de recourir à une clé privée non chiffrée pour plus de simplicité.

### Comment estimer la taille du serveur syslog externe

En principe, la taille de la grille est adaptée au débit requis, défini en termes d'opérations S3 par seconde ou d'octets par seconde. Par exemple, votre grid peut être capable de gérer 1,000 opérations S3 par seconde ou 2,000 Mo par seconde, d'ingales et de récupérations d'objets. Il est conseillé de dimensionner votre serveur

syslog externe en fonction des besoins de votre grid.

Cette section fournit des formules heuristiques qui vous aident à estimer le taux et la taille moyenne des messages de journal de différents types requis par votre serveur syslog externe en termes de caractéristiques de performance connues ou souhaitées de la grille (opérations S3 par seconde).

### Utilisez des opérations S3 par seconde dans les formules d'estimation

Si votre grille a été dimensionnée pour un débit exprimé en octets par seconde, vous devez convertir ce dimensionnement en opérations S3 par seconde afin d'utiliser les formules d'estimation. Pour convertir le débit du grid, vous devez d'abord déterminer la taille d'objet moyenne que vous pouvez utiliser les informations des journaux d'audit et des mesures existants (le cas échéant), ou en utilisant vos connaissances des applications qui utilisent StorageGRID. Par exemple, si la taille du grid a été dimensionnée pour atteindre un débit de 2,000 Mo/seconde, et que la taille d'objet moyenne est de 2 Mo, votre grille a été dimensionnée pour traiter 1,000 opérations S3 par seconde (2,000 Mo/2 Mo).



Les formules de dimensionnement externe du serveur syslog présentées dans les sections suivantes fournissent des estimations communes (plutôt que des estimations de cas les plus défavorables). Selon votre configuration et votre charge de travail, un taux plus élevé ou moins élevé de messages syslog ou de données syslog peut être constaté que les formules le prévoient. Les formules sont destinées à être utilisées uniquement comme directives.

### Formules d'estimation pour les journaux d'audit

Si vous ne disposez d'aucune information concernant votre charge de travail S3 autre que le nombre d'opérations S3 par seconde que votre grille doit prendre en charge, vous pouvez estimer le volume des journaux d'audit que votre serveur syslog externe devra gérer à l'aide des formules suivantes : Dans l'hypothèse où vous laissez les niveaux d'audit définis sur les valeurs par défaut (toutes les catégories sont définies sur Normal, sauf Storage, qui est défini sur erreur) :

```
Audit Log Rate = 2 x S3 Operations Rate  
Audit Log Average Size = 800 bytes
```

Par exemple, si le grid est dimensionné pour 1,000 opérations S3 par seconde, votre serveur syslog externe doit être dimensionné pour prendre en charge 2,000 messages syslog par seconde et doit être capable de recevoir (et généralement stocker) les données du journal d'audit à un taux de 1.6 Mo par seconde.

Si vous en savez plus sur votre charge de travail, des estimations plus précises sont possibles. Pour les journaux d'audit, les variables supplémentaires les plus importantes sont le pourcentage d'opérations S3 PUT (vs. Gets) et la taille moyenne, en octets, des champs S3 suivants (les abréviations de 4 caractères utilisées dans le tableau sont des noms de champs de journal d'audit) :

Code	Champ	Description
CCUA	Nom du compte de locataire S3 (expéditeur de la demande)	Nom du compte de tenant pour l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.

Code	Champ	Description
SBAC	Nom de compte de locataire S3 (propriétaire du compartiment)	Nom du compte du locataire pour le propriétaire du compartiment. Permet d'identifier les accès inter-comptes ou anonymes.
S3BK	Compartiment S3	Nom du compartiment S3.
S3KY	Touche S3	Le nom de la clé S3 n'inclut pas le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.

Nous allons utiliser P pour représenter le pourcentage d'opérations S3 qui sont PUT, où  $0 \leq P \leq 1$  (pour une charge de travail PUT de 100 %,  $P = 1$ , et pour une charge DE travail GET de 100 %,  $P = 0$ ).

Utilisons K pour représenter la taille moyenne de la somme des noms des comptes S3, du compartiment S3 et de la clé S3. Supposons que le nom de compte S3 soit toujours mon compte s3 (13 octets), que les compartiments ont des noms de longueur fixe comme /my/application/catg-12345 (28 octets) et que les objets ont des clés à longueur fixe comme 5733a5d7-f069-41ef-8fbd-132449c69c (36 octets). La valeur de K est alors de 90 (13+13+28+36).

Si vous pouvez déterminer les valeurs P et K, vous pouvez estimer le volume des journaux d'audit que votre serveur syslog externe doit traiter à l'aide des formules suivantes, en supposant que vous laissez les niveaux d'audit par défaut (toutes les catégories définies sur Normal, sauf Storage, Qui est défini sur erreur) :

$$\text{Audit Log Rate} = ((2 \times P) + (1 - P)) \times \text{S3 Operations Rate}$$

$$\text{Audit Log Average Size} = (570 + K) \text{ bytes}$$

Par exemple, si le grid est dimensionné pour 1,000 opérations S3 par seconde, le workload est PUT à 50 %, et les noms de compte S3, les noms de compartiment, Et les noms d'objet utilisent une moyenne de 90 octets. Votre serveur syslog externe doit être dimensionné pour prendre en charge 1,500 messages syslog par seconde et doit être capable de recevoir (et généralement stocker) les données du journal d'audit à un taux d'environ 1 Mo par seconde.

### Formules d'estimation pour les niveaux d'audit non par défaut

Les formules fournies pour les journaux d'audit supposent l'utilisation des paramètres par défaut du niveau d'audit (toutes les catégories sont définies sur Normal, sauf Storage, qui est défini sur erreur). Les formules détaillées d'estimation du taux et de la taille moyenne des messages d'audit pour les paramètres de niveau d'audit non par défaut ne sont pas disponibles. Toutefois, le tableau suivant peut être utilisé pour faire une estimation approximative du taux; vous pouvez utiliser la formule de taille moyenne fournie pour les journaux d'audit, mais sachez qu'elle risque de générer une surestimation car les messages d'audit « supplémentaires » sont, en moyenne, inférieurs aux messages d'audit par défaut.

Condition	Formule
Réplication : niveaux d'audit tous définis sur débogage ou Normal	Débit du journal d'audit = 8 x taux d'opérations S3

Condition	Formule
Codage d'effacement : les niveaux d'audit sont tous définis sur débogage ou Normal	Utiliser la même formule que pour les paramètres par défaut

### Formules d'estimation pour les événements de sécurité

Les événements de sécurité ne sont pas corrélés avec les opérations S3 et produisent généralement un volume négligeable de journaux et de données. Pour ces raisons, aucune formule d'estimation n'est fournie.

### Formules d'estimation pour les journaux d'application

Si vous ne disposez d'aucune information concernant votre charge de travail S3 autre que le nombre d'opérations S3 par seconde que votre grid est censé prendre en charge, vous pouvez estimer le volume des journaux d'applications que votre serveur syslog externe devra gérer à l'aide des formules suivantes :

```
Application Log Rate = 3.3 x S3 Operations Rate
Application Log Average Size = 350 bytes
```

Par exemple, si le grid est dimensionné pour 1,000 opérations S3 par seconde, votre serveur syslog externe doit être dimensionné pour prendre en charge 3,300 journaux d'application par seconde et être capable de recevoir (et de stocker) les données de journaux d'application à un taux de 1.2 Mo par seconde environ.

Si vous en savez plus sur votre charge de travail, des estimations plus précises sont possibles. Pour les journaux d'applications, les variables supplémentaires les plus importantes sont la stratégie de protection des données (réplication vs code d'effacement), le pourcentage d'opérations S3 PUT (vs. Gets/autre) et la taille moyenne, en octets, des champs S3 suivants (les abréviations de 4 caractères utilisées dans le tableau sont des noms de champs de journal d'audit) :

Code	Champ	Description
CCUA	Nom du compte de locataire S3 (expéditeur de la demande)	Nom du compte de tenant pour l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SBAC	Nom de compte de locataire S3 (propriétaire du compartiment)	Nom du compte du locataire pour le propriétaire du compartiment. Permet d'identifier les accès inter-comptes ou anonymes.
S3BK	Compartiment S3	Nom du compartiment S3.
S3KY	Touche S3	Le nom de la clé S3 n'inclut pas le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.

## Exemples d'estimations de dimensionnement

Cette section explique des exemples d'utilisation des formules d'estimation pour les grilles avec les méthodes de protection des données suivantes :

- La réplication
- Le code d'effacement

### Si vous utilisez la réplication pour la protection des données

La  $p$  représente le pourcentage d'opérations S3 qui sont PUT,  $0 \leq P \leq 1$  (pour une charge de travail PUT de 100 %,  $P = 1$  et POUR une charge DE travail GET de 100 %,  $P = 0$ ).

$K$  représente la taille moyenne de la somme des noms de compte S3, du compartiment S3 et de la clé S3. Supposons que le nom de compte S3 soit toujours mon compte s3 (13 octets), que les compartiments ont des noms de longueur fixe comme /my/application/catg-12345 (28 octets) et que les objets ont des clés à longueur fixe comme 5733a5d7-f069-41ef-8fbd-132449c69c (36 octets). Ensuite  $K$  a une valeur de 90 (13+13+28+36).

Si vous pouvez déterminer des valeurs pour  $P$  et  $K$ , vous pouvez estimer le volume des journaux d'application que votre serveur syslog externe devra traiter à l'aide des formules suivantes.

```
Application Log Rate = ((1.1 x P) + (2.5 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (220 + K)) + ((1 - P) x (240 + (0.2 x K))) Bytes
```

Par exemple, si le grid est dimensionné pour 1,000 opérations S3 par seconde, le workload est utilisé à 50 % et les noms de comptes S3, de compartiments et de noms d'objet moyenne à 90 octets, votre serveur syslog externe doit être dimensionné pour prendre en charge 1800 journaux d'applications par seconde. Et sera en mesure de recevoir (et de stocker en général) des données d'application à un taux de 0.5 Mo par seconde.

### Si vous utilisez le code d'effacement pour la protection des données

La  $p$  représente le pourcentage d'opérations S3 qui sont PUT,  $0 \leq P \leq 1$  (pour une charge de travail PUT de 100 %,  $P = 1$  et POUR une charge DE travail GET de 100 %,  $P = 0$ ).

$K$  représente la taille moyenne de la somme des noms de compte S3, du compartiment S3 et de la clé S3. Supposons que le nom de compte S3 soit toujours mon compte s3 (13 octets), que les compartiments ont des noms de longueur fixe comme /my/application/catg-12345 (28 octets) et que les objets ont des clés à longueur fixe comme 5733a5d7-f069-41ef-8fbd-132449c69c (36 octets). Ensuite  $K$  a une valeur de 90 (13+13+28+36).

Si vous pouvez déterminer des valeurs pour  $P$  et  $K$ , vous pouvez estimer le volume des journaux d'application que votre serveur syslog externe devra traiter à l'aide des formules suivantes.

```
Application Log Rate = ((3.2 x P) + (1.3 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (240 + (0.4 x K))) + ((1 - P) x (185 + (0.9 x K))) Bytes
```

Par exemple, si votre grid est dimensionné pour 1,000 opérations S3 par seconde, votre workload pèse 50 % du volume et vos noms de compte S3, noms de compartiment, les noms d'objets sont en moyenne de 90 octets. votre serveur syslog externe doit être dimensionné pour prendre en charge 2,250 journaux

d'applications par seconde et être capable de recevoir (et généralement de stocker) des données d'application à un taux de 0.6 Mo par seconde.

## Configurer les messages d'audit et le serveur syslog externe

Vous pouvez configurer un certain nombre de paramètres liés aux messages d'audit. Vous pouvez ajuster le nombre de messages d'audit enregistrés, définir les en-têtes de requête HTTP que vous souhaitez inclure dans les messages d'audit de lecture et d'écriture des clients, configurer un serveur syslog externe et spécifier l'emplacement d'envoi des journaux d'audit, des journaux d'événements de sécurité et des journaux logiciels StorageGRID.

Les messages d'audit et les journaux enregistrent les activités du système et les événements de sécurité. Ils constituent les outils essentiels de surveillance et de dépannage. Tous les nœuds StorageGRID génèrent des messages d'audit et des journaux pour suivre l'activité et les événements du système.

Vous pouvez également configurer un serveur syslog externe pour enregistrer les informations d'audit à distance. L'utilisation d'un serveur externe réduit l'impact sur les performances de la journalisation des messages d'audit sans réduire l'exhaustivité des données d'audit. Un serveur syslog externe est particulièrement utile si vous disposez d'une grande grille, utilisez plusieurs types d'applications S3 ou souhaitez conserver toutes les données d'audit. Voir ["Configurer les messages d'audit et le serveur syslog externe"](#) pour plus de détails.

### Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Maintenance ou autorisation d'accès racine"](#).
- Si vous prévoyez de configurer un serveur syslog externe, vous avez examiné le système et vous ["considérations relatives à l'utilisation d'un serveur syslog externe"](#)êtes assuré que le serveur dispose d'une capacité suffisante pour recevoir et stocker les fichiers journaux.
- Si vous prévoyez de configurer un serveur syslog externe à l'aide du protocole TLS ou RELP/TLS, vous disposez des certificats CA serveur et client requis et de la clé privée client.

### Modifier les niveaux des messages d'audit

Vous pouvez définir un niveau d'audit différent pour chacune des catégories de messages suivantes dans le journal d'audit :

Catégorie de vérification	Paramètre par défaut	Plus d'informations
Système	Normale	<a href="#">"Messages d'audit système"</a>
Stockage	Erreur	<a href="#">"Messages d'audit du stockage objet"</a>
Gestion	Normale	<a href="#">"Message d'audit de gestion"</a>
Lectures du client	Normale	<a href="#">"Messages d'audit de lecture du client"</a>

Catégorie de vérification	Paramètre par défaut	Plus d'informations
Écritures des clients	Normale	"Écrire des messages d'audit client"
ILM	Normale	"Messages d'audit ILM"
Réplication entre plusieurs grilles	Erreur	"CGRR : demande de réplication croisée"



Ces valeurs par défaut s'appliquent si vous avez installé StorageGRID à l'origine à l'aide de la version 10.3 ou ultérieure. Si vous avez initialement utilisé une version antérieure de StorageGRID, la valeur par défaut pour toutes les catégories est Normal.



Durant les mises à niveau, les configurations des niveaux d'audit ne seront pas effectives immédiatement.

## Étapes

1. Sélectionnez **CONFIGURATION > surveillance > serveur d'audit et syslog**.
2. Pour chaque catégorie de message d'audit, sélectionnez un niveau d'audit dans la liste déroulante :

Niveau d'audit	Description
Arrêt	Aucun message d'audit de la catégorie n'est enregistré.
Erreur	Seuls les messages d'erreur sont consignés—les messages d'audit pour lesquels le code de résultat n'a pas été « réussi » (CMC).
Normale	Les messages transactionnels standard sont consignés—les messages répertoriés dans ces instructions pour la catégorie.
Débogage	Obsolète. Ce niveau se comporte de la même manière que le niveau d'audit normal.

Les messages inclus pour tout niveau particulier incluent ceux qui seraient consignés aux niveaux supérieurs. Par exemple, le niveau Normal inclut tous les messages d'erreur.



Si vous n'avez pas besoin d'un enregistrement détaillé des opérations de lecture du client pour vos applications S3, vous pouvez éventuellement définir le paramètre **lecture du client** sur **erreur** pour diminuer le nombre de messages d'audit enregistrés dans le journal d'audit.

3. Sélectionnez **Enregistrer**.

Une bannière verte indique que votre configuration a été enregistrée.

## Définissez les en-têtes de requête HTTP

Vous pouvez éventuellement définir les en-têtes de requête HTTP que vous souhaitez inclure dans les messages d'audit de lecture et d'écriture du client. Ces en-têtes de protocole s'appliquent uniquement aux requêtes S3.

### Étapes

1. Dans la section **en-têtes de protocole d'audit**, définissez les en-têtes de requête HTTP que vous souhaitez inclure dans les messages d'audit de lecture et d'écriture du client.

Utilisez un astérisque (\*) comme caractère générique pour qu'il corresponde à zéro ou à plusieurs caractères. Utilisez la séquence d'échappement (\\*) pour faire correspondre un astérisque littéral.

2. Sélectionnez **Ajouter un autre en-tête** pour créer des en-têtes supplémentaires, si nécessaire.

Lorsque des en-têtes HTTP sont trouvés dans une requête, ils sont inclus dans le message d'audit sous le champ HTRH.



Les en-têtes de requête de protocole d'audit ne sont consignés que si le niveau d'audit pour **lecture client** ou **écriture client** n'est pas **off**.

3. Sélectionnez **Enregistrer**

Une bannière verte indique que votre configuration a été enregistrée.

### utilisez un serveur syslog externe

Vous pouvez également configurer un serveur syslog externe pour enregistrer les journaux d'audit, les journaux d'application et les journaux d'événements de sécurité dans un emplacement en dehors de votre grille.



Si vous ne souhaitez pas utiliser de serveur syslog externe, ignorez cette étape et passez à [Sélectionnez les destinations des informations d'audit](#) .



Si les options de configuration disponibles dans cette procédure ne sont pas suffisamment flexibles pour répondre à vos besoins, des options de configuration supplémentaires peuvent être appliquées à l'aide des `audit-destinations` noeuds finaux, qui se trouvent dans la section API privée de la ["API de gestion du grid"](#). Par exemple, vous pouvez utiliser l'API si vous souhaitez utiliser différents serveurs syslog pour différents groupes de nœuds.

## Entrez les informations syslog

Accédez à l'assistant configurer le serveur syslog externe et fournissez les informations dont StorageGRID a besoin pour accéder au serveur syslog externe.

### Étapes

1. Sur la page Audit and syslog Server, sélectionnez **Configure External syslog Server**. Ou, si vous avez déjà configuré un serveur syslog externe, sélectionnez **Modifier le serveur syslog externe**.

L'assistant configurer le serveur syslog externe s'affiche.

2. Pour l'étape **Entrez les informations syslog** de l'assistant, entrez un nom de domaine complet valide ou une adresse IPv4 ou IPv6 pour le serveur syslog externe dans le champ **Host**.



3. Entrez le port de destination sur le serveur syslog externe (doit être un entier compris entre 1 et 65535). Le port par défaut est 514.
4. Sélectionnez le protocole utilisé pour envoyer les informations d'audit au serveur syslog externe.

Il est recommandé d'utiliser **TLS** ou **RELP/TLS**. Vous devez télécharger un certificat de serveur pour utiliser l'une de ces options. L'utilisation de certificats permet de sécuriser les connexions entre votre grille et le serveur syslog externe. Pour plus d'informations, voir "[Gérer les certificats de sécurité](#)".

Toutes les options de protocole requièrent la prise en charge par le serveur syslog externe ainsi que sa configuration. Vous devez choisir une option compatible avec le serveur syslog externe.



Le protocole RELP (fiable Event Logging Protocol) étend la fonctionnalité du protocole syslog afin de fournir des messages d'événement fiables. L'utilisation de RELP peut aider à éviter la perte d'informations d'audit si votre serveur syslog externe doit redémarrer.

5. Sélectionnez **Continuer**.
6. si vous avez sélectionné **TLS** ou **RELP/TLS**, téléchargez les certificats de l'autorité de certification du serveur, le certificat du client et la clé privée du client.
  - a. Sélectionnez **Parcourir** pour le certificat ou la clé que vous souhaitez utiliser.
  - b. Sélectionnez le certificat ou le fichier de clé.
  - c. Sélectionnez **Ouvrir** pour charger le fichier.

Une coche verte s'affiche en regard du nom du fichier de certificat ou de clé, vous informant qu'il a été téléchargé avec succès.

7. Sélectionnez **Continuer**.

## Gérer le contenu du journal système

Vous pouvez sélectionner les informations à envoyer au serveur syslog externe.

### Étapes

1. Pour l'étape **gérer le contenu syslog** de l'assistant, sélectionnez chaque type d'informations d'audit que vous souhaitez envoyer au serveur syslog externe.
  - **Envoyer les journaux d'audit** : envoie les événements StorageGRID et les activités système
  - **Envoyer des événements de sécurité** : envoie des événements de sécurité tels qu'une tentative d'ouverture de session par un utilisateur non autorisé ou une ouverture de session par un utilisateur en tant que root
  - **Envoyer les journaux d'application** : envoie des messages "[Fichiers journaux du logiciel StorageGRID](#)" utiles pour le dépannage, notamment :
    - `bycast-err.log`
    - `bycast.log`
    - `jaeger.log`
    - `nms.log` (Nœuds d'administration uniquement)
    - `prometheus.log`
    - `raft.log`

▪ `hagroups.log`

- **Envoyer les journaux d'accès** : envoie les journaux d'accès HTTP pour les demandes externes à Grid Manager, tenant Manager, les noeuds finaux configurés de l'équilibreur de charge et les demandes de fédération de grille à partir de systèmes distants.

2. Utilisez les menus déroulants pour sélectionner la gravité et l'établissement (type de message) pour chaque catégorie d'informations d'audit que vous souhaitez envoyer.

La définition de la gravité et des valeurs de l'établissement peut vous aider à regrouper les journaux de manière personnalisable pour une analyse plus facile.

- a. Pour **gravité**, sélectionnez **passer-système** ou sélectionnez une valeur de gravité comprise entre 0 et 7.

Si vous sélectionnez une valeur, la valeur sélectionnée sera appliquée à tous les messages de ce type. Les informations sur les différentes gravité seront perdues si vous remplacez la gravité par une valeur fixe.

Gravité	Description
Passe-système	Chaque message envoyé au syslog externe a la même valeur de gravité que lorsqu'il a été connecté localement au nœud : <ul style="list-style-type: none"><li>• Pour les journaux d'audit, la gravité est « info ».</li><li>• Pour les événements de sécurité, les valeurs de gravité sont générées par la distribution Linux sur les nœuds.</li><li>• Pour les journaux d'application, les niveaux de gravité varient entre « info » et « avis », selon le problème. Par exemple, l'ajout d'un serveur NTP et la configuration d'un groupe HA donnent la valeur « INFO », tandis que l'arrêt délibéré du service SSM ou RSM donne la valeur « notification ».</li><li>• Pour les journaux d'accès, la gravité est « info ».</li></ul>
0	Urgence : le système est inutilisable
1	Alerte : une action doit être effectuée immédiatement
2	Critique : conditions critiques
3	Erreur : conditions d'erreur
4	Avertissement : conditions d'avertissement
5	Remarque : condition normale mais significative
6	Information : messages d'information
7	Débogage : messages de niveau débogage

b. Pour **facility**, sélectionnez **Passthrough** ou sélectionnez une valeur d'installation comprise entre 0 et 23.

Si vous sélectionnez une valeur, elle sera appliquée à tous les messages de ce type. Les informations concernant les différents sites seront perdues si vous remplacez l'établissement par une valeur fixe.

Installation	Description
Passe-système	<p>Chaque message envoyé au syslog externe a la même valeur d'installation que lorsqu'il a été connecté localement au nœud :</p> <ul style="list-style-type: none"> <li>• Pour les journaux d'audit, la fonction envoyée au serveur syslog externe est « local7 ».</li> <li>• Pour les événements de sécurité, les valeurs d'installation sont générées par la distribution linux sur les nœuds.</li> <li>• Pour les journaux d'application, les journaux d'application envoyés au serveur syslog externe ont les valeurs suivantes : <ul style="list-style-type: none"> <li>◦ <code>bycast.log</code>: utilisateur ou démon</li> <li>◦ <code>bycast-err.log</code>: utilisateur, démon, local3 ou local4</li> <li>◦ <code>jaeger.log</code>: local2</li> <li>◦ <code>nms.log</code>: local3</li> <li>◦ <code>prometheus.log</code>: local4</li> <li>◦ <code>raft.log</code>: local5</li> <li>◦ <code>hagroups.log</code>: local6</li> </ul> </li> <li>• Pour les journaux d'accès, la fonction envoyée au serveur syslog externe est "local0".</li> </ul>
0	kern (messages du noyau)
1	utilisateur (messages de niveau utilisateur)
2	e-mail
3	démon (démons système)
4	auth (messages de sécurité/d'autorisation)
5	syslog (messages générés en interne par syslogd)
6	lpr (sous-système d'imprimante ligne)
7	news (sous-système d'informations réseau)
8	UCP

Installation	Description
9	cron (démon d'horloge)
10	sécurité (messages de sécurité/d'autorisation)
11	FTP
12	NTP
13	audit journal (audit du journal)
14	alerte journal (alerte de journal)
15	horloge (démon d'horloge)
16	local0
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6
23	local7

3. Sélectionnez **Continuer**.

### Envoyer des messages de test

Avant de commencer à utiliser un serveur syslog externe, vous devez demander à tous les nœuds de votre grille d'envoyer des messages de test au serveur syslog externe. Ces messages de test vous aideront à valider l'intégralité de votre infrastructure de collecte de journaux avant de vous engager à envoyer des données au serveur syslog externe.



N'utilisez pas la configuration du serveur syslog externe tant que vous n'avez pas confirmé que le serveur syslog externe a reçu un message test de chaque nœud de votre grille et que le message a été traité comme prévu.

### Étapes

1. Si vous ne souhaitez pas envoyer de messages de test parce que vous êtes certain que votre serveur

syslog externe est correctement configuré et peut recevoir des informations d'audit de tous les nœuds de votre grille, sélectionnez **Ignorer et terminer**.

Une bannière verte indique que la configuration a été enregistrée.

2. Sinon, sélectionnez **Envoyer les messages de test** (recommandé).

Les résultats de test apparaissent en permanence sur la page jusqu'à ce que vous arrêtez le test. Pendant que le test est en cours, vos messages d'audit continuent d'être envoyés à vos destinations précédemment configurées.

3. Si vous recevez des erreurs, corrigez-les et sélectionnez à nouveau **Envoyer des messages de test**.

Reportez-vous "[Dépanner un serveur syslog externe](#)" à pour résoudre les erreurs.

4. Attendez qu'une bannière verte indique que tous les nœuds ont réussi le test.
5. Vérifiez votre serveur syslog pour déterminer si les messages de test sont reçus et traités comme prévu.



Si vous utilisez UDP, vérifiez l'ensemble de votre infrastructure de collecte de journaux. Le protocole UDP ne permet pas une détection d'erreur aussi rigoureuse que les autres protocoles.

6. Sélectionnez **Arrêter et Terminer**.

Vous revenez à la page **Audit and syslog Server**. Une bannière verte indique que la configuration du serveur syslog a été enregistrée.



Les informations d'audit StorageGRID ne sont pas envoyées au serveur syslog externe tant que vous ne sélectionnez pas une destination incluant le serveur syslog externe.

### Sélectionnez les destinations des informations d'audit

Vous pouvez spécifier l'emplacement d'envoi des journaux d'audit, des journaux d'événements de sécurité et "[Journaux du logiciel StorageGRID](#)".



StorageGRID utilise par défaut les destinations d'audit de nœud local et stocke les informations d'audit dans `/var/local/log/localaudit.log`.

Lors de l'utilisation de `/var/local/log/localaudit.log`, les entrées du journal d'audit Grid Manager et tenant Manager peuvent être envoyées à un nœud de stockage. Vous pouvez trouver le nœud qui contient les entrées les plus récentes à l'aide de la `run-each-node --parallel "zgrep MGAU /var/local/log/localaudit.log | tail"` commande.

Certaines destinations ne sont disponibles que si vous avez configuré un serveur syslog externe.

### Étapes

1. Sur la page serveur d'audit et syslog, sélectionnez la destination des informations d'audit.



**Les nœuds locaux uniquement et le serveur syslog externe** fournissent généralement de meilleures performances.

Option	Description
Nœuds locaux uniquement (par défaut)	<p>Les messages d'audit, les journaux d'événements de sécurité et les journaux d'applications ne sont pas envoyés aux nœuds d'administration. Ils sont enregistrés uniquement sur les nœuds qui les ont générés (« le nœud local »). Les informations d'audit générées sur chaque nœud local sont stockées dans <code>/var/local/log/localaudit.log</code>.</p> <p><b>Remarque :</b> StorageGRID supprime périodiquement les journaux locaux dans une rotation pour libérer de l'espace. Lorsque le fichier journal d'un nœud atteint 1 Go, le fichier existant est enregistré et un nouveau fichier journal est démarré. La limite de rotation du journal est de 21 fichiers. Lorsque la 22e version du fichier journal est créée, le fichier journal le plus ancien est supprimé. En moyenne, environ 20 Go de données de journalisation sont stockés sur chaque nœud.</p>
Nœuds d'administration/nœuds locaux	<p>Les messages d'audit sont envoyés au journal d'audit sur les nœuds d'administration, et les journaux d'événements de sécurité et d'applications sont stockés sur les nœuds qui les ont générés. Les informations d'audit sont stockées dans les fichiers suivants :</p> <ul style="list-style-type: none"> <li>• Nœuds d'administration (primaire et non primaire) : <code>/var/local/audit/export/audit.log</code></li> <li>• Tous les nœuds : le <code>/var/local/log/localaudit.log</code> fichier est généralement vide ou manquant. Il peut contenir des informations secondaires, telles qu'une copie supplémentaire de certains messages.</li> </ul>
Serveur syslog externe	<p>Les informations d'audit sont envoyées à un serveur syslog externe et enregistrées sur les nœuds locaux (<code>/var/local/log/localaudit.log</code>). Le type d'information envoyée dépend de la façon dont vous avez configuré le serveur syslog externe. Cette option n'est activée qu'après avoir configuré un serveur syslog externe.</p>
Nœud d'administration et serveur syslog externe	<p>Les messages d'audit sont envoyés au journal d'audit (<code>/var/local/audit/export/audit.log</code>) sur les nœuds d'administration, et les informations d'audit sont envoyées au serveur syslog externe et enregistrées sur le nœud local (<code>/var/local/log/localaudit.log</code>). Le type d'information envoyée dépend de la façon dont vous avez configuré le serveur syslog externe. Cette option n'est activée qu'après avoir configuré un serveur syslog externe.</p>

## 2. Sélectionnez **Enregistrer**.

Un message d'avertissement s'affiche.

## 3. Sélectionnez **OK** pour confirmer que vous souhaitez modifier la destination des informations d'audit.

Une bannière verte indique que la configuration d'audit a été enregistrée.

Les nouveaux journaux sont envoyés aux destinations que vous avez sélectionnées. Les journaux existants restent à leur emplacement actuel.

## Utiliser la surveillance SNMP

### Utiliser la surveillance SNMP

Si vous souhaitez surveiller StorageGRID à l'aide du protocole SNMP (simple Network Management Protocol), vous devez configurer l'agent SNMP inclus avec StorageGRID.

- ["Configurez l'agent SNMP"](#)
- ["Mettez à jour l'agent SNMP"](#)

### Capacités

Chaque nœud StorageGRID exécute un agent SNMP, ou démon, qui fournit une MIB. La MIB StorageGRID contient des définitions de tableau et de notification pour les alertes. La base MIB contient également des informations de description du système, telles que la plateforme et le numéro de modèle pour chaque nœud. Chaque nœud StorageGRID supporte également un sous-ensemble d'objets MIB-II.



Vérifiez ["Accéder aux fichiers MIB"](#) si vous souhaitez télécharger les fichiers MIB sur vos nœuds grid.

Au départ, le protocole SNMP est désactivé sur tous les nœuds. Lorsque vous configurez l'agent SNMP, tous les nœuds StorageGRID reçoivent la même configuration.

L'agent SNMP StorageGRID prend en charge les trois versions du protocole SNMP. Il fournit un accès MIB en lecture seule pour les requêtes et il peut envoyer deux types de notifications événementielle à un système de gestion :

### Recouvrements

Les interruptions sont des notifications envoyées par l'agent SNMP qui ne nécessitent pas d'accusé de réception par le système de gestion. Les interruptions servent à signaler au système de gestion qu'une alerte s'est produite au sein de StorageGRID, par exemple.

Les traps sont pris en charge dans les trois versions de SNMP.

### Informe

Les informations sont similaires aux pièges, mais elles nécessitent une reconnaissance par le système de gestion. Si l'agent SNMP ne reçoit pas d'accusé de réception dans un certain délai, il renvoie l'information jusqu'à ce qu'un accusé de réception soit reçu ou que la valeur de relance maximale ait été atteinte.

Les informations sont prises en charge dans SNMPv2c et SNMPv3.

Les notifications d'interruption et d'information sont envoyées dans les cas suivants :

- Une alerte par défaut ou personnalisée est déclenchée à tout niveau de gravité. Pour supprimer les notifications SNMP pour une alerte, vous devez ["configurer un silence"](#) pour l'alerte. Les notifications d'alerte sont envoyées par ["Nœud d'administration de l'expéditeur préféré"](#).

Chaque alerte est associée à l'un des trois types de déroutement en fonction du niveau de gravité de l'alerte : `activeMinorAlert`, `activeMajorAlert` et `activeCriticalAlert`. Pour obtenir la liste des alertes pouvant

déclencher ces interruptions, reportez-vous à la ["Référence des alertes"](#).

### Prise en charge de la version SNMP

Le tableau fournit un résumé détaillé des éléments pris en charge pour chaque version de SNMP.

	SNMPv1	SNMPv2c	SNMPv3
Requêtes (OBTENIR et GETNEXT)	Requêtes MIB en lecture seule	Requêtes MIB en lecture seule	Requêtes MIB en lecture seule
Authentification par requête	Chaîne de communauté	Chaîne de communauté	Utilisateur USM (User Security Model)
Notifications (PIÈGE et INFORMATION)	Traps uniquement	Pièges et information	Pièges et information
Authentification des notifications	Communauté d'interruptions par défaut ou chaîne de communauté personnalisée pour chaque destination d'interruption	Communauté d'interruptions par défaut ou chaîne de communauté personnalisée pour chaque destination d'interruption	Utilisateur USM pour chaque destination d'interruption

### Limites

- StorageGRID supporte l'accès MIB en lecture seule. L'accès en lecture/écriture n'est pas pris en charge.
- Tous les nœuds de la grille reçoivent la même configuration.
- SNMPv3 : StorageGRID ne prend pas en charge le mode support transport (TSM).
- SNMPv3 : le seul protocole d'authentification pris en charge est SHA (HMAC-SHA-96).
- SNMPv3 : le seul protocole de confidentialité pris en charge est AES.

### Configurez l'agent SNMP

Vous pouvez configurer l'agent SNMP StorageGRID pour qu'il utilise un système de gestion SNMP tiers pour l'accès MIB en lecture seule et les notifications.

#### Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Autorisation d'accès racine"](#).

#### Description de la tâche

L'agent SNMP StorageGRID prend en charge SNMPv1, SNMPv2c et SNMPv3. Vous pouvez configurer l'agent pour une ou plusieurs versions. Pour SNMPv3, seule l'authentification USM (User Security Model) est prise en charge.



Tous les nœuds de la grille utilisent la même configuration SNMP.

### Spécifiez la configuration de base

Dans un premier temps, activez l'agent SNMP StorageGRID et fournissez des informations de base.

### Étapes

1. Sélectionnez **CONFIGURATION > surveillance > agent SNMP**.

La page agent SNMP s'affiche.

2. Pour activer l'agent SNMP sur tous les nœuds de la grille, cochez la case **Activer SNMP**.
3. Entrez les informations suivantes dans la section Configuration de base.

Champ	Description
Contact système	Facultatif. Le contact principal du système StorageGRID, qui est renvoyé dans les messages SNMP en tant que sysContact.  Le contact système est généralement une adresse e-mail. Cette valeur s'applique à tous les nœuds du système StorageGRID. <b>Le contact système</b> peut comporter un maximum de 255 caractères.
Emplacement du système	Facultatif. Emplacement du système StorageGRID, qui est renvoyé dans les messages SNMP sous le nom sysLocation.  L'emplacement du système peut être toute information utile pour identifier l'emplacement de votre système StorageGRID. Par exemple, vous pouvez utiliser l'adresse d'un établissement. Cette valeur s'applique à tous les nœuds du système StorageGRID. <b>L'emplacement du système</b> peut comporter un maximum de 255 caractères.
Activer les notifications d'agent SNMP	<ul style="list-style-type: none"><li>• Si cette option est sélectionnée, l'agent SNMP StorageGRID envoie des notifications d'interruption et d'information.</li><li>• Si cette option n'est pas sélectionnée, l'agent SNMP prend en charge l'accès MIB en lecture seule, mais n'envoie pas de notifications SNMP.</li></ul>
Activer les interruptions d'authentification	Si cette option est sélectionnée, l'agent SNMP StorageGRID envoie des interruptions d'authentification s'il reçoit des messages de protocole authentifiés de manière incorrecte.

### Entrez des chaînes de communauté

Si vous utilisez SNMPv1 ou SNMPv2c, complétez la section chaînes de communauté.

Lorsque le système de gestion interroge la MIB StorageGRID, il envoie une chaîne de communauté. Si la chaîne de communauté correspond à l'une des valeurs spécifiées ici, l'agent SNMP envoie une réponse au système de gestion.

## Étapes

1. Pour **communauté en lecture seule**, vous pouvez éventuellement entrer une chaîne de communauté pour autoriser l'accès MIB en lecture seule sur les adresses d'agent IPv4 et IPv6.



Pour garantir la sécurité de votre système StorageGRID, n'utilisez pas la chaîne de communauté « public ». Si vous laissez ce champ vide, l'agent SNMP utilise l'ID de grille de votre système StorageGRID comme chaîne de communauté.

Chaque chaîne de communauté peut comporter un maximum de 32 caractères et ne peut pas contenir de caractères d'espace.

2. Sélectionnez **Ajouter une autre chaîne de communauté** pour ajouter des chaînes supplémentaires.

Jusqu'à cinq chaînes sont autorisées.

### Créer des destinations de déROUTement

Utilisez l'onglet destinations d'interruption de la section autres configurations pour définir une ou plusieurs destinations pour les notifications d'interruption ou d'information StorageGRID. Lorsque vous activez l'agent SNMP et sélectionnez **Enregistrer**, StorageGRID envoie des notifications à chaque destination définie lorsque des alertes sont déclenchées. Les notifications standard sont également envoyées pour les entités MIB-II prises en charge (par exemple, ifdown et coldStart).

## Étapes

1. Pour le champ **Default trap community**, vous pouvez éventuellement saisir la chaîne de communauté par défaut que vous souhaitez utiliser pour les destinations d'interruption SNMPv1 ou SNMPv2.

Si nécessaire, vous pouvez fournir une chaîne de communauté différente (« personnalisée ») lorsque vous définissez une destination d'interruption spécifique.

**La communauté de recouvrement par défaut** peut comporter 32 caractères maximum et ne peut pas contenir de caractères d'espace.

2. Pour ajouter une destination d'interruption, sélectionnez **Créer**.
3. Sélectionnez la version SNMP qui sera utilisée pour cette destination d'interruption.
4. Remplissez le formulaire Créer une destination d'interruption pour la version que vous avez sélectionnée.

### SNMPv1

Si vous avez sélectionné SNMPv1 comme version, renseignez ces champs.

Champ	Description
Type	Doit être Trap pour SNMPv1.
Hôte	Une adresse IPv4 ou IPv6 ou un nom de domaine complet (FQDN) pour recevoir l'interruption.
Port	Utilisez 162, le port standard pour les interruptions SNMP, sauf si vous devez utiliser une autre valeur.
Protocole	Utilisez UDP, qui est le protocole de déROUTement SNMP standard, sauf si vous avez besoin d'utiliser TCP.
Chaîne de communauté	Utilisez la communauté d'interruptions par défaut, si elle a été spécifiée, ou entrez une chaîne de communauté personnalisée pour cette destination d'interruptions.  La chaîne de communauté personnalisée peut comporter jusqu'à 32 caractères et ne peut pas contenir d'espace.

### SNMPv2c

Si vous avez sélectionné SNMPv2c comme version, renseignez ces champs.

Champ	Description
Type	Indique si la destination sera utilisée pour les interruptions ou les informations.
Hôte	Une adresse IPv4 ou IPv6 ou un nom de domaine complet pour recevoir l'interruption.
Port	Utilisez 162, qui est le port standard pour les interruptions SNMP, sauf si vous devez utiliser une autre valeur.
Protocole	Utilisez UDP, qui est le protocole de déROUTement SNMP standard, sauf si vous avez besoin d'utiliser TCP.
Chaîne de communauté	Utilisez la communauté d'interruptions par défaut, si elle a été spécifiée, ou entrez une chaîne de communauté personnalisée pour cette destination d'interruptions.  La chaîne de communauté personnalisée peut comporter jusqu'à 32 caractères et ne peut pas contenir d'espace.

### SNMPv3

Si vous avez sélectionné SNMPv3 comme version, renseignez ces champs.

Champ	Description
Type	Indique si la destination sera utilisée pour les interruptions ou les informations.
Hôte	Une adresse IPv4 ou IPv6 ou un nom de domaine complet pour recevoir l'interruption.
Port	Utilisez 162, qui est le port standard pour les interruptions SNMP, sauf si vous devez utiliser une autre valeur.
Protocole	Utilisez UDP, qui est le protocole de déROUTement SNMP standard, sauf si vous avez besoin d'utiliser TCP.
Utilisateur USM	Utilisateur USM qui sera utilisé pour l'authentification. <ul style="list-style-type: none"><li>• Si vous avez sélectionné <b>Trap</b>, seuls les utilisateurs d'USM sans ID de moteur faisant autorité sont affichés.</li><li>• Si vous avez sélectionné <b>INFORM</b>, seuls les utilisateurs d'USM avec des ID de moteur faisant autorité sont affichés.</li><li>• Si aucun utilisateur n'est affiché :<ol style="list-style-type: none"><li>i. Créez et enregistrez la destination de l'interruption.</li><li>ii. Accédez à <a href="#">Créez des utilisateurs USM</a> et créez l'utilisateur.</li><li>iii. Revenez à l'onglet destinations des interruptions, sélectionnez la destination enregistrée dans le tableau et sélectionnez <b>Modifier</b>.</li><li>iv. Sélectionnez l'utilisateur.</li></ol></li></ul>

##### 5. Sélectionnez **Créer**.

La destination de la trappe est créée et ajoutée à la table.

#### Créez des adresses d'agent

Vous pouvez également utiliser l'onglet adresses des agents de la section autres configurations pour spécifier une ou plusieurs « adresses d'écoute ». Il s'agit des adresses StorageGRID sur lesquelles l'agent SNMP peut recevoir des requêtes.

Si vous ne configurez pas d'adresse d'agent, l'adresse d'écoute par défaut est le port UDP 161 sur tous les réseaux StorageGRID.

#### Étapes

1. Sélectionnez **Créer**.
2. Entrez les informations suivantes.

Champ	Description
Protocole Internet	Indique si cette adresse utilisera IPv4 ou IPv6.  Par défaut, SNMP utilise IPv4.
Protocole de transport	Indique si cette adresse utilise UDP ou TCP.  Par défaut, SNMP utilise UDP.
Réseau StorageGRID	Quel réseau StorageGRID l'agent écoutera ? <ul style="list-style-type: none"> <li>• Réseaux Grid, Admin et client : l'agent SNMP écoute les requêtes sur les trois réseaux.</li> <li>• Réseau Grid</li> <li>• Réseau d'administration</li> <li>• Réseau client</li> </ul> <p><b>Remarque</b> : si vous utilisez le réseau client pour des données non sécurisées et que vous créez une adresse d'agent pour le réseau client, sachez que le trafic SNMP sera également non sécurisé.</p>
Port	Éventuellement, le numéro de port sur lequel l'agent SNMP doit écouter.  Le port UDP par défaut d'un agent SNMP est 161, mais vous pouvez entrer n'importe quel numéro de port inutilisé.  <b>Remarque</b> : lorsque vous enregistrez l'agent SNMP, StorageGRID ouvre automatiquement les ports d'adresse de l'agent sur le pare-feu interne. Vous devez vous assurer que tous les pare-feu externes autorisent l'accès à ces ports.

### 3. Sélectionnez **Créer**.

L'adresse de l'agent est créée et ajoutée à la table.

#### Créez des utilisateurs USM

Si vous utilisez SNMPv3, utilisez l'onglet utilisateurs USM de la section autres configurations pour définir les utilisateurs USM autorisés à interroger la MIB ou à recevoir des interruptions et des informations.



Les destinations SNMPv3 *INFORM* doivent avoir des utilisateurs avec des ID de moteur. SNMPv3 *trap* destination ne peut pas avoir d'utilisateurs avec des ID de moteur.

Ces étapes ne s'appliquent pas si vous utilisez uniquement SNMPv1 ou SNMPv2c.

#### Étapes

##### 1. Sélectionnez **Créer**.

2. Entrez les informations suivantes.

Champ	Description
Nom d'utilisateur	<p>Un nom unique pour cet utilisateur USM.</p> <p>Les noms d'utilisateur peuvent comporter jusqu'à 32 caractères et ne peuvent pas contenir de caractères d'espace. Le nom d'utilisateur ne peut pas être modifié après la création de l'utilisateur.</p>
Accès MIB en lecture seule	<p>Si cette option est sélectionnée, cet utilisateur doit disposer d'un accès en lecture seule à la MIB.</p>
ID de moteur autoritaire	<p>Si cet utilisateur sera utilisé dans une destination INFORM, l'ID de moteur faisant autorité pour cet utilisateur.</p> <p>Entrez 10 à 64 caractères hexadécimaux (5 à 32 octets) sans espace. Cette valeur est requise pour les utilisateurs USM qui seront sélectionnés dans les destinations d'interruption pour les informations. Cette valeur n'est pas autorisée pour les utilisateurs USM qui seront sélectionnés dans les destinations d'interruption pour les interruptions.</p> <p><b>Remarque</b> : ce champ n'est pas affiché si vous avez sélectionné <b>accès MIB en lecture seule</b> car les utilisateurs USM qui ont un accès MIB en lecture seule ne peuvent pas avoir d'ID moteur.</p>
Niveau de sécurité	<p>Le niveau de sécurité de l'utilisateur USM :</p> <ul style="list-style-type: none"> <li>• <b>AuthPriv</b> : cet utilisateur communique avec l'authentification et la confidentialité (cryptage). Vous devez spécifier un protocole d'authentification et un mot de passe ainsi qu'un protocole de confidentialité et un mot de passe.</li> <li>• <b>AuthNoPriv</b>: Cet utilisateur communique avec l'authentification et sans confidentialité (pas de cryptage). Vous devez spécifier un protocole d'authentification et un mot de passe.</li> </ul>
Protocole d'authentification	<p>Toujours défini sur SHA, qui est le seul protocole pris en charge (HMAC-SHA-96).</p>
Mot de passe	<p>Le mot de passe que cet utilisateur utilisera pour l'authentification.</p>
Protocole de confidentialité	<p>Affiché uniquement si vous avez sélectionné <b>authPriv</b> et toujours réglé sur AES, qui est le seul protocole de confidentialité pris en charge.</p>
Mot de passe	<p>Affiché uniquement si vous avez sélectionné <b>authPriv</b>. Le mot de passe que cet utilisateur utilisera pour la confidentialité.</p>

3. Sélectionnez **Créer**.

L'utilisateur USM est créé et ajouté à la table.

4. Une fois la configuration de l'agent SNMP terminée, sélectionnez **Enregistrer**.

La nouvelle configuration de l'agent SNMP devient active.

## Mettez à jour l'agent SNMP

Vous pouvez désactiver les notifications SNMP, mettre à jour les chaînes de communauté ou ajouter ou supprimer des adresses d'agent, des utilisateurs USM et des destinations d'interruption.

### Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Autorisation d'accès racine"](#).

### Description de la tâche

Pour plus de détails sur chaque champ de la page agent SNMP, reportez-vous à la section ["Configurez l'agent SNMP"](#). Vous devez sélectionner **Enregistrer** au bas de la page pour valider les modifications que vous apportez à chaque onglet.

### Étapes

1. Sélectionnez **CONFIGURATION > surveillance > agent SNMP**.

La page agent SNMP s'affiche.

2. Pour désactiver l'agent SNMP sur tous les nœuds de la grille, décochez la case **Activer SNMP** et sélectionnez **Enregistrer**.

Si vous réactivez l'agent SNMP, tous les paramètres de configuration SNMP précédents sont conservés.

3. Si vous le souhaitez, mettez à jour les informations de la section Configuration de base :

- a. Si nécessaire, mettez à jour le **contact système** et **emplacement système**.
- b. Vous pouvez également cocher ou décocher la case **Activer les notifications d'agent SNMP** pour contrôler si l'agent SNMP StorageGRID envoie des notifications d'interruption et d'information.

Lorsque cette case est décochée, l'agent SNMP prend en charge l'accès MIB en lecture seule, mais n'envoie pas de notifications SNMP.

- c. Si vous le souhaitez, cochez ou décochez la case **Activer les interruptions d'authentification** pour contrôler si l'agent SNMP StorageGRID envoie des interruptions d'authentification lorsqu'il reçoit des messages de protocole incorrectement authentifiés.

4. Si vous utilisez SNMPv1 ou SNMPv2c, vous pouvez éventuellement mettre à jour ou ajouter une communauté **en lecture seule** dans la section chaînes de communauté.

5. Pour mettre à jour les destinations des interruptions, sélectionnez l'onglet destinations des interruptions dans la section autres configurations.

Utilisez cet onglet pour définir une ou plusieurs destinations pour les notifications d'interruption StorageGRID ou d'information. Lorsque vous activez l'agent SNMP et sélectionnez **Enregistrer**, StorageGRID envoie des notifications à chaque destination définie lorsque des alertes sont déclenchées. Les notifications standard sont également envoyées pour les entités MIB-II prises en charge (par exemple,

ifdown et coldStart).

Pour plus de détails sur ce que vous devez saisir, reportez-vous à ["Créer des destinations de recouvrement"](#) la section .

- Vous pouvez également mettre à jour ou supprimer la communauté de dérouterments par défaut.

Si vous supprimez la communauté d'interruptions par défaut, vous devez d'abord vous assurer que toutes les destinations d'interruptions existantes utilisent une chaîne de communauté personnalisée.

- Pour ajouter une destination d'interruption, sélectionnez **Créer**.
- Pour modifier une destination d'interruption, sélectionnez le bouton radio et sélectionnez **Modifier**.
- Pour supprimer une destination d'interruption, sélectionnez le bouton radio et sélectionnez **Supprimer**.
- Pour valider vos modifications, sélectionnez **Enregistrer** en bas de la page.

6. Pour mettre à jour les adresses des agents, sélectionnez l'onglet adresses des agents dans la section autres configurations.

Utilisez cet onglet pour spécifier une ou plusieurs « adresses d'écoute ». Il s'agit des adresses StorageGRID sur lesquelles l'agent SNMP peut recevoir des requêtes.

Pour plus de détails sur ce que vous devez saisir, reportez-vous à ["Créez des adresses d'agent"](#) la section .

- Pour ajouter une adresse d'agent, sélectionnez **Créer**.
- Pour modifier une adresse d'agent, sélectionnez le bouton radio et sélectionnez **Modifier**.
- Pour supprimer une adresse d'agent, sélectionnez le bouton radio et sélectionnez **Supprimer**.
- Pour valider vos modifications, sélectionnez **Enregistrer** en bas de la page.

7. Pour mettre à jour les utilisateurs USM, sélectionnez l'onglet utilisateurs USM dans la section autres configurations.

Utilisez cet onglet pour définir les utilisateurs USM autorisés à interroger la MIB ou à recevoir des interruptions et des informations.

Pour plus de détails sur ce que vous devez saisir, reportez-vous à ["Créez des utilisateurs USM"](#) la section .

- Pour ajouter un utilisateur USM, sélectionnez **Create**.
- Pour modifier un utilisateur USM, sélectionnez le bouton radio et sélectionnez **Modifier**.

Le nom d'utilisateur d'un utilisateur USM existant ne peut pas être modifié. Si vous devez modifier un nom d'utilisateur, vous devez le supprimer et en créer un nouveau.



Si vous ajoutez ou supprimez l'ID de moteur d'un utilisateur faisant autorité et que cet utilisateur est actuellement sélectionné pour une destination, vous devez modifier ou supprimer la destination. Sinon, une erreur de validation se produit lorsque vous enregistrez la configuration de l'agent SNMP.

- Pour supprimer un utilisateur USM, sélectionnez le bouton radio et sélectionnez **Supprimer**.





Si l'utilisateur que vous avez supprimé est actuellement sélectionné pour une destination d'interruption, vous devez modifier ou supprimer la destination. Sinon, une erreur de validation se produit lorsque vous enregistrez la configuration de l'agent SNMP.

- Pour valider vos modifications, sélectionnez **Enregistrer** en bas de la page.

8. Lorsque vous avez mis à jour la configuration de l'agent SNMP, sélectionnez **Enregistrer**.

### Accéder aux fichiers MIB

Les fichiers MIB contiennent des définitions et des informations sur les propriétés des ressources et services gérés pour les nœuds de votre grille. Vous pouvez accéder aux fichiers MIB qui définissent les objets et les notifications pour StorageGRID. Ces fichiers peuvent être utiles pour la surveillance de votre grille.

Voir "[Utiliser la surveillance SNMP](#)" pour plus d'informations sur les fichiers SNMP et MIB.

### Accéder aux fichiers MIB

Procédez comme suit pour accéder aux fichiers MIB.

### Étapes

1. Sélectionnez **CONFIGURATION > surveillance > agent SNMP**.
2. Sur la page agent SNMP, sélectionnez le fichier à télécharger :
  - **NETAPP-STORAGEGRID-MIB.txt** : définit la table d'alertes et les notifications (traps) accessibles sur tous les nœuds d'administration.
  - **ES-NETAPP-06-MIB.mib** : définit les objets et les notifications pour les appliances basées sur E-Series.
  - **MIB\_1\_10.zip** : définit les objets et les notifications pour les appareils dotés d'une interface BMC.



Vous pouvez également accéder aux fichiers MIB à l'emplacement suivant sur n'importe quel nœud StorageGRID : `/usr/share/snmp/mibs`

3. Pour extraire les OID StorageGRID du fichier MIB :

- a. Obtenir l'OID de la racine de la MIB StorageGRID :

```
root@user-adm1:~ # snmptranslate -On -IR storagegrid
```

Résultat : `.1.3.6.1.4.1.789.28669` (28669 est toujours l'OID pour StorageGRID)

- a. Grep pour l'OID StorageGRID dans toute l'arborescence (utilisation de `paste` pour joindre les lignes) :

```
root@user-adm1:~ # snmptranslate -Tso | paste -d " " - - | grep 28669
```



La `snmptranslate` commande a de nombreuses options qui sont utiles pour explorer la MIB. Cette commande est disponible sur n'importe quel nœud StorageGRID.

## Contenu du fichier MIB

Tous les objets se trouvent sous l'OID StorageGRID.

Nom de l'objet	ID objet (OID)	Description
		Le module MIB pour les entités NetApp StorageGRID.

## Objets MIB

Nom de l'objet	ID objet (OID)	Description
ActiveAlertCount		Nombre d'alertes actives dans activeAlertTable.
ActiveAlertTable		Tableau des alertes actives dans StorageGRID.
ActiveAlertId		ID de l'alerte. Uniquement unique dans l'ensemble actuel d'alertes actives.
ActiveAlertName		Nom de l'alerte.
ActiveAlertInstance		Nom de l'entité qui a généré l'alerte, en général le nom du nœud.
ActiveAlertSeverity		Gravité de l'alerte.
ActiveAlertStartTime		Date et heure de déclenchement de l'alerte.

## Types de notification (interruptions)

Toutes les notifications incluent les variables suivantes en tant que variables :

- ActiveAlertId
- ActiveAlertName
- ActiveAlertInstance
- ActiveAlertSeverity
- ActiveAlertStartTime

Type de notification	ID objet (OID)	Description
ActiveMinorAlert		Alerte avec gravité mineure
ActiveMajorAlert		Alerte de gravité majeure
ActiveCriticalAlert		Alerte avec gravité critique

## Collecte de données StorageGRID supplémentaires

### Utilisez des graphiques et des graphiques

Vous pouvez utiliser des graphiques et des rapports pour surveiller l'état du système StorageGRID et résoudre les problèmes.

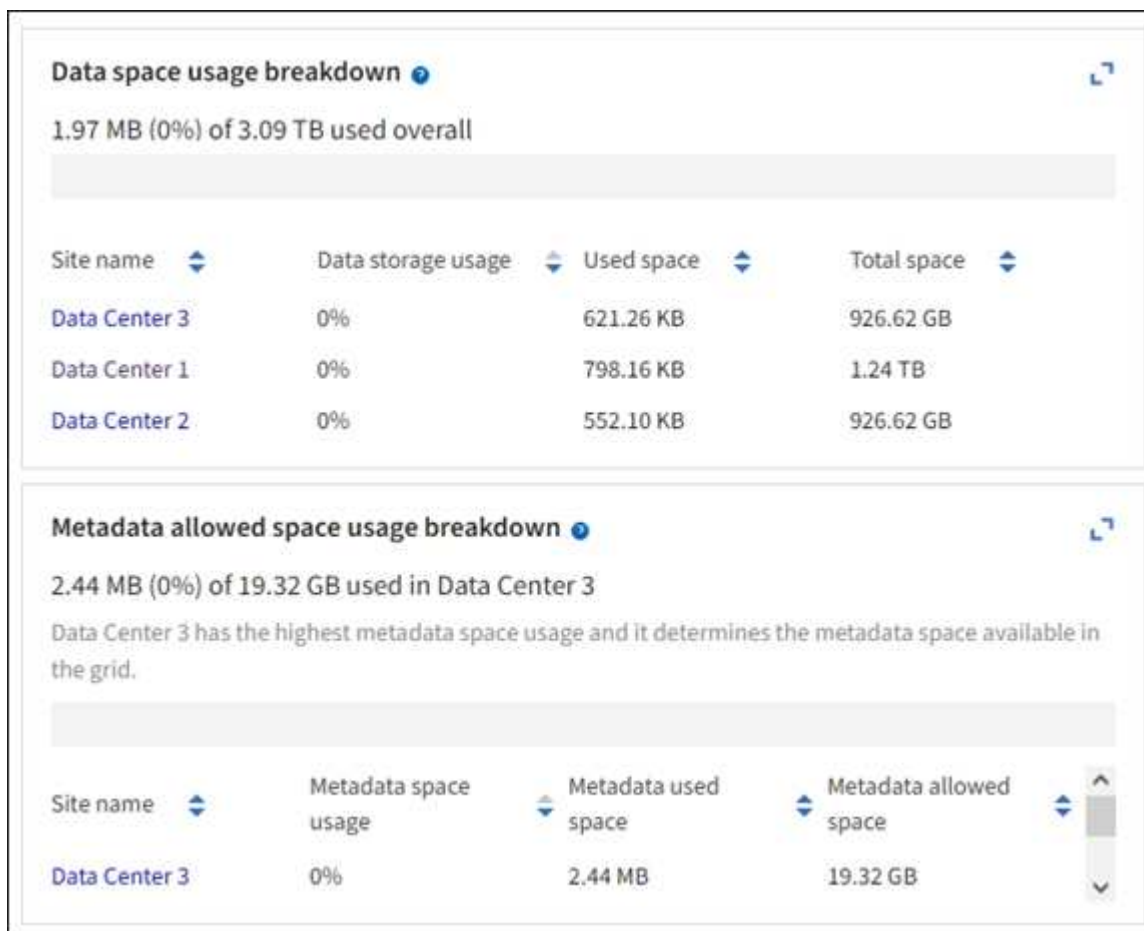


Le Gestionnaire de grille est mis à jour avec chaque version et peut ne pas correspondre aux exemples de captures d'écran de cette page.

### Types de graphiques

Les graphiques et les graphiques résumés les valeurs des mesures et des attributs StorageGRID spécifiques.

Le tableau de bord Grid Manager inclut des cartes qui résumés le stockage disponible pour la grille et chaque site.



Le panneau Storage usage (utilisation du stockage) du tableau de bord du gestionnaire de locataires affiche les informations suivantes :

- Liste des compartiments les plus grands (S3) ou des conteneurs (Swift) du locataire
- Un graphique à barres qui représente les tailles relatives des grands godets ou conteneurs
- La quantité totale d'espace utilisé et, si un quota est défini, la quantité et le pourcentage d'espace restant

# Dashboard

**16** Buckets  
View buckets

**2** Platform services endpoints  
View endpoints

**0** Groups  
View groups

**1** User  
View users

## Storage usage [?](#)

6.5 TB of 7.2 TB used

0.7 TB (10.1%) remaining



Bucket name	Space used	Number of objects
Bucket-15	969.2 GB	913,425
Bucket-04	937.2 GB	576,806
Bucket-13	815.2 GB	957,389
Bucket-06	812.5 GB	193,843
Bucket-10	473.9 GB	583,245
Bucket-03	403.2 GB	981,226
Bucket-07	362.5 GB	420,726
Bucket-05	294.4 GB	785,190
8 other buckets	1.4 TB	3,007,036

## Top buckets by capacity limit usage [?](#)

Bucket name	Usage
Bucket-10	82%
Bucket-03	57%
Bucket-15	20%

## Tenant details [?](#)

Name: Tenant02  
ID: 3341 1240 0546 8283 2208

- ✓ Platform services enabled
- ✓ Can use own identity source
- ✓ S3 Select enabled

De plus, les graphiques qui montrent comment les mesures et les attributs StorageGRID changent au fil du temps sont disponibles à partir de la page nœuds et de la page **SUPPORT > Outils > topologie de grille**.

Il existe quatre types de graphiques :

- **Graphiques Grafana** : affichés sur la page nœuds, les graphiques Grafana sont utilisés pour tracer les valeurs des metrics Prometheus dans le temps. Par exemple, l'onglet **NOEUDS > réseau** d'un nœud de stockage comprend un tableau Grafana pour le trafic réseau.

# DC1-S2 (Storage Node)

Overview

Hardware

Network

Storage

Objects

ILM

Tasks

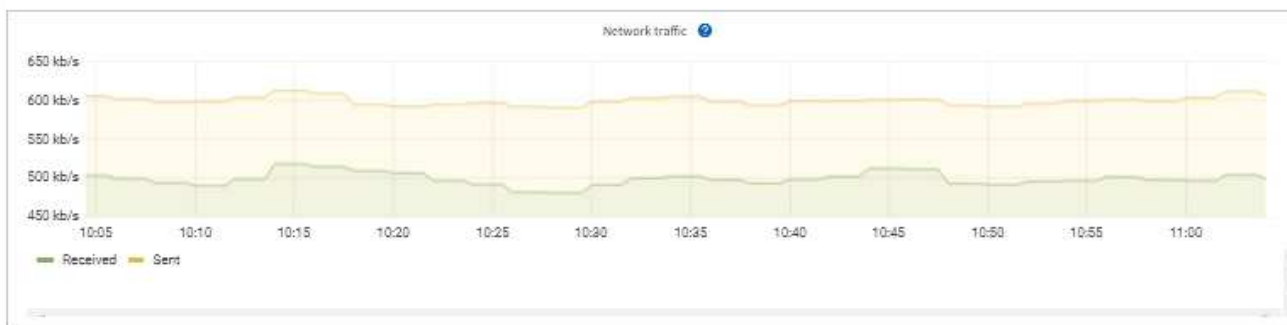
1 hour

1 day

1 week

1 month

Custom



## Network interfaces

Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status
eth0	00:50:56:A7:E8:1D	10 Gigabit	Full	Off	Up

## Network communication

### Receive


Interface	Data	Packets	Errors	Dropped	Frame overruns	Frames
eth0	3.04 GB	20,403,428	0	24,899	0	0

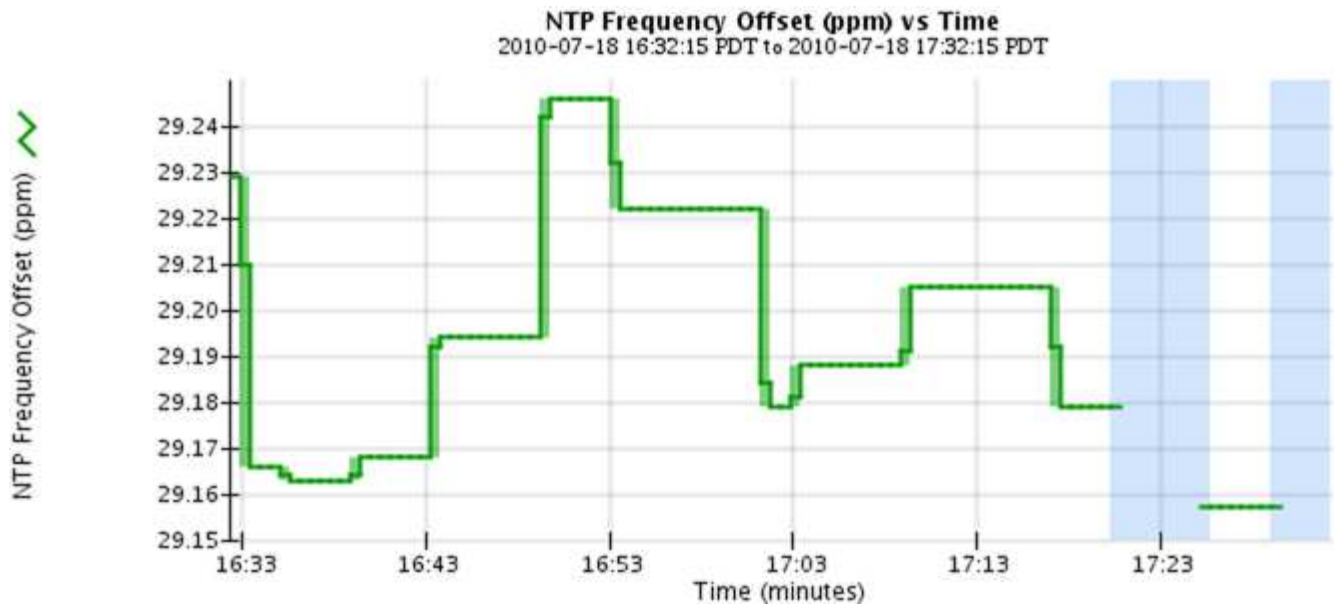
### Transmit


Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	3.65 GB	19,061,947	0	0	0	0

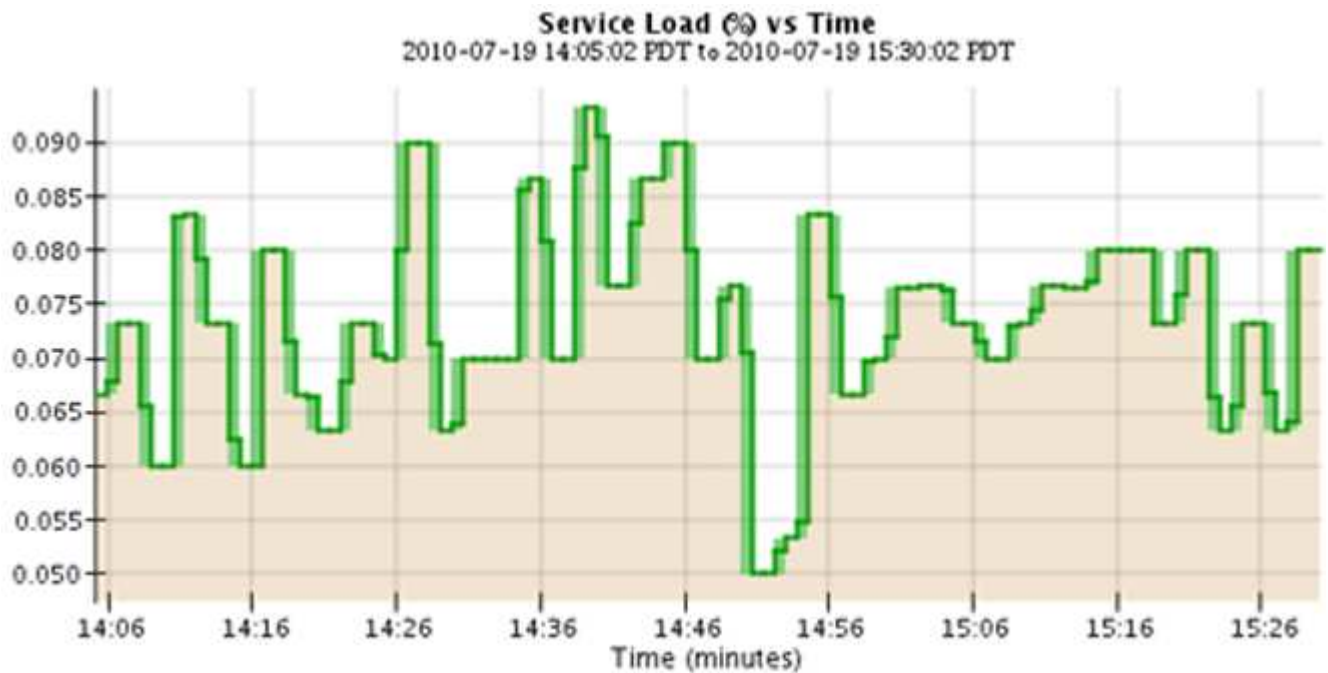


Les graphiques Grafana sont également inclus dans les tableaux de bord pré-construits disponibles à partir de la page **SUPPORT > Tools > Metrics**.

- **Graphiques linéaires** : disponibles à partir de la page nœuds et de la page **SUPPORT > Outils > topologie de grille** (sélectionnez l'icône de graphique  après une valeur de données), les graphiques linéaires sont utilisés pour tracer les valeurs des attributs StorageGRID ayant une valeur unitaire (comme le décalage de fréquence NTP, en ppm). Les modifications de la valeur sont tracées dans des intervalles de données réguliers (bacs) au fil du temps.



- **Graphiques de surface** : disponibles à partir de la page nœuds et de la page **SUPPORT > Outils > topologie de grille** (sélectionnez l'icône de graphique  après une valeur de données), les graphiques de zone sont utilisés pour tracer les quantités d'attributs volumétriques, telles que les nombres d'objets ou les valeurs de charge de service. Les graphiques de zone sont similaires aux graphiques de ligne, mais incluent un ombrage marron clair en dessous de la ligne. Les modifications de la valeur sont tracées dans des intervalles de données réguliers (bacs) au fil du temps.



- Certains graphiques sont signalés par un autre type d'icône de graphique  et ont un format différent :


1 hour      1 day      1 week      1 month      Custom

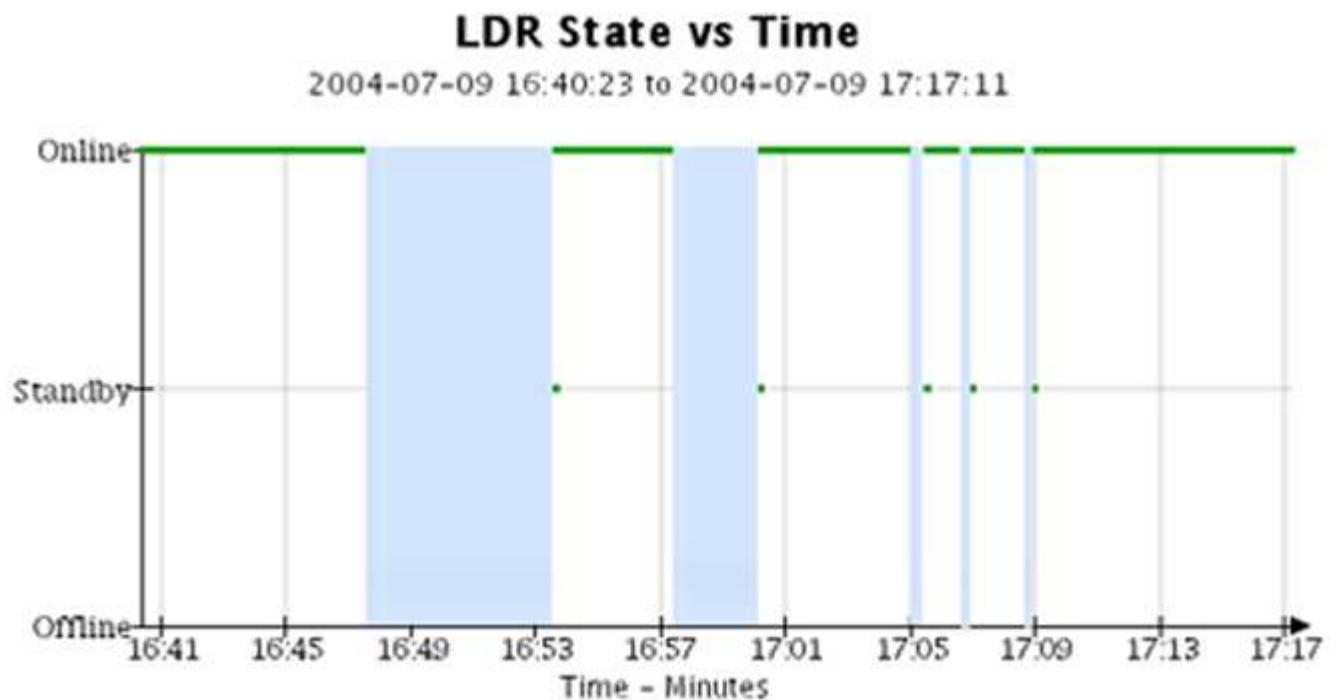
From: 2020-10-01 [calendar icon] 12 : 45 PM PDT

To: 2020-10-01 [calendar icon] 01 : 10 PM PDT [Apply](#)



[Close](#)

- **Graphique d'état** : disponible à partir de la page **SUPPORT > Outils > topologie de grille** (sélectionnez l'icône du graphique  après une valeur de données), les graphiques d'état sont utilisés pour tracer des valeurs d'attribut représentant des États distincts, tels qu'un état de service pouvant être en ligne, en veille ou hors ligne. Les graphiques d'état sont similaires aux graphiques linéaires, mais la transition est discontinue. En d'autres termes, la valeur passe d'une valeur d'état à une autre.









Informations associées

- ["Afficher la page nœuds"](#)
- ["Afficher l'arborescence de la grille topologique"](#)
- ["Examinez les metrics de support"](#)

### Légende du graphique

Les lignes et les couleurs utilisées pour dessiner des graphiques ont une signification spécifique.

Exemple	Signification
	Les valeurs des attributs signalés sont tracées à l'aide de lignes vert foncé.
	Un ombrage vert clair autour des lignes vert foncé indique que les valeurs réelles de cette plage horaire varient et ont été « regroupées » pour un tracé plus rapide. La ligne foncée représente la moyenne pondérée. La plage en vert clair indique les valeurs maximum et minimum dans le bac. L'ombrage marron clair est utilisé pour les graphiques de zone pour indiquer les données volumétriques.
	Les zones vierges (aucune donnée tracée) indiquent que les valeurs d'attribut ne sont pas disponibles. L'arrière-plan peut être bleu, gris ou un mélange de gris et de bleu, selon l'état du service signalant l'attribut.
	L'ombrage bleu clair indique que certaines ou toutes les valeurs d'attribut à ce moment étaient indéterminées ; l'attribut n'a pas signalé de valeurs parce que le service était dans un état inconnu.
	L'ombrage gris indique que certaines ou toutes les valeurs d'attribut à ce moment n'étaient pas connues car le service signalant les attributs était administrativement en panne.
	Un mélange d'ombrage gris et bleu indique que certaines des valeurs d'attribut au moment étaient indéterminées (parce que le service était dans un état inconnu), tandis que d'autres n'étaient pas connus car le service signalant les attributs était administrativement en panne.

### Affichez des graphiques et des graphiques

La page nœuds contient les graphiques et les graphiques auxquels vous devez accéder régulièrement pour surveiller les attributs tels que la capacité de stockage et le débit. Dans certains cas, en particulier lorsque vous travaillez avec le support technique, vous pouvez utiliser la page **SUPPORT** > **Outils** > **topologie de grille** pour accéder à des graphiques supplémentaires.

### Avant de commencer

Vous devez être connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).

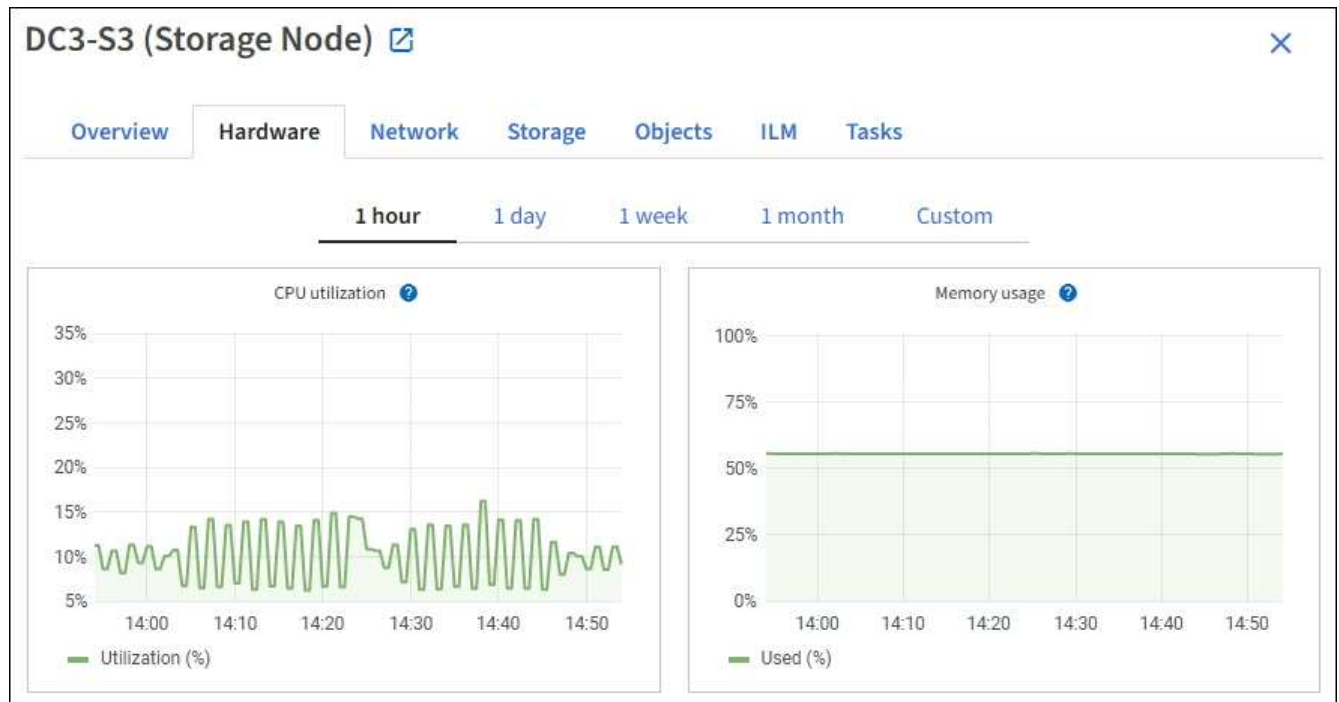
### Étapes

1. Sélectionnez **NOEUDS**. Ensuite, sélectionnez un nœud, un site ou la grille entière.
2. Sélectionnez l'onglet pour lequel vous souhaitez afficher les informations.

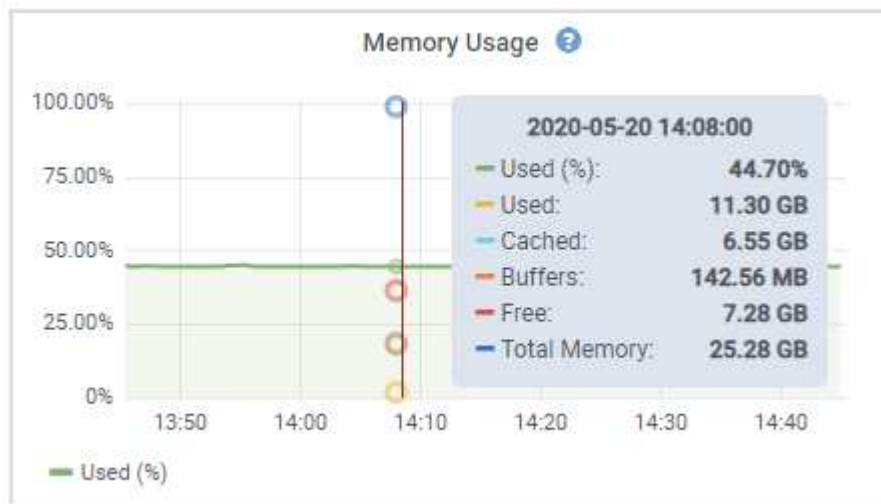
Certains onglets comprennent un ou plusieurs graphiques Grafana, qui sont utilisés pour tracer les valeurs



des metrics Prometheus dans le temps. Par exemple, l'onglet **NODES** > **Hardware** d'un noeud comprend deux diagrammes Grafana.




3. Si vous le souhaitez, placez votre curseur sur le graphique pour afficher des valeurs plus détaillées pour un point particulier dans le temps.



4. Si nécessaire, vous pouvez souvent afficher un graphique pour un attribut ou une mesure spécifique. Dans le tableau de la page nœuds, sélectionnez l'icône de graphique  située à droite du nom de l'attribut.

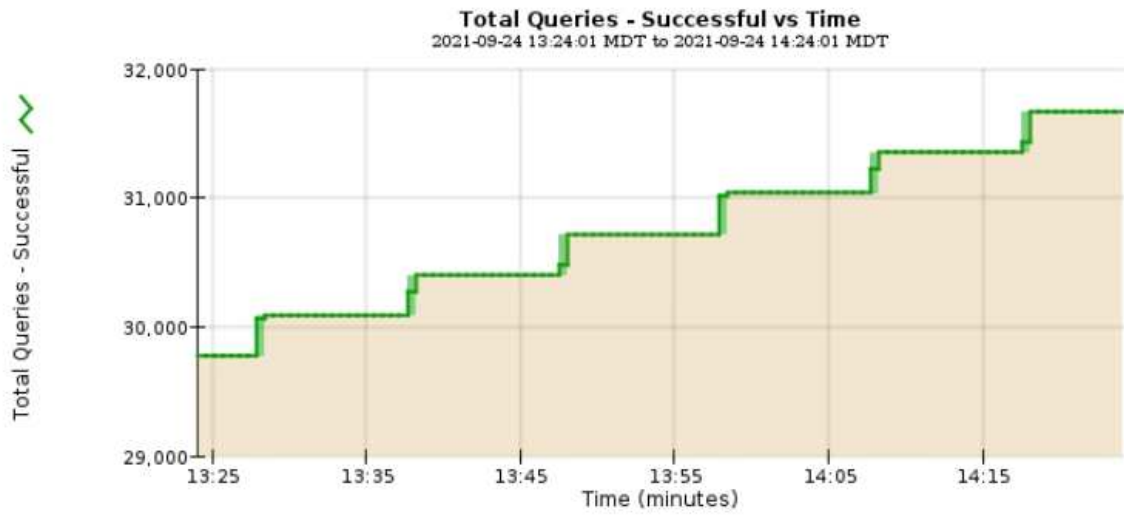


Les graphiques ne sont pas disponibles pour toutes les mesures et tous les attributs.

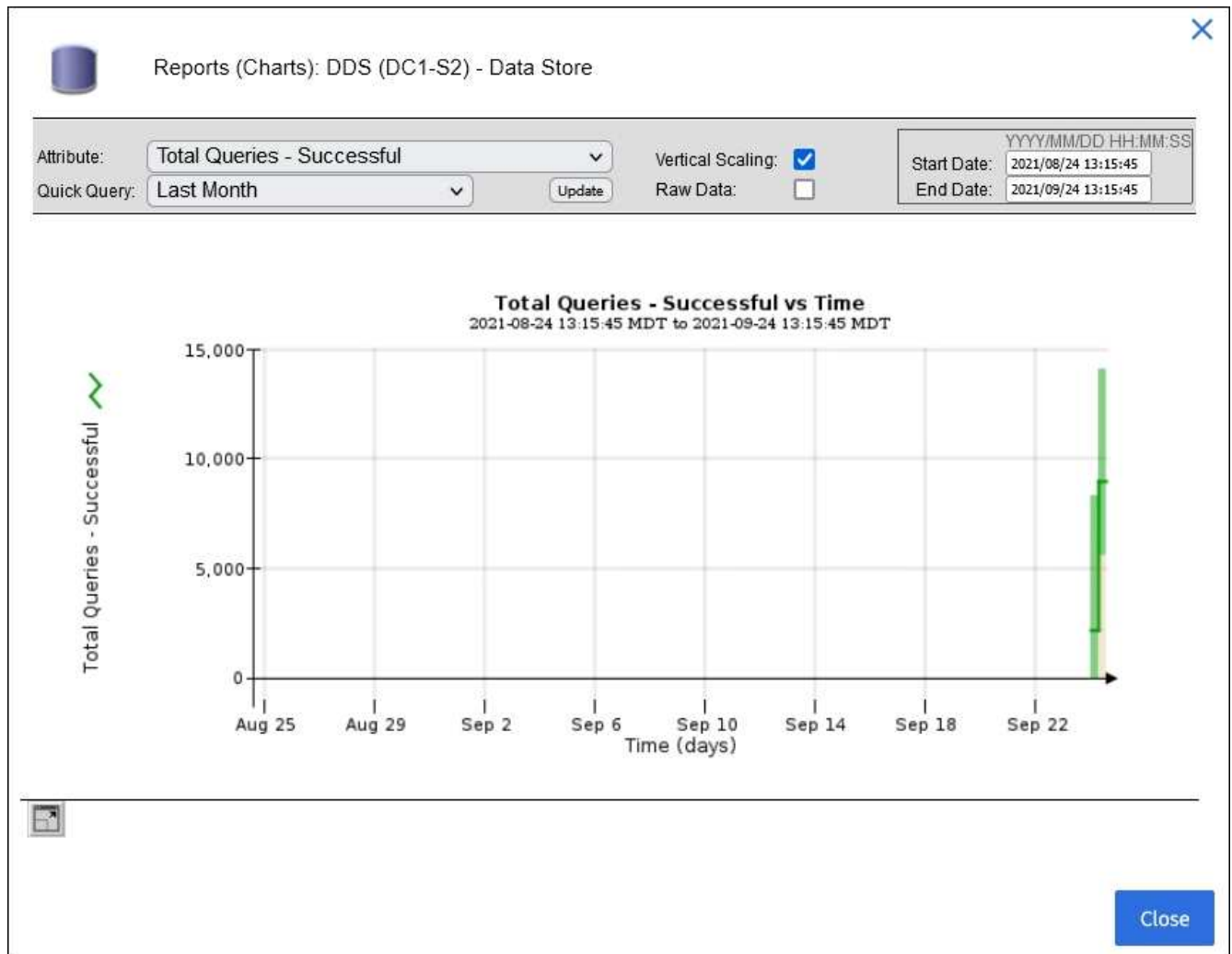
**Exemple 1** : dans l'onglet objets d'un noeud de stockage, vous pouvez sélectionner l'icône du diagramme  pour voir le nombre total de requêtes de stockage de métadonnées réussies pour le noeud de stockage.



Attribute: Total Queries - Successful Vertical Scaling:   
Quick Query: Last Hour Update Raw Data:   
Start Date: 2021/09/24 13:24:01 End Date: 2021/09/24 14:24:01




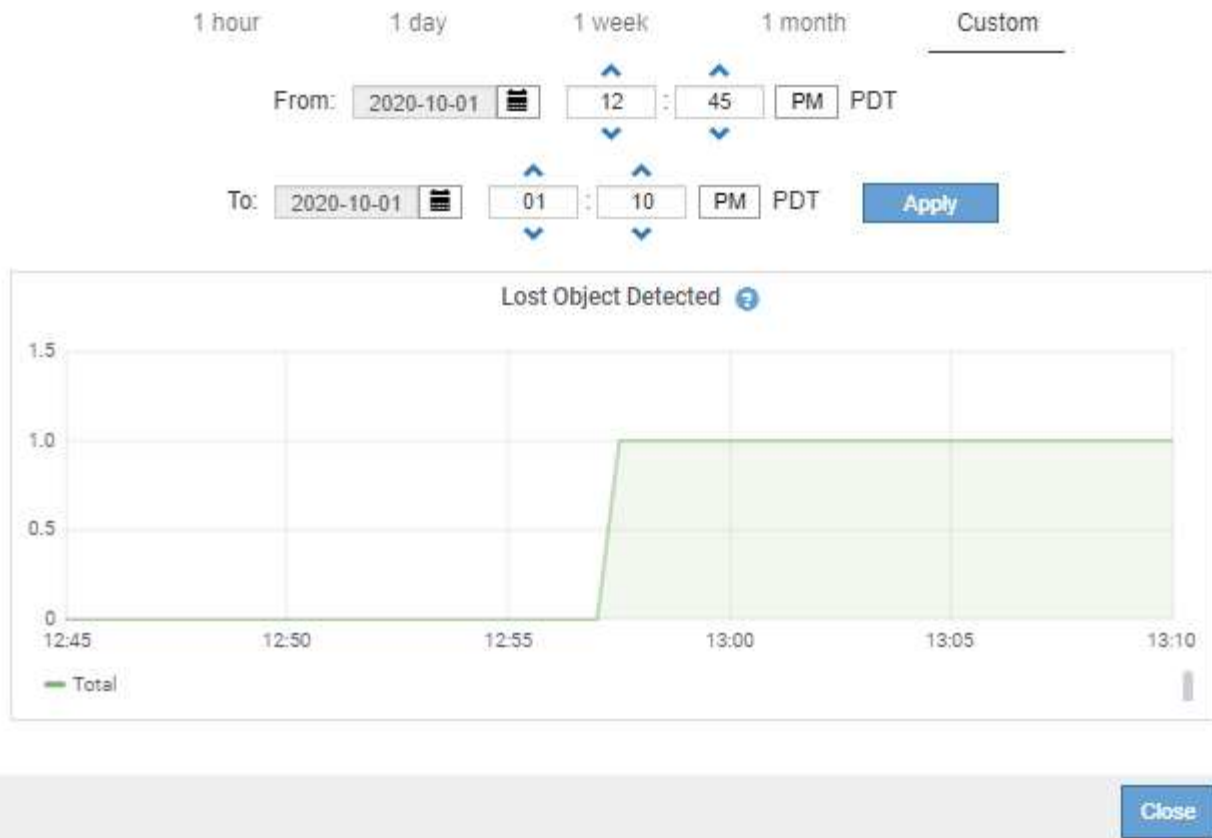
Close



**Exemple 2** : dans l'onglet objets d'un noeud de stockage, vous pouvez sélectionner l'icône du graphique  pour afficher le graphique Grafana du nombre d'objets perdus détectés au fil du temps.



Object Counts	
Total Objects	1
Lost Objects	1
S3 Buckets and Swift Containers	1





5. Pour afficher les graphiques des attributs qui ne sont pas affichés sur la page nœud, sélectionnez **SUPPORT > Outils > topologie de grille.**
6. Sélectionnez **grid node > component ou service > Présentation > main.**

### Computational Resources

Service Restarts:	1	
Service Runtime:	6 days	
Service Uptime:	6 days	
Service CPU Seconds:	10666 s	
Service Load:	0.266 %	

### Memory

Installed Memory:	8.38 GB	
Available Memory:	2.9 GB	

### Processors

Processor Number	Vendor	Type	Cache
1	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
2	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
3	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
4	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
5	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
6	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
7	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
8	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB

7. Sélectionnez l'icône de graphique  en regard de l'attribut.

L'affichage passe automatiquement à la page **Rapports > graphiques**. Le graphique affiche les données de l'attribut au cours du dernier jour.

### Générer des graphiques

Les graphiques affichent une représentation graphique des valeurs de données d'attribut. Vous pouvez générer des rapports sur un site de data Center, un nœud grid, un composant ou un service.

### Avant de commencer

- Vous devez être connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".
- Vous avez "autorisations d'accès spécifiques".

### Étapes

1. Sélectionnez **SUPPORT > Outils > topologie de grille**.
2. Sélectionnez **grid node > component ou service > Rapports > diagrammes**.
3. Sélectionnez l'attribut à rapporter dans la liste déroulante **attribut**.
4. Pour forcer l'axe y à commencer à zéro, décochez la case **mise à l'échelle verticale**.
5. Pour afficher les valeurs avec une précision maximale, cochez la case **données brutes** ou pour arrondir

les valeurs à un maximum de trois décimales (par exemple, pour les attributs signalés en pourcentage), décochez la case **données brutes**.

6. Sélectionnez la période à laquelle effectuer le rapport dans la liste déroulante **requête rapide**.

Sélectionnez l'option requête personnalisée pour sélectionner une plage de temps spécifique.

Le graphique apparaît après quelques instants. Prévoir plusieurs minutes pour la totalisation de longues plages de temps.

7. Si vous avez sélectionné requête personnalisée, personnalisez la période de temps du graphique en saisissant **Date de début** et **Date de fin**.

Utilisez le format *YYYY/MM/DDHH:MM:SS* en heure locale. Des zéros non significatifs sont nécessaires pour correspondre au format. Par exemple, la validation a échoué dans 2017/4/6 7:30:00. Le format correct est: 2017/04/06 07:30:00.

8. Sélectionnez **mettre à jour**.

Un graphique est généré après quelques secondes. Prévoir plusieurs minutes pour la totalisation de longues plages de temps. En fonction de la durée définie pour la requête, un rapport texte brut ou texte agrégé s'affiche.

## Utilisez les rapports texte

Les rapports texte affichent une représentation textuelle des valeurs de données d'attribut traitées par le service NMS. Il existe deux types de rapports générés selon la période de temps sur laquelle vous vous signalez : des rapports de texte brut pour des périodes inférieures à une semaine et des rapports de texte agrégés pour des périodes supérieures à une semaine.

### Rapports de texte brut

Un rapport en texte brut affiche des détails sur l'attribut sélectionné :

- Heure de réception : date et heure locales auxquelles une valeur d'échantillon des données d'un attribut a été traitée par le service NMS.
- Heure de l'échantillon : date et heure locales auxquelles une valeur d'attribut a été échantillonnée ou modifiée à la source.
- Valeur : valeur d'attribut au moment de l'échantillon.

## Text Results for Services: Load - System Logging

2010-07-18 15:58:39 PDT To 2010-07-19 15:58:39 PDT

Time Received	Sample Time	Value
2010-07-19 15:58:09	2010-07-19 15:58:09	0.016 %
2010-07-19 15:56:06	2010-07-19 15:56:06	0.024 %
2010-07-19 15:54:02	2010-07-19 15:54:02	0.033 %
2010-07-19 15:52:00	2010-07-19 15:52:00	0.016 %
2010-07-19 15:49:57	2010-07-19 15:49:57	0.008 %
2010-07-19 15:47:54	2010-07-19 15:47:54	0.024 %
2010-07-19 15:45:50	2010-07-19 15:45:50	0.016 %
2010-07-19 15:43:47	2010-07-19 15:43:47	0.024 %
2010-07-19 15:41:43	2010-07-19 15:41:43	0.032 %
2010-07-19 15:39:40	2010-07-19 15:39:40	0.024 %
2010-07-19 15:37:37	2010-07-19 15:37:37	0.008 %
2010-07-19 15:35:34	2010-07-19 15:35:34	0.016 %
2010-07-19 15:33:31	2010-07-19 15:33:31	0.024 %
2010-07-19 15:31:27	2010-07-19 15:31:27	0.032 %
2010-07-19 15:29:24	2010-07-19 15:29:24	0.032 %
2010-07-19 15:27:21	2010-07-19 15:27:21	0.049 %
2010-07-19 15:25:18	2010-07-19 15:25:18	0.024 %
2010-07-19 15:21:12	2010-07-19 15:21:12	0.016 %
2010-07-19 15:19:09	2010-07-19 15:19:09	0.008 %
2010-07-19 15:17:07	2010-07-19 15:17:07	0.016 %

### Agréger les rapports de texte

Un rapport texte agrégé affiche des données sur une période plus longue (généralement une semaine) qu'un rapport texte brut. Chaque entrée est le résultat d'un résumé de plusieurs valeurs d'attribut (un ensemble de valeurs d'attribut) par le service NMS dans le temps en une seule entrée avec des valeurs moyennes, maximales et minimales dérivées de l'agrégation.

Chaque entrée affiche les informations suivantes :

- Heure d'agrégation : dernière date et heure locales que le service NMS a agrégées (recueillies) un ensemble de valeurs d'attribut modifiées.
- Valeur moyenne : moyenne de la valeur de l'attribut sur la période de temps agrégée.
- Valeur minimale : valeur minimale sur la période de temps agrégée.
- Valeur maximale : valeur maximale sur la période de temps agrégée.

## Text Results for Attribute Send to Relay Rate

2010-07-11 16:02:46 PDT To 2010-07-19 16:02:46 PDT

Aggregate Time	Average Value	Minimum Value	Maximum Value
2010-07-19 15:59:52	0.271072196 Messages/s	0.266649743 Messages/s	0.274983464 Messages/s
2010-07-19 15:53:52	0.275585378 Messages/s	0.266562352 Messages/s	0.283302736 Messages/s
2010-07-19 15:49:52	0.279315709 Messages/s	0.233318712 Messages/s	0.333313579 Messages/s
2010-07-19 15:43:52	0.28181323 Messages/s	0.241651024 Messages/s	0.374976601 Messages/s
2010-07-19 15:39:52	0.284233141 Messages/s	0.249982001 Messages/s	0.324971987 Messages/s
2010-07-19 15:33:52	0.325752083 Messages/s	0.266641993 Messages/s	0.358306197 Messages/s
2010-07-19 15:29:52	0.278531507 Messages/s	0.274984766 Messages/s	0.283320999 Messages/s
2010-07-19 15:23:52	0.281437642 Messages/s	0.274981961 Messages/s	0.291577735 Messages/s
2010-07-19 15:17:52	0.261563307 Messages/s	0.258318006 Messages/s	0.266655787 Messages/s
2010-07-19 15:13:52	0.265159147 Messages/s	0.258318557 Messages/s	0.26663986 Messages/s

### Générer des rapports texte

Les rapports texte affichent une représentation textuelle des valeurs de données d'attribut traitées par le service NMS. Vous pouvez générer des rapports sur un site de data Center, un nœud grid, un composant ou un service.

### Avant de commencer

- Vous devez être connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).

### Description de la tâche

Pour les données d'attribut qui devraient changer en permanence, ces données d'attribut sont échantillonnées par le service NMS (à la source) à intervalles réguliers. Pour les données d'attribut qui changent rarement (par exemple, les données en fonction d'événements tels que les changements d'état ou d'état), une valeur d'attribut est envoyée au service NMS lorsque la valeur change.

Le type de rapport affiché dépend de la période configurée. Par défaut, les rapports de texte agrégés sont générés pour les périodes de plus d'une semaine.

Le texte gris indique que le service a été désactivé administrativement au cours de l'échantillonnage. Le texte bleu indique que le service était dans un état inconnu.

### Étapes

1. Sélectionnez **SUPPORT > Outils > topologie de grille**.
2. Sélectionnez **grid node > component ou service > Reports > Text**.
3. Sélectionnez l'attribut à rapporter dans la liste déroulante **attribut**.
4. Sélectionnez le nombre de résultats par page dans la liste déroulante **Résultats par page**.
5. Pour arrondir les valeurs à un maximum de trois décimales (par exemple, pour les attributs signalés en pourcentage), décochez la case **données brutes**.
6. Sélectionnez la période à laquelle effectuer le rapport dans la liste déroulante **requête rapide**.

Sélectionnez l'option requête personnalisée pour sélectionner une plage de temps spécifique.



Le rapport apparaît après quelques instants. Prévoir plusieurs minutes pour la totalisation de longues plages de temps.

- Si vous avez sélectionné requête personnalisée, vous devez personnaliser la période de rapport en entrant **Date de début** et **Date de fin**.

Utilisez le format `YYYY/MM/DDHH:MM:SS` en heure locale. Des zéros non significatifs sont nécessaires pour correspondre au format. Par exemple, la validation a échoué dans `2017/4/6 7:30:00`. Le format correct est: `2017/04/06 07:30:00`.

- Cliquez sur **mettre à jour**.

Un rapport texte est généré au bout de quelques instants. Prévoir plusieurs minutes pour la totalisation de longues plages de temps. En fonction de la durée définie pour la requête, un rapport texte brut ou texte agrégé s'affiche.


### Exporter les rapports texte

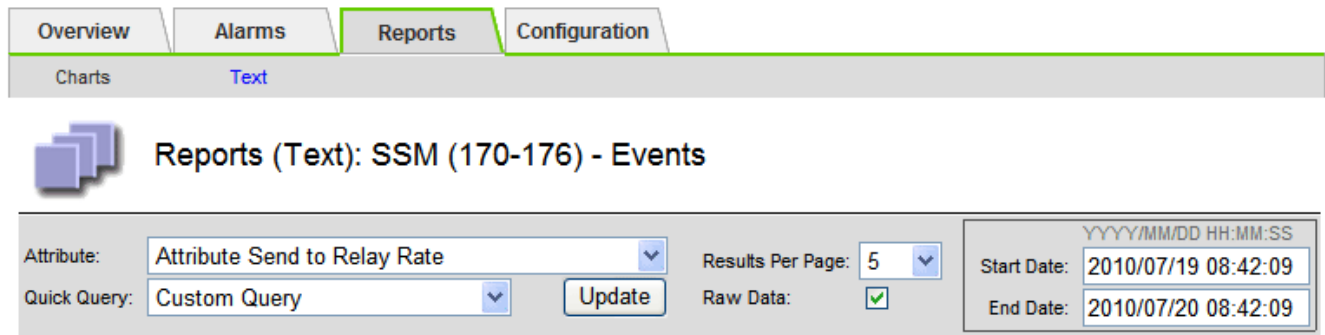
Les rapports texte exportés ouvrent un nouvel onglet de navigateur, qui vous permet de sélectionner et de copier les données.

### Description de la tâche

Les données copiées peuvent ensuite être enregistrées dans un nouveau document (par exemple, une feuille de calcul) et utilisées pour analyser les performances du système StorageGRID.


### Étapes

- Sélectionnez **SUPPORT > Outils > topologie de grille**.
- Créer un rapport texte.
- Cliquez sur **\*Exporter\*** .



#### Text Results for Attribute Send to Relay Rate

2010-07-19 08:42:09 PDT To 2010-07-20 08:42:09 PDT

1 - 5 of 254 

Time Received	Sample Time	Value
2010-07-20 08:40:46	2010-07-20 08:40:46	0.274981485 Messages/s
2010-07-20 08:38:46	2010-07-20 08:38:46	0.274989 Messages/s
2010-07-20 08:36:46	2010-07-20 08:36:46	0.283317543 Messages/s
2010-07-20 08:34:46	2010-07-20 08:34:46	0.274982493 Messages/s
2010-07-20 08:32:46	2010-07-20 08:32:46	0.291646426 Messages/s

Previous « 1 2 3 4 5 » Next

La fenêtre Exporter un rapport texte s'ouvre et affiche le rapport.

Grid ID: 000 000

OID: 2.16.124.113590.2.1.400019.1.1.1.1.16996732.200

Node Path: Site/170-176/SSM/Events

Attribute: Attribute Send to Relay Rate (ABSR)

Query Start Date: 2010-07-19 08:42:09 PDT

Query End Date: 2010-07-20 08:42:09 PDT

Time Received,Time Received (Epoch),Sample Time,Sample Time (Epoch),Value,Type

2010-07-20 08:40:46,1279640446559000,2010-07-20 08:40:46,1279640446537209,0.274981485 Messages/s,U

2010-07-20 08:38:46,1279640326561000,2010-07-20 08:38:46,1279640326529124,0.274989 Messages/s,U

2010-07-20 08:36:46,1279640206556000,2010-07-20 08:36:46,1279640206524330,0.283317543 Messages/s,U

2010-07-20 08:34:46,1279640086540000,2010-07-20 08:34:46,1279640086517645,0.274982493 Messages/s,U

2010-07-20 08:32:46,1279639966543000,2010-07-20 08:32:46,1279639966510022,0.291646426 Messages/s,U

2010-07-20 08:30:46,1279639846561000,2010-07-20 08:30:46,1279639846501672,0.308315369 Messages/s,U

2010-07-20 08:28:46,1279639726527000,2010-07-20 08:28:46,1279639726494673,0.291657509 Messages/s,U

2010-07-20 08:26:46,1279639606526000,2010-07-20 08:26:46,1279639606490890,0.266627739 Messages/s,U

2010-07-20 08:24:46,1279639486495000,2010-07-20 08:24:46,1279639486473368,0.258318523 Messages/s,U

2010-07-20 08:22:46,1279639366480000,2010-07-20 08:22:46,1279639366466497,0.274985902 Messages/s,U

2010-07-20 08:20:46,1279639246469000,2010-07-20 08:20:46,1279639246460346,0.283253871 Messages/s,U

2010-07-20 08:18:46,1279639126469000,2010-07-20 08:18:46,1279639126426669,0.274982804 Messages/s,U

2010-07-20 08:16:46,1279639006437000,2010-07-20 08:16:46,1279639006419168,0.283315503 Messages/s,U

4. Sélectionnez et copiez le contenu de la fenêtre Exporter un rapport texte.

Ces données peuvent maintenant être collées dans un document tiers, tel qu'une feuille de calcul.

## Surveillez L'PUT et OBTENEZ des performances

Vous pouvez surveiller les performances de certaines opérations, telles que le stockage et la récupération d'objets, afin de faciliter l'identification des modifications qui pourraient nécessiter une investigation plus poussée.

### Description de la tâche

Pour surveiller les PUT et GET, vous pouvez exécuter les commandes S3 directement depuis un poste de travail ou via l'application open source S3tester. Ces méthodes vous permettent d'évaluer la performance indépendamment des facteurs externes à StorageGRID, tels que les problèmes liés à une application client ou à un réseau externe.

Lorsque vous effectuez des tests de MISE EN PLACE et D'OBTENTION d'opérations, suivez les instructions suivantes :

- Utilisez des tailles d'objet comparables aux objets que vous ingérer dans votre grid.
- Exécutez vos opérations sur des sites locaux et distants.

Les messages du "[journal d'audit](#)" indiquent le temps total nécessaire à l'exécution de certaines opérations. Par exemple, pour déterminer le temps de traitement total d'une demande GET S3, vous pouvez vérifier la valeur de l'attribut TIME dans le message d'audit SGET. Vous pouvez également trouver l'attribut TIME dans les messages d'audit pour les opérations S3 suivantes : DELETE, GET, HEAD, metadata Updated, POST, PUT

Lors de l'analyse des résultats, examinez le temps moyen requis pour répondre à une demande, ainsi que le débit global que vous pouvez atteindre. Répétez régulièrement les mêmes tests et notez les résultats afin d'identifier les tendances qui pourraient nécessiter une enquête.

- Vous pouvez "[Téléchargez S3Tester sur github](#)".

## Surveiller les opérations de vérification d'objets

Le système StorageGRID peut vérifier l'intégrité des données d'objet sur les nœuds de stockage en vérifiant la présence d'objets corrompus et manquants.

### Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur web pris en charge](#)".
- Vous avez le "[Maintenance ou autorisation d'accès racine](#)".

### Description de la tâche

Deux "[processus de vérification](#)" fonctionnent ensemble pour garantir l'intégrité des données :

- **Vérification de l'arrière-plan** s'exécute automatiquement, en vérifiant continuellement l'exactitude des données de l'objet.

La vérification en arrière-plan vérifie automatiquement et en continu tous les nœuds de stockage pour déterminer s'il existe des copies corrompues des données d'objet répliquées et codées par effacement. Si un problème est détecté, le système StorageGRID tente automatiquement de remplacer les données d'objet corrompues à partir des copies stockées ailleurs dans le système. La vérification en arrière-plan ne s'exécute pas sur les objets d'un pool de stockage cloud.



L'alerte **objet corrompu non identifié détecté** est déclenchée si le système détecte un objet corrompu qui ne peut pas être corrigé automatiquement.

- **La vérification de l'existence d'objet** peut être déclenchée par un utilisateur pour vérifier plus rapidement l'existence (mais pas l'exactitude) des données d'objet.

Le contrôle d'existence d'objet vérifie si toutes les copies répliquées attendues d'objets et de fragments avec code d'effacement existent sur un nœud de stockage. La vérification de l'existence d'un objet permet de vérifier l'intégrité des périphériques de stockage, en particulier si un problème matériel récent peut avoir une incidence sur l'intégrité des données.

Vous devez consulter régulièrement les résultats des vérifications de fond et des contrôles d'existence d'objet. Recherchez immédiatement toute instance de données d'objet corrompues ou manquantes afin de déterminer la cause première.

### Étapes

1. Examiner les résultats des vérifications de base :
  - a. Sélectionnez **NODES > Storage Node > Objects**.
  - b. Vérifier les résultats de la vérification :
    - Pour vérifier la vérification des données d'objet répliqué, consultez les attributs de la section Vérification.

### Verification

Status: ?	No errors	
Percent complete: ?	0.00%	
Average stat time: ?	0.00 microseconds	
Objects verified: ?	0	
Object verification rate: ?	0.00 objects / second	
Data verified: ?	0 bytes	
Data verification rate: ?	0.00 bytes / second	
Missing objects: ?	0	
Corrupt objects: ?	0	
Corrupt objects unidentified: ?	0	
Quarantined objects: ?	0	

- Pour vérifier la vérification du fragment avec code d'effacement, sélectionnez **Storage Node > ILM** et examinez les attributs de la section Vérification du code d'effacement.

### Erasure coding verification

Status: ?	Idle	
Next scheduled: ?	2021-10-08 10:45:19 MDT	
Fragments verified: ?	0	
Data verified: ?	0 bytes	
Corrupt copies: ?	0	
Corrupt fragments: ?	0	
Missing fragments: ?	0	

Sélectionnez le point d'interrogation ? en regard du nom d'un attribut pour afficher le texte d'aide.

2. Examinez les résultats des travaux de vérification de l'existence d'un objet :
  - a. Sélectionnez **MAINTENANCE > Vérification de l'existence d'objet > Historique du travail**.
  - b. Scannez la colonne copies d'objet manquantes détectées. Si des travaux ont entraîné 100 copies d'objets manquantes ou plus et que l'alerte **objets perdus** a été déclenchée, contactez le support technique.

# Object existence check

Perform an object existence check if you suspect storage volumes have been damaged or are corrupt. You can verify that objects defined by your ILM policy, still exist on the volumes.

Active job		Job history		
Delete	Search...			
<input type="checkbox"/>	Job ID ?	Status	Nodes (volumes) ?	Missing object copies detected ?
<input type="checkbox"/>	15816859223101303015	Completed	DC2-S1 (3 volumes)	0
<input type="checkbox"/>	12538643155010477372	Completed	DC1-S3 (1 volume)	0
<input type="checkbox"/>	5490044849774982476	Completed	DC1-S2 (1 volume)	0
<input type="checkbox"/>	3395284277055907678	Completed	DC1-S1 (3 volumes) DC1-S2 (3 volumes) DC1-S3 (3 volumes) and <a href="#">7 more</a>	0

## Contrôle des événements

Vous pouvez surveiller les événements détectés par un nœud de grille, y compris les événements personnalisés que vous avez créés pour suivre les événements qui sont consignés sur le serveur syslog. Le message dernier événement affiché dans Grid Manager fournit plus d'informations sur l'événement le plus récent.

Les messages d'événement sont également répertoriés dans `/var/local/log/bycast-err.log` le fichier journal. Voir la "[Référence des fichiers journaux](#)".

L'alarme SMTT (Total Events) peut être déclenchée à plusieurs reprises par des problèmes tels que des problèmes de réseau, des pannes de courant ou des mises à niveau. Cette section contient des informations sur l'investigation des événements afin que vous puissiez mieux comprendre pourquoi ces alarmes se sont produites. Si un événement s'est produit à cause d'un problème connu, il est possible de réinitialiser les compteurs d'événements.

## Étapes

1. Examinez les événements du système pour chaque nœud du grid :
  - a. Sélectionnez **SUPPORT > Outils > topologie de grille**.
  - b. Sélectionnez **site > grid node > SSM > Events > Overview > main**.
2. Générer une liste de messages d'événement précédents pour vous aider à isoler les problèmes qui se

sont produits auparavant :

- a. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
- b. Sélectionnez **site** > **grid node** > **SSM** > **Events** > **Reports**.
- c. Sélectionnez **texte**.

L'attribut **Last Event** n'apparaît pas dans le "affichage des graphiques". Pour l'afficher :

- d. Remplacez **attribut** par **dernier événement**.
- e. Vous pouvez également sélectionner une période pour **requête rapide**.
- f. Sélectionnez **mettre à jour**.

Overview Alarms Reports Configuration

Charts Text

Reports (Text): SSM (170-41) - Events

Attribute: Last Event Results Per Page: 20 Start Date: 2009/04/15 15:19:53

Quick Query: Last 5 Minutes Update Raw Data:  End Date: 2009/04/15 15:24:53

**Text Results for Last Event**  
2009-04-15 15:19:53 PDT To 2009-04-15 15:24:53 PDT

1 - 2 of 2

Time Received	Sample Time	Value
2009-04-15 15:24:22	2009-04-15 15:24:22	hdc: task_no_data_intr: status=0x51 { DriveReady SeekComplete Error }
2009-04-15 15:24:11	2009-04-15 15:23:39	hdc: task_no_data_intr: status=0x51 { DriveReady SeekComplete Error }

## Créer des événements syslog personnalisés

Les événements personnalisés vous permettent de suivre tous les événements utilisateur du noyau, du démon, de l'erreur et du niveau critique consignés sur le serveur syslog. Un événement personnalisé peut être utile pour surveiller l'occurrence des messages du journal système (et donc les événements de sécurité réseau et les défaillances matérielles).



### Description de la tâche

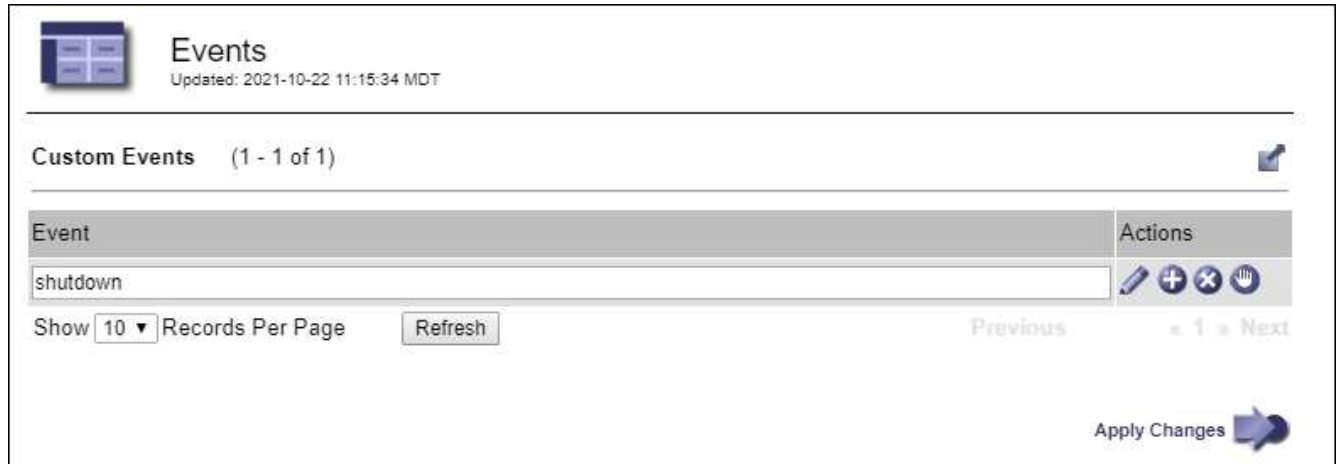
Pensez à créer des événements personnalisés pour surveiller les problèmes récurrents. Les considérations suivantes s'appliquent aux événements personnalisés.

- Après la création d'un événement personnalisé, chaque occurrence de celui-ci est surveillée.
- Pour créer un événement personnalisé basé sur des mots clés dans les `/var/local/log/messages` fichiers, les journaux de ces fichiers doivent être :
  - Généré par le noyau
  - Généré par un démon ou un programme utilisateur au niveau d'erreur ou critique

**Note:** toutes les entrées dans les fichiers ne seront pas `/var/local/log/messages` appariées à moins qu'elles ne répondent aux exigences énoncées ci-dessus.





### Étapes

1. Sélectionnez **SUPPORT** > **alarmes (hérité)** > **événements personnalisés**.
2. Cliquez sur **Modifier**  (ou sur **Insérer**  s'il ne s'agit pas du premier événement).
3. Entrez une chaîne d'événement personnalisée, par exemple, l'arrêt




Events  
Updated: 2021-10-22 11:15:34 MDT

Custom Events (1 - 1 of 1)

Event	Actions
shutdown	   

Show 10 Records Per Page Refresh Previous 1 Next

Apply Changes 

4. Sélectionnez **appliquer les modifications**.
5. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
6. Sélectionnez **GRID node** > **SSM** > **Events**.
7. Localisez l'entrée événements personnalisés dans le tableau Evénements et surveillez la valeur de **Count**.

Si le nombre augmente, un événement personnalisé que vous surveillez est déclenché sur ce nœud de la grille.

Overview
Alarms
Reports
Configuration

Main

## Overview: SSM (DC1-ADM1) - Events

Updated: 2021-10-22 11:19:18 MDT

### System Events

Log Monitor State:
Connected
🟢

Total Events:
0
🟢

Last Event:
No Events

Description	Count	
Abnormal Software Events	0	🔍
Account Service Events	0	🔍
Cassandra Errors	0	🔍
Cassandra Heap Out Of Memory Errors	0	🔍
Chunk Service Events	0	🔍
Custom Events	0	🔍
Data-Mover Service Events	0	🔍
File System Errors	0	🔍
Forced Termination Events	0	🔍
Grid Node Errors	0	🔍
Hotfix Installation Failure Events	0	🔍
I/O Errors	0	🔍
IDE Errors	0	🔍
Identity Service Events	0	🔍
Kernel Errors	0	🔍
Kernel Memory Allocation Failure	0	🔍
Keystone Service Events	0	🔍
Network Receive Errors	0	🔍
Network Transmit Errors	0	🔍
Out Of Memory Errors	0	🔍
Replicated State Machine Service Events	0	🔍
SCSI Errors	0	🔍

### Réinitialisez le nombre d'événements personnalisés


Si vous souhaitez réinitialiser le compteur uniquement pour les événements personnalisés, vous devez utiliser la page topologie de la grille dans le menu support.

La réinitialisation d'un compteur entraîne le déclenchement de l'alarme par l'événement suivant. En revanche, lorsque vous reconnaissez une alarme, celle-ci n'est déclenchée que si le niveau de seuil suivant est atteint.

### Étapes

1. Sélectionnez **SUPPORT > Outils > topologie de grille**.
2. Sélectionnez **GRID node > SSM > Events > Configuration > main**.
3. Cochez la case **Réinitialiser** pour les événements personnalisés.



Overview			Alarms			Reports			Configuration		
Main			Alarms								
 <b>Configuration: SSM (DC2-ADM1) - Events</b> Updated: 2018-04-11 10:35:44 MDT											
Description	Count	Reset									
Abnormal Software Events	0	<input type="checkbox"/>									
Account Service Events	0	<input type="checkbox"/>									
Cassandra Errors	0	<input type="checkbox"/>									
Cassandra Heap Out Of Memory Errors	0	<input type="checkbox"/>									
Custom Events	0	<input checked="" type="checkbox"/>									
File System Errors	0	<input type="checkbox"/>									
Forced Termination Events	0	<input type="checkbox"/>									

4. Sélectionnez **appliquer les modifications**.

### Examiner les messages d'audit

Les messages d'audit vous permettent de mieux comprendre le fonctionnement détaillé de votre système StorageGRID. Vous pouvez utiliser les journaux d'audit pour résoudre les problèmes et évaluer les performances.

Pendant le fonctionnement normal du système, tous les services StorageGRID génèrent des messages d'audit comme suit :

- Les messages d'audit système sont liés au système d'audit lui-même, à l'état du nœud de la grille, à l'activité des tâches à l'échelle du système et aux opérations de sauvegarde du service.
- Les messages d'audit du stockage objet sont liés au stockage et à la gestion des objets dans StorageGRID, notamment le stockage objet et les récupérations, les transferts entre nœuds de grille et nœuds de grille, et les vérifications.
- Les messages d'audit de lecture et d'écriture du client sont consignés lorsqu'une application client S3 demande de création, de modification ou de récupération d'un objet.
- Les messages d'audit de gestion consigne les demandes des utilisateurs vers l'API de gestion.

Chaque nœud d'administration stocke les messages d'audit dans des fichiers texte. Le partage d'audit contient le fichier actif (audit.log) ainsi que les journaux d'audit compressés des jours précédents. Chaque nœud de la grille stocke également une copie des informations d'audit générées sur le nœud.

Vous pouvez accéder aux fichiers journaux d'audit directement à partir de la ligne de commande du nœud d'administration.

StorageGRID peut envoyer les informations d'audit par défaut ou modifier la destination :

- StorageGRID sélectionne par défaut les destinations d'audit de nœud local.
- Les entrées du journal d'audit Grid Manager et tenant Manager peuvent être envoyées à un nœud de

stockage.

- Vous pouvez également modifier la destination des journaux d'audit et envoyer des informations d'audit à un serveur syslog externe. Les journaux locaux des enregistrements d'audit continuent à être générés et stockés lorsqu'un serveur syslog externe est configuré.
- ["Découvrez comment configurer les messages d'audit et les destinations des journaux"](#).

Pour plus de détails sur le fichier journal d'audit, le format des messages d'audit, les types de messages d'audit et les outils disponibles pour analyser les messages d'audit, reportez-vous à la section ["Examiner les journaux d'audit"](#).

## Collecte de fichiers journaux et de données système

Vous pouvez utiliser le Gestionnaire de grille pour récupérer les fichiers journaux et les données système (y compris les données de configuration) de votre système StorageGRID.

### Avant de commencer

- Vous devez être connecté au gestionnaire de grille sur le nœud d'administration principal à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).
- Vous devez disposer de la phrase secrète pour le provisionnement.

### Description de la tâche

Vous pouvez utiliser le gestionnaire de grille pour collecter ["fichiers journaux"](#), les données système et les données de configuration de n'importe quel nœud de grille pour la période que vous sélectionnez. Les données sont collectées et archivées dans un fichier .tar.gz que vous pouvez ensuite télécharger sur votre ordinateur local.

Vous pouvez également modifier la destination des journaux d'audit et envoyer des informations d'audit à un serveur syslog externe. Les journaux locaux des enregistrements d'audit continuent à être générés et stockés lorsqu'un serveur syslog externe est configuré. Voir ["Configurez les messages d'audit et les destinations des journaux"](#).

### Étapes

1. Sélectionnez **SUPPORT > Outils > journaux**.

2. Sélectionnez les nœuds de grille pour lesquels vous souhaitez collecter les fichiers journaux.

Si nécessaire, vous pouvez collecter des fichiers journaux pour l'intégralité de la grille ou un site de data Center.

3. Sélectionnez une **heure de début** et **heure de fin** pour définir la plage horaire des données à inclure dans les fichiers journaux.

Si vous sélectionnez une période très longue ou que vous collectez des journaux de tous les nœuds d'un grand grid, l'archivage des journaux risque de devenir trop volumineux pour être stocké sur un nœud, ou trop volumineux pour être collecté sur le nœud d'administration principal pour le téléchargement. Dans ce cas, vous devez redémarrer la collecte de journaux avec un jeu de données plus petit.

4. Sélectionnez les types de journaux que vous souhaitez collecter.

- **Journaux d'applications** : journaux spécifiques à l'application que le support technique utilise le plus fréquemment pour le dépannage. Les journaux collectés sont un sous-ensemble des journaux d'application disponibles.
- **Journaux d'audit** : journaux contenant les messages d'audit générés pendant le fonctionnement normal du système.
- **Trace réseau** : journaux utilisés pour le débogage réseau.
- **Base de données Prometheus** : indicateurs de séries chronologiques des services sur tous les nœuds.

5. Vous pouvez également saisir des notes concernant les fichiers journaux que vous recueillez dans la zone de texte **Notes**.

Vous pouvez utiliser ces notes pour fournir des informations de support technique sur le problème qui vous a demandé de collecter les fichiers journaux. Vos notes sont ajoutées à un fichier appelé `info.txt`, ainsi qu'à d'autres informations sur la collection de fichiers journaux. Le `info.txt` fichier est enregistré dans le package d'archivage du fichier journal.

6. Saisissez le mot de passe de provisionnement de votre système StorageGRID dans la zone de texte **phrase de passe de provisionnement**.

7. Sélectionnez **collecter les journaux**.

Lorsque vous soumettez une nouvelle demande, la collection précédente de fichiers journaux est supprimée.

Vous pouvez utiliser la page journaux pour surveiller la progression de la collecte des fichiers journaux pour chaque nœud de la grille.

Si vous recevez un message d'erreur sur la taille du journal, essayez de collecter les journaux pour une période plus courte ou pour moins de nœuds.

8. Sélectionnez **Download** lorsque la collecte des fichiers journaux est terminée.

Le fichier `.tar.gz` contient tous les fichiers journaux de tous les nœuds de la grille où la collecte des journaux a réussi. Dans le fichier combiné `.tar.gz`, il y a une archive de fichier journal pour chaque nœud de la grille.

### Une fois que vous avez terminé

Vous pouvez télécharger à nouveau le package d'archivage des fichiers journaux ultérieurement si nécessaire.

Vous pouvez également sélectionner **Supprimer** pour supprimer le paquet d'archive de fichier journal et libérer de l'espace disque. Le progiciel d'archivage du fichier journal actuel est automatiquement supprimé lors de la prochaine collecte de fichiers journaux.

### Déclencher manuellement un package AutoSupport

Pour aider le support technique à résoudre les problèmes liés à votre système StorageGRID, vous pouvez déclencher manuellement l'envoi d'un pack AutoSupport.

#### Avant de commencer

- Vous devez être connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous devez disposer de l'accès racine ou d'une autre autorisation de configuration de grille.

#### Étapes

1. Sélectionnez **SUPPORT > Outils > AutoSupport**.
2. Dans l'onglet **actions**, sélectionnez **Envoyer AutoSupport déclenché par l'utilisateur**.

StorageGRID tente d'envoyer un pack AutoSupport sur le site de support NetApp. Si la tentative réussit, les valeurs **résultat le plus récent** et **dernier temps** réussi dans l'onglet **Résultats** sont mises à jour. En cas de problème, la valeur **résultat le plus récent** est mise à jour sur « échec » et StorageGRID n'essaie pas d'envoyer à nouveau le paquet AutoSupport.

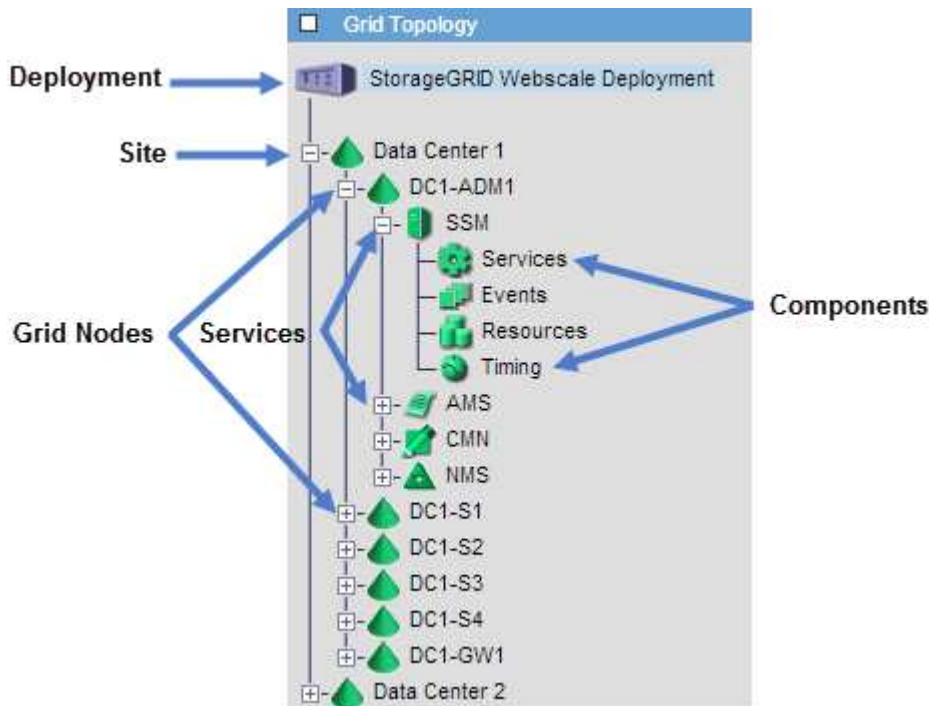


Après avoir envoyé un pack AutoSupport déclenché par l'utilisateur, actualisez la page AutoSupport de votre navigateur au bout d'une minute pour accéder aux résultats les plus récents.

## Afficher l'arborescence de la grille topologique

L'arborescence de la grille topologie permet d'accéder à des informations détaillées sur les éléments du système StorageGRID, notamment les sites, les nœuds de la grille, les services et les composants. Dans la plupart des cas, il vous suffit d'accéder à l'arborescence de la grille topologique lorsque vous y êtes invité ou lorsque vous collaborez avec le support technique.

Pour accéder à l'arborescence de la topologie de grille, sélectionnez **SUPPORT > Outils > topologie de grille**.



Pour développer ou réduire l'arborescence topologie de la grille, cliquez sur **+** ou **-** au niveau du site, du nœud ou du service. Pour développer ou réduire tous les éléments du site entier ou de chaque nœud, maintenez la touche **<Ctrl>** enfoncée et cliquez sur.

## Attributs des StorageGRID

Attributs valeurs et États du rapport pour la plupart des fonctions du système StorageGRID. Des valeurs d'attribut sont disponibles pour chaque nœud de grille, chaque site et la grille entière.

Les attributs StorageGRID sont utilisés à plusieurs endroits dans le Gestionnaire de grille :

- **Page nœuds** : la plupart des valeurs affichées sur la page noeuds sont des attributs StorageGRID. (Les metrics de Prometheus sont également affichés sur les pages nœuds.)
- **Grid Topology Tree** : les valeurs d'attribut sont affichées dans l'arborescence de la topologie de la grille (**SUPPORT > Outils > topologie de la grille**).
- **Événements** : les événements système se produisent lorsque certains attributs enregistrent une condition d'erreur ou de panne pour un nœud, y compris des erreurs telles que des erreurs réseau.

## Valeurs d'attribut

Les attributs sont rapportés sur la base du meilleur effort et sont approximativement corrects. Les mises à jour d'attributs peuvent être perdues dans certains cas, comme la panne d'un service ou la panne et la reconstruction d'un nœud de la grille.

En outre, les retards de propagation peuvent ralentir le reporting des attributs. Les valeurs mises à jour pour la plupart des attributs sont envoyées au système StorageGRID à intervalles fixes. Plusieurs minutes peuvent être nécessaires avant qu'une mise à jour soit visible dans le système et deux attributs qui changent plus ou moins simultanément peuvent être signalés à des moments légèrement différents.

## Examinez les metrics de support

Lorsque vous dépannez un problème, vous pouvez consulter les graphiques et les metrics détaillés de votre système StorageGRID en collaboration avec le support technique.

### Avant de commencer

- Vous devez être connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).

### Description de la tâche

La page Metrics vous permet d'accéder aux interfaces utilisateur de Prometheus et Grafana. Prometheus est un logiciel open source qui permet de collecter des metrics. Grafana est un logiciel open source permettant de visualiser les metrics.



Les outils disponibles sur la page métriques sont destinés au support technique. Certaines fonctions et options de menu de ces outils sont intentionnellement non fonctionnelles et peuvent faire l'objet de modifications. Voir la liste de ["Metrics Prometheus couramment utilisés"](#).

### Étapes

1. Comme indiqué par le support technique, sélectionnez **SUPPORT > Outils > métriques**.

Voici un exemple de la page métriques :

# Metrics

Access charts and metrics to help troubleshoot issues.

 The tools available on this page are intended for use by technical support. Some features and menu items within these tools are intentionally non-functional.

## Prometheus

Prometheus is an open-source toolkit for collecting metrics. The Prometheus interface allows you to query the current values of metrics and to view charts of the values over time.

Access the Prometheus UI using the link below. You must be signed in to the Grid Manager.

- [https://\[redacted\]](https://[redacted])

## Grafana

Grafana is open-source software for metrics visualization. The Grafana interface provides pre-constructed dashboards that contain graphs of important metric values over time.

Access the Grafana dashboards using the links below. You must be signed in to the Grid Manager.

<a href="#">ADE</a>	<a href="#">EC Overview</a>	<a href="#">Replicated Read Path Overview</a>
<a href="#">Account Service Overview</a>	<a href="#">Grid</a>	<a href="#">S3 - Node</a>
<a href="#">Alertmanager</a>	<a href="#">ILM</a>	<a href="#">S3 Overview</a>
<a href="#">Audit Overview</a>	<a href="#">Identity Service Overview</a>	<a href="#">S3 Select</a>
<a href="#">Cassandra Cluster Overview</a>	<a href="#">Ingests</a>	<a href="#">Site</a>
<a href="#">Cassandra Network Overview</a>	<a href="#">Node</a>	<a href="#">Support</a>
<a href="#">Cassandra Node Overview</a>	<a href="#">Node (Internal Use)</a>	<a href="#">Traces</a>
<a href="#">Cross Grid Replication</a>	<a href="#">OSL - AsyncIO</a>	<a href="#">Traffic Classification Policy</a>
<a href="#">Cloud Storage Pool Overview</a>	<a href="#">Platform Services Commits</a>	<a href="#">Usage Processing</a>
<a href="#">EC - ADE</a>	<a href="#">Platform Services Overview</a>	<a href="#">Virtual Memory (vmstat)</a>
<a href="#">EC - Chunk Service</a>	<a href="#">Platform Services Processing</a>	

2. Pour interroger les valeurs actuelles des metrics StorageGRID et afficher les graphiques des valeurs dans le temps, cliquez sur le lien de la section Prometheus.

L'interface Prometheus s'affiche. Vous pouvez utiliser cette interface pour exécuter des requêtes sur les mesures StorageGRID disponibles et pour générer des graphiques sur les mesures StorageGRID au fil du temps.



Les indicateurs qui incluent *private* dans leurs noms sont destinés à un usage interne uniquement et peuvent être modifiés sans préavis entre les versions de StorageGRID.

3. Pour accéder aux tableaux de bord pré-construits contenant des graphiques des mesures StorageGRID au fil du temps, cliquez sur les liens de la section Grafana.

L'interface Grafana pour le lien que vous avez sélectionné s'affiche.



## Exécuter les diagnostics

Lors du dépannage d'un problème, vous pouvez vous aider avec le support technique à exécuter des diagnostics sur votre système StorageGRID et examiner les résultats.

- ["Examinez les metrics de support"](#)
- ["Metrics Prometheus couramment utilisés"](#)

### Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).

### Description de la tâche

La page Diagnostics effectue un ensemble de contrôles de diagnostic sur l'état actuel de la grille. Chaque vérification de diagnostic peut avoir l'un des trois États suivants :

-



- ✓ **Normal** : toutes les valeurs sont comprises dans la plage normale.
- ⚠ **Attention** : une ou plusieurs valeurs sont en dehors de la plage normale.
- ✖ **Attention** : une ou plusieurs des valeurs sont nettement en dehors de la plage normale.

Les États de diagnostic sont indépendants des alertes en cours et peuvent ne pas indiquer de problèmes opérationnels dans la grille. Par exemple, une vérification de diagnostic peut afficher l'état de mise en garde même si aucune alerte n'a été déclenchée.

## Étapes

1. Sélectionnez **SUPPORT > Outils > Diagnostics**.

La page Diagnostics s'affiche et répertorie les résultats de chaque vérification de diagnostic. Les résultats sont triés par gravité (attention, attention, puis normale). Dans chaque gravité, les résultats sont triés par ordre alphabétique.

Dans cet exemple, tous les diagnostics ont un état Normal.

2. Pour en savoir plus sur un diagnostic spécifique, cliquez n'importe où dans la ligne.

Des détails sur le diagnostic et ses résultats actuels s'affichent. Les informations suivantes sont répertoriées :

- **Etat** : état actuel de ce diagnostic : normal, attention ou attention.
- **Requête Prometheus** : si utilisé pour le diagnostic, l'expression Prometheus qui a été utilisée pour

générer les valeurs d'état. (Une expression Prometheus n'est pas utilisée pour tous les diagnostics.)

- **Seuils** : si disponibles pour le diagnostic, les seuils définis par le système pour chaque état de diagnostic anormal. (Les valeurs de seuil ne sont pas utilisées pour tous les diagnostics.)



Vous ne pouvez pas modifier ces seuils.

- **Valeurs d'état** : tableau indiquant l'état et la valeur du diagnostic dans l'ensemble du système StorageGRID. Dans cet exemple, l'utilisation actuelle du processeur pour chaque nœud d'un système StorageGRID est indiquée. Toutes les valeurs de nœud sont inférieures aux seuils attention et mise en garde, de sorte que l'état général du diagnostic est Normal.

✓ **CPU utilization**

Checks the current CPU utilization on each node.

To view charts of CPU utilization and other per-node metrics, access the [Node Grafana dashboard](#).

**Status** ✓ Normal

**Prometheus query** `sum by (instance) (sum by (instance, mode) (irate(node_cpu_seconds_total{mode!="idle"}[5m])) / count by (instance, mode)(node_cpu_seconds_total{mode!="idle"}))`  
[View in Prometheus](#)

**Thresholds**  
⚠ Attention >= 75%  
⛔ Caution >= 95%

Status	Instance	CPU Utilization
✓	DC1-ADM1	2.598%
✓	DC1-ARC1	0.937%
✓	DC1-G1	2.119%
✓	DC1-S1	8.708%
✓	DC1-S2	8.142%
✓	DC1-S3	9.669%
✓	DC2-ADM1	2.515%
✓	DC2-ARC1	1.152%
✓	DC2-S1	8.204%
✓	DC2-S2	5.000%
✓	DC2-S3	10.469%

3. **Facultatif** : pour afficher les graphiques Grafana relatifs à ce diagnostic, cliquez sur le lien **Dashboard**.

Ce lien ne s'affiche pas pour tous les diagnostics.

Le tableau de bord associé à Grafana s'affiche. Dans cet exemple, le tableau de bord des nœuds apparaît et affiche l'utilisation des CPU dans le temps pour ce nœud, ainsi que d'autres graphiques Grafana pour le nœud.



Vous pouvez également accéder aux tableaux de bord pré-construits Grafana à partir de la section **SUPPORT > Tools > Metrics**.



4. **Facultatif** : pour afficher un graphique de l'expression Prometheus au fil du temps, cliquez sur **Afficher dans Prometheus**.

Un graphique Prometheus de l'expression utilisée dans le diagnostic s'affiche.

Enable query history

```
sum by (instance) (sum by (instance, mode) (irate(node_cpu_seconds_total{mode!="idle"}[5m])) / count by (instance, mode))
```

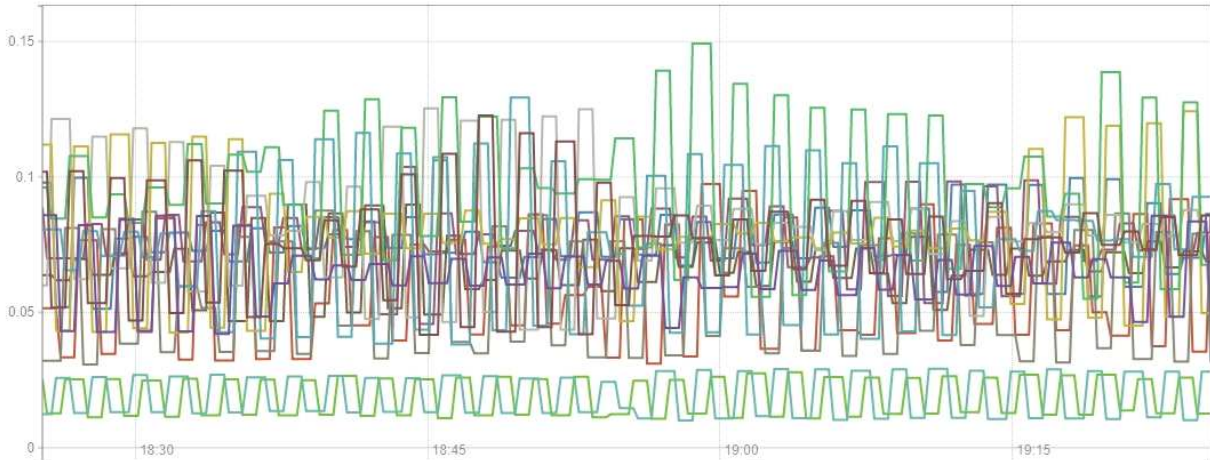
Load time: 547ms  
Resolution: 14s  
Total time series: 13

Execute

- insert metric at cursor -

Graph Console

1h    +    << Until >>    Res. (s)     stacked



- {instance="DC3-S3"}
- {instance="DC3-S2"}
- {instance="DC3-S1"}
- {instance="DC2-S3"}
- {instance="DC2-S2"}
- {instance="DC2-S1"}
- {instance="DC2-ADM1"}
- {instance="DC1-S3"}
- {instance="DC1-S2"}
- {instance="DC1-S1"}
- {instance="DC1-G1"}
- {instance="DC1-ARC1"}
- {instance="DC1-ADM1"}

Remove Graph

Add Graph

## Créer des applications de surveillance personnalisées

Vous pouvez créer des applications et des tableaux de bord de surveillance personnalisés à l'aide des metrics StorageGRID disponibles dans l'API de gestion du grid.

Si vous souhaitez surveiller des mesures qui ne s'affichent pas sur une page existante du Gestionnaire de grille ou si vous souhaitez créer des tableaux de bord personnalisés pour StorageGRID, vous pouvez utiliser l'API de gestion de grille pour interroger les mesures StorageGRID.

Vous pouvez également accéder directement à des metrics Prometheus à l'aide d'un outil de surveillance externe tel que Grafana. Pour utiliser un outil externe, vous devez télécharger ou générer un certificat de client d'administration afin de permettre à StorageGRID d'authentifier l'outil pour la sécurité. Voir la "[Instructions d'administration de StorageGRID](#)".

Pour afficher les opérations de l'API de metrics, y compris la liste complète des metrics disponibles, rendez-vous sur Grid Manager. En haut de la page, sélectionnez l'icône d'aide et sélectionnez **documentation API** >

metrics.

## metrics Operations on metrics



GET	<code>/grid/metric-labels/{label}/values</code>	Lists the values for a metric label	
GET	<code>/grid/metric-names</code>	Lists all available metric names	
GET	<code>/grid/metric-query</code>	Performs an instant metric query at a single point in time	
GET	<code>/grid/metric-query-range</code>	Performs a metric query over a range of time	

Les détails de la mise en œuvre d'une application de surveillance personnalisée dépassent le champ d'application de cette documentation.

# Dépanner le système StorageGRID

## Dépanner un système StorageGRID

Si vous rencontrez un problème avec un système StorageGRID, consultez les conseils et les instructions de cette section pour déterminer et résoudre le problème.

Vous pouvez souvent résoudre vous-même certains problèmes, mais vous devrez peut-être les faire remonter au support technique.

### définir le problème

La première étape pour résoudre un problème est de définir clairement le problème.

Ce tableau fournit des exemples de types d'informations que vous pouvez collecter pour définir un problème :

Question	Exemple de réponse
Que fait ou ne fait pas le système StorageGRID ? Quels sont ses symptômes ?	Les applications client signalent que les objets ne peuvent pas être ingérés dans StorageGRID.
Quand le problème a-t-il démarré ?	L'ingestion d'objet a d'abord été refusée à environ 14:50 le 8 janvier 2020.
Comment avez-vous remarqué le problème pour la première fois ?	Notifié par la demande du client. Vous avez également reçu des notifications par e-mail d'alerte.
Le problème se produit-il de manière cohérente ou seulement parfois ?	Le problème est en cours.
Si le problème se produit régulièrement, quelles sont les étapes à suivre	Un problème se produit à chaque fois qu'un client tente d'ingérer un objet.

Question	Exemple de réponse
Si le problème se produit par intermittence, quand cela se produit-il? Notez l'heure de chaque incident que vous connaissez.	Le problème n'est pas intermittent.
Avez-vous déjà vu ce problème ? À quelle fréquence avez-vous eu ce problème par le passé ?	C'est la première fois que j'ai vu cette question.

### Évaluez les risques et l'impact sur le système

Une fois le problème défini, évaluez les risques et l'impact sur le système StorageGRID. Par exemple, la présence d'alertes critiques ne signifie pas nécessairement que le système ne fournit pas de services de base.

Ce tableau récapitule l'impact du problème exemple sur les opérations du système :

Question	Exemple de réponse
Le système StorageGRID est-il en mesure d'ingérer du contenu ?	Non
Les applications client peuvent-elles récupérer du contenu ?	Certains objets peuvent être récupérés et d'autres ne le peuvent pas.
Les données sont-elles menacées ?	Non
La capacité à mener des activités est-elle gravement affectée ?	Oui, car les applications client ne peuvent pas stocker d'objets sur le système StorageGRID et les données ne peuvent pas être récupérées de manière cohérente.

### Collecte de données

Une fois que vous avez défini le problème et évalué ses risques et son impact, collectez des données pour analyse. Le type de données les plus utiles à recueillir dépend de la nature du problème.

Type de données à collecter	Pourquoi collecter ces données	Instructions
Créer le calendrier des modifications récentes	Toute modification de votre système StorageGRID, de sa configuration ou de son environnement peut provoquer un nouveau comportement.	<ul style="list-style-type: none"> <li>• <a href="#">Créer un calendrier des modifications récentes</a></li> </ul>

Type de données à collecter	Pourquoi collecter ces données	Instructions
Consultez les alertes	<p>Les alertes vous aident à déterminer rapidement la cause première d'un problème en fournissant des indices importants sur les problèmes sous-jacents qui pourraient l'être.</p> <p>Consultez la liste des alertes actuelles pour voir si StorageGRID a identifié la cause première d'un problème pour vous.</p> <p>Examinez les alertes déclenchées par le passé pour obtenir des informations supplémentaires.</p>	<ul style="list-style-type: none"> <li>• "Afficher les alertes actuelles et résolues"</li> </ul>
Contrôle des événements	<p>Les événements incluent les événements d'erreur système ou de panne pour un nœud, y compris les erreurs telles que les erreurs réseau. Surveiller les événements pour en savoir plus sur les problèmes ou obtenir de l'aide pour les résoudre.</p>	<ul style="list-style-type: none"> <li>• "Contrôle des événements"</li> </ul>
Identifier les tendances à l'aide de graphiques et de rapports texte	<p>Les tendances peuvent donner des indications précieuses sur le moment où les problèmes sont apparus et vous aider à comprendre la rapidité à laquelle les choses évoluent.</p>	<ul style="list-style-type: none"> <li>• "Utilisez des graphiques et des rapports texte"</li> <li>• "Utilisez les rapports texte"</li> </ul>
Établir les lignes de base	<p>Collectez des informations sur les niveaux normaux de différentes valeurs opérationnelles. Ces valeurs de référence, ainsi que les écarts par rapport à ces lignes de base, peuvent fournir des indices précieux.</p>	<ul style="list-style-type: none"> <li>• Établir les lignes de base</li> </ul>
Tests d'entrée et de récupération	<p>Pour résoudre les problèmes de performance liés à l'entrée et à la récupération, utilisez un poste de travail pour stocker et récupérer des objets. Comparez les résultats obtenus avec ceux observés lors de l'utilisation de l'application client.</p>	<ul style="list-style-type: none"> <li>• "Surveillez L'PUT et OBTENEZ des performances"</li> </ul>
Examiner les messages d'audit	<p>Examinez les messages d'audit afin de suivre les opérations StorageGRID en détail. Les détails dans les messages d'audit peuvent être utiles pour le dépannage de nombreux types de problèmes, y compris les problèmes de performance.</p>	<ul style="list-style-type: none"> <li>• "Examiner les messages d'audit"</li> </ul>

Type de données à collecter	Pourquoi collecter ces données	Instructions
Vérifier l'emplacement des objets et l'intégrité du stockage	En cas de problèmes de stockage, vérifiez que les objets sont placés à l'endroit où vous vous attendez. Vérifiez l'intégrité des données d'objet sur un nœud de stockage.	<ul style="list-style-type: none"> <li>• "Surveiller les opérations de vérification d'objets"</li> <li>• "Confirmer l'emplacement des données d'objet"</li> <li>• "Vérifiez l'intégrité de l'objet"</li> </ul>
Collecte de données pour le support technique	L'assistance technique peut vous demander de collecter des données ou de passer en revue des informations spécifiques pour résoudre les problèmes.	<ul style="list-style-type: none"> <li>• "Collecte de fichiers journaux et de données système"</li> <li>• "Déclencher manuellement un package AutoSupport"</li> <li>• "Examinez les metrics de support"</li> </ul>

#### Créez un calendrier des modifications récentes

En cas de problème, vous devriez considérer ce qui a changé récemment et quand ces changements se sont produits.

- Toute modification de votre système StorageGRID, de sa configuration ou de son environnement peut provoquer un nouveau comportement.
- Un calendrier des modifications peut vous aider à identifier les changements susceptibles d'être responsables d'un problème, ainsi que la manière dont chaque changement pourrait avoir affecté son développement.

Créez un tableau des dernières modifications apportées à votre système, qui contient des informations sur la date à laquelle chaque modification a eu lieu, ainsi que des informations pertinentes sur la modification, telles que les autres événements survenus pendant que la modification a été en cours :

Heure de la modification	Type de modification	Détails
Par exemple : <ul style="list-style-type: none"> <li>• Quand avez-vous démarré la restauration du nœud ?</li> <li>• Quand la mise à niveau logicielle s'est-elle terminée ?</li> <li>• Avez-vous interrompu le processus ?</li> </ul>	Que s'est-il passé ? Qu'avez-vous fait ?	Documentez toute information pertinente concernant la modification. Par exemple : <ul style="list-style-type: none"> <li>• Détails des modifications du réseau.</li> <li>• Quel correctif a été installé.</li> <li>• Changement des workloads clients.</li> </ul> Assurez-vous de noter si plusieurs changements ont eu lieu en même temps. Par exemple, ce changement a-t-il été effectué pendant qu'une mise à niveau était en cours ?



## Exemples de changements récents importants

Voici quelques exemples de changements potentiellement importants :

- Le système StorageGRID a-t-il été récemment installé, étendu ou récupéré ?
- Le système a-t-il été mis à niveau récemment ? Un correctif a-t-il été appliqué ?
- Du matériel a-t-il été réparé ou modifié récemment ?
- La règle ILM a-t-elle été mise à jour ?
- La charge de travail client a-t-elle changé ?
- L'application client ou son comportement a-t-il changé ?
- Avez-vous modifié des équilibres de charge, ou ajouté ou supprimé un groupe haute disponibilité de nœuds d'administration ou de nœuds de passerelle ?
- Certaines tâches lancées peuvent-elles prendre un certain temps ? Voici quelques exemples :
  - Récupération d'un nœud de stockage défaillant
  - Désaffectation des nœuds de stockage
- Des modifications ont-elles été apportées à l'authentification utilisateur, par exemple l'ajout d'un locataire ou la modification de la configuration LDAP ?
- La migration des données a-t-elle lieu ?
- Les services de plateforme ont-ils été récemment activés ou modifiés ?
- La conformité a-t-elle été activée récemment ?
- Les pools de stockage cloud ont-ils été ajoutés ou supprimés ?
- La compression du stockage ou le chiffrement ont-ils été modifiés ?
- L'infrastructure réseau a-t-elle été modifiée ? Par exemple, VLAN, routeurs ou DNS.
- Des modifications ont-elles été apportées aux sources NTP ?
- Des modifications ont-elles été apportées aux interfaces réseau Grid, Admin ou client ?
- Le système StorageGRID ou son environnement a-t-il subi d'autres modifications ?

### Établir les lignes de base

Vous pouvez établir des lignes de base pour votre système en enregistrant les niveaux normaux de différentes valeurs opérationnelles. À l'avenir, vous pourrez comparer les valeurs actuelles à ces lignes de base afin de détecter et de résoudre les valeurs anormales.

Propriété	Valeur	Comment obtenir
Consommation de stockage moyenne	Go utilisés/jour  Pourcentage consommé/jour	<p>Accédez à Grid Manager. Sur la page nœuds, sélectionnez la totalité de la grille ou d'un site et accédez à l'onglet stockage.</p> <p>Dans le graphique stockage utilisé - données d'objet, recherchez une période où la ligne est assez stable. Positionnez le curseur de votre souris sur le graphique pour estimer la quantité de stockage consommée chaque jour</p> <p>Vous pouvez collecter ces informations pour l'intégralité du système ou pour un data Center spécifique.</p>
Consommation moyenne des métadonnées	Go utilisés/jour  Pourcentage consommé/jour	<p>Accédez à Grid Manager. Sur la page nœuds, sélectionnez la totalité de la grille ou d'un site et accédez à l'onglet stockage.</p> <p>Dans le graphique stockage utilisé - métadonnées d'objet, recherchez une période où la ligne est assez stable. Positionnez le curseur de votre souris sur le graphique pour estimer la quantité de stockage de métadonnées consommée chaque jour</p> <p>Vous pouvez collecter ces informations pour l'intégralité du système ou pour un data Center spécifique.</p>
Vitesse des opérations S3/Swift	Opérations/seconde	<p>Sur le tableau de bord Grid Manager, sélectionnez <b>Performance &gt; S3 Operations</b> ou <b>Performance &gt; Swift Operations</b>.</p> <p>Pour afficher les taux d'entrée et de récupération et les nombres pour un site ou un nœud spécifique, sélectionnez <b>NODES &gt; site ou nœud de stockage &gt; objets</b>. Placez le curseur sur le graphique Ingest and Retrieve pour S3.</p>
Échec des opérations S3/Swift	Exploitation	<p>Sélectionnez <b>SUPPORT &gt; Outils &gt; topologie de grille</b>. Dans l'onglet Présentation de la section opérations d'API, affichez la valeur des opérations S3 - FAILED ou opérations Swift - FAILED.</p>
Évaluation des règles ILM	Objets/seconde	<p>Dans la page noeuds, sélectionnez <b>grid &gt; ILM</b>.</p> <p>Dans le graphique ILM Queue, recherchez une période où la ligne est assez stable. Placez votre curseur sur le graphique pour estimer la valeur de référence du <b>taux d'évaluation</b> pour votre système.</p>

Propriété	Valeur	Comment obtenir
Taux d'analyse ILM	Objets/seconde	Sélectionnez <b>NODES &gt; grid &gt; ILM</b> .  Dans le graphique ILM Queue, recherchez une période où la ligne est assez stable. Placez le curseur sur le graphique pour estimer la valeur de référence de <b>Scan Rate</b> pour votre système.
Objets mis en file d'attente à partir des opérations client	Objets/seconde	Sélectionnez <b>NODES &gt; grid &gt; ILM</b> .  Dans le graphique ILM Queue, recherchez une période où la ligne est assez stable. Placez votre curseur sur le graphique pour estimer la valeur de base des <b>objets mis en file d'attente (à partir des opérations client)</b> pour votre système.
Latence moyenne des requêtes	Millisecondes	Sélectionnez <b>NODES &gt; Storage Node &gt; Objects</b> . Dans le tableau requêtes, affichez la valeur de la latence moyenne.

### Analysez les données


Utilisez les informations que vous recueillez pour déterminer la cause du problème et les solutions potentielles.

L'analyse dépend du problème, mais en général :

- Identifiez les points de défaillance et les goulots d'étranglement à l'aide des alertes.
- Reconstituez l'historique des problèmes à l'aide de l'historique des alertes et des graphiques.
- Utilisez les tableaux pour rechercher des anomalies et comparer la situation du problème avec le fonctionnement normal.

### Liste de contrôle des informations de réaffectation

Si vous ne parvenez pas à résoudre le problème par vous-même, contactez le support technique. Avant de contacter le support technique, collectez les informations du tableau ci-dessous pour faciliter la résolution de votre problème.

	Élément	Remarques
	Énoncé du problème	Quels sont les symptômes du problème ? Quand le problème a-t-il démarré ? Cela se produit-il de manière cohérente ou intermittente ? Si elle est intermittente, à quelle heure s'est-elle produite ?  <a href="#">Définissez le problème</a>

✓	Élément	Remarques
	Évaluation de l'impact	<p>Quelle est la gravité du problème ? Quel est l'impact sur l'application client ?</p> <ul style="list-style-type: none"> <li>• Le client a-t-il déjà été connecté avec succès ?</li> <li>• Le client est-il en mesure d'ingérer, de récupérer et de supprimer des données ?</li> </ul>
	ID du système StorageGRID	Sélectionnez <b>MAINTENANCE</b> > <b>système</b> > <b>Licence</b> . L'ID système StorageGRID s'affiche dans le cadre de la licence actuelle.
	Version logicielle	Dans la partie supérieure du Gestionnaire de grille, sélectionnez l'icône d'aide et sélectionnez <b>About</b> pour afficher la version StorageGRID.
	Personnalisation	<p>Résumez le mode de configuration de votre système StorageGRID. Par exemple, énumérez les éléments suivants :</p> <ul style="list-style-type: none"> <li>• La grille utilise-t-elle la compression du stockage, le chiffrement du stockage ou la conformité ?</li> <li>• La méthode ILM permet-elle de répliquer des objets ou de les coder en effacement ? La ILM permet-elle la redondance des sites ? Les règles ILM utilisent-elles des comportements d'ingestion équilibrés, stricts ou Double validation ?</li> </ul>
	Fichiers journaux et données système	<p>Collecte des fichiers journaux et des données système pour votre système. Sélectionnez <b>SUPPORT</b> &gt; <b>Outils</b> &gt; <b>journaux</b>.</p> <p>Vous pouvez collecter les journaux pour toute la grille ou pour certains nœuds.</p> <p>Si vous ne recueillez des journaux que pour les nœuds sélectionnés, veillez à inclure au moins un nœud de stockage disposant du service ADC. (Les trois premiers nœuds de stockage d'un site incluent le service ADC.)</p> <p><a href="#">"Collecte de fichiers journaux et de données système"</a></p>
	Informations de base	<p>Collectez les informations de base relatives aux opérations d'entrée, aux opérations de récupération et à la consommation du stockage.</p> <p><a href="#">Établir les lignes de base</a></p>

✓	Élément	Remarques
	Chronologie des modifications récentes	Créez un calendrier qui résume les modifications récentes apportées au système ou à son environnement.  <a href="#">Créer un calendrier des modifications récentes</a>
	Historique des efforts déployés pour diagnostiquer le problème	Si vous avez pris des mesures pour diagnostiquer ou résoudre vous-même le problème, assurez-vous d'enregistrer les mesures que vous avez prises et les résultats obtenus.

## Résoudre les problèmes liés au stockage et aux objets

### Confirmer l'emplacement des données d'objet

Selon le problème, vous pouvez vouloir "[confirmez l'emplacement de stockage des données d'objet](#)". Par exemple, vous pouvez vérifier que la règle ILM fonctionne comme prévu et que les données d'objet sont stockées à l'emplacement prévu.

#### Avant de commencer

- Vous devez disposer d'un identifiant d'objet, qui peut être l'un des suivants :
  - **UUID** : identifiant unique universel de l'objet. Saisissez le UUID en majuscules.
  - **CBID** : identifiant unique de l'objet dans StorageGRID . Vous pouvez obtenir le CBID d'un objet à partir du journal d'audit. Saisissez le CBID en majuscules.
  - **S3 bucket et clé d'objet** : lorsqu'un objet est ingéré via "[Interface S3](#)", l'application client utilise une combinaison de clé de compartiment et d'objet pour stocker et identifier l'objet.

#### Étapes

1. Sélectionnez **ILM > Object metadata Lookup**.
2. Saisissez l'identifiant de l'objet dans le champ **Identificateur**.

Vous pouvez entrer un UUID, un CBID, un compartiment S3/une clé-objet ou un nom-objet/conteneur Swift.

3. Si vous souhaitez rechercher une version spécifique de l'objet, saisissez l'ID de version (facultatif).

4. Sélectionnez **rechercher**.

Le s'"résultats de la recherche de métadonnées d'objet" affiche. Cette page répertorie les types d'informations suivants :

- Les métadonnées système, y compris l'ID d'objet (UUID), l'ID de version (facultatif), le nom de l'objet, le nom du conteneur, le nom ou l'ID du compte de locataire, la taille logique de l'objet, la date et l'heure de la première création de l'objet, ainsi que la date et l'heure de la dernière modification de l'objet.
- Toutes les paires de clé-valeur de métadonnées utilisateur personnalisées associées à l'objet.
- Pour les objets S3, toutes les paires de clé-valeur de balise d'objet associées à l'objet.
- Pour les copies d'objet répliquées, emplacement de stockage actuel de chaque copie.
- Pour les copies d'objets avec code d'effacement, l'emplacement de stockage actuel de chaque fragment.
- Pour les copies d'objet dans Cloud Storage Pool, l'emplacement de l'objet, notamment le nom du compartiment externe et l'identifiant unique de l'objet.
- Pour les objets segmentés et les objets multisegments, une liste de segments d'objet, y compris les identificateurs de segments et la taille des données. Pour les objets de plus de 100 segments, seuls les 100 premiers segments sont affichés.
- Toutes les métadonnées d'objet dans le format de stockage interne non traité. Ces métadonnées brutes incluent les métadonnées du système interne qui ne sont pas garanties de la version à la version.

L'exemple suivant présente les résultats de la recherche de métadonnées d'objet pour un objet de test S3 stocké sous forme de deux copies répliquées.

### System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

### Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H\$ TFbnQQ} CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H\$ TFboW28 CXG%

### Raw Metadata

```
{
  "TYPE": "CTNT",
  "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
  "NAME": "testobject",
  "CBID": "0x88230E7EC7C10416",
  "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
  "PPTH": "source",
  "META": {
    "BASE": {
      "PAIRS": "2",










```

### Défaillances de stockage d'objets (volume de stockage)




















Le stockage sous-jacent d'un nœud de stockage est divisé en magasins d'objets. Les magasins d'objets sont également appelés volumes de stockage.

Vous pouvez afficher les informations de magasin d'objets pour chaque nœud de stockage. Les magasins d'objets sont affichés en bas de la page **NOEUDS > Storage Node > Storage**.






























## Disk devices

Name  	World Wide Name  	I/O load  	Read rate  	Write rate  
sdc(8:16,sdb)	N/A	0.05%	0 bytes/s	4 KB/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s
sdf(8:64,sde)	N/A	0.00%	0 bytes/s	82 bytes/s
sdg(8:80,sdf)	N/A	0.00%	0 bytes/s	82 bytes/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	4 KB/s
cvloc(8:2,sda2)	N/A	0.95%	0 bytes/s	52 KB/s

## Volumes

Mount point  	Device  	Status  	Size  	Available  	Write cache status  
/	croot	Online	21.00 GB	14.73 GB 	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB 	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB 	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB 	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB 	Enabled
/var/local/rangedb/3	sdf	Online	107.32 GB	107.18 GB 	Enabled
/var/local/rangedb/4	sdg	Online	107.32 GB	107.18 GB 	Enabled

## Object stores

ID  	Size  	Available  	Replicated data  	EC data  	Object data (%)  	Health  
0000	107.32 GB	96.44 GB 	1.55 MB 	0 bytes 	0.00%	No Errors
0001	107.32 GB	107.18 GB 	0 bytes 	0 bytes 	0.00%	No Errors
0002	107.32 GB	107.18 GB 	0 bytes 	0 bytes 	0.00%	No Errors
0003	107.32 GB	107.18 GB 	0 bytes 	0 bytes 	0.00%	No Errors
0004	107.32 GB	107.18 GB 	0 bytes 	0 bytes 	0.00%	No Errors



Pour en savoir plus "[Détails sur chaque nœud de stockage](#)", procédez comme suit :

1. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
2. Sélectionnez **site** > **Storage Node** > **LDR** > **Storage** > **Présentation** > **main**.

**Overview: LDR (DC1-S1) - Storage**  
Updated: 2020-01-29 15:03:39 PST

---

Storage State - Desired:	Online	
Storage State - Current:	Online	
Storage Status:	No Errors	

### Utilization

Total Space:	322 GB	
Total Usable Space:	311 GB	
Total Usable Space (Percent):	96.534 %	
Total Data:	994 KB	
Total Data (Percent):	0 %	

### Replication

Block Reads:	0	
Block Writes:	0	
Objects Retrieved:	0	
Objects Committed:	0	
Objects Deleted:	0	
Delete Service State:	Enabled	

### Object Store Volumes

ID	Total	Available	Replicated Data	EC Data	Stored (%)	Health	
0000	107 GB	96.4 GB	994 KB	0 B	0.001 %	No Errors	
0001	107 GB	107 GB	0 B	0 B	0 %	No Errors	
0002	107 GB	107 GB	0 B	0 B	0 %	No Errors	

Selon la nature de la défaillance, les défaillances avec un volume de stockage peuvent être reflétées dans "[alertes de volume de stockage](#)". En cas de défaillance d'un volume de stockage, réparez le volume de stockage défectueux pour restaurer le nœud de stockage à son plein fonctionnement dès que possible. Si nécessaire, vous pouvez accéder à l'onglet **Configuration** "[Placez le nœud de stockage en lecture seule](#)" pour que le système StorageGRID puisse l'utiliser pour la récupération des données tout en vous préparant à une récupération complète du serveur.

### Vérifiez l'intégrité de l'objet

Le système StorageGRID vérifie l'intégrité des données d'objet sur les nœuds de stockage, en vérifiant la présence d'objets corrompus et manquants.

Il existe deux processus de vérification : la vérification des antécédents et la vérification de l'existence des objets (anciennement appelée vérification de premier plan). Elles travaillent ensemble pour assurer l'intégrité des données. La vérification en arrière-plan s'exécute automatiquement et vérifie en continu l'exactitude des données d'objet. La vérification de l'existence d'un objet peut être déclenchée par un utilisateur pour vérifier plus rapidement l'existence (mais pas l'exactitude) d'objets.

### Qu'est-ce que la vérification des antécédents ?

Le processus de vérification en arrière-plan vérifie automatiquement et en continu les nœuds de stockage pour

détecter des copies corrompues de données d'objet et tente automatiquement de résoudre les problèmes qu'il trouve.

La vérification en arrière-plan vérifie l'intégrité des objets répliqués et des objets avec code d'effacement, comme suit :

- **Objets répliqués** : si le processus de vérification en arrière-plan trouve un objet répliqué corrompu, la copie corrompue est supprimée de son emplacement et mise en quarantaine ailleurs sur le nœud de stockage. Une nouvelle copie non corrompue est ensuite générée et placée pour respecter les règles ILM actives. Il se peut que la nouvelle copie ne soit pas placée sur le nœud de stockage utilisé pour la copie d'origine.



Les données d'objet corrompues sont mises en quarantaine au lieu d'être supprimées du système, de sorte qu'elles soient toujours accessibles. Pour plus d'informations sur l'accès aux données d'objet en quarantaine, contactez le support technique.

- **Objets avec code d'effacement** : si le processus de vérification en arrière-plan détecte qu'un fragment d'un objet avec code d'effacement est corrompu, StorageGRID tente automatiquement de reconstruire le fragment manquant en place sur le même nœud de stockage, en utilisant les données restantes et les fragments de parité. Si le fragment corrompu ne peut pas être reconstruit, une tentative est faite pour extraire une autre copie de l'objet. Lorsque la récupération réussit, une évaluation du ILM est effectuée pour créer une copie de remplacement de l'objet avec code d'effacement.

Le processus de vérification en arrière-plan vérifie uniquement les objets sur les nœuds de stockage. Elle ne vérifie pas les objets dans un pool de stockage cloud. Les objets doivent être âgés de plus de quatre jours pour être admissibles à la vérification des antécédents.

La vérification des antécédents s'exécute à un taux continu conçu pour ne pas interférer avec les activités ordinaires du système. Impossible d'arrêter la vérification en arrière-plan. Toutefois, vous pouvez augmenter le taux de vérification en arrière-plan pour vérifier plus rapidement le contenu d'un nœud de stockage si vous soupçonnez un problème.

### Alertes liées à la vérification des antécédents

Si le système détecte un objet corrompu qu'il ne peut pas corriger automatiquement (parce que la corruption empêche l'objet d'être identifié), l'alerte **objet corrompu non identifié détecté** est déclenchée.

Si la vérification en arrière-plan ne peut pas remplacer un objet corrompu car il ne peut pas localiser une autre copie, l'alerte **objets perdus** est déclenchée.

### Modifier le taux de vérification des antécédents

Vous pouvez modifier la vitesse à laquelle la vérification en arrière-plan vérifie les données d'objet répliquées sur un nœud de stockage si vous avez des problèmes d'intégrité des données.

#### Avant de commencer

- Vous devez être connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).

#### Description de la tâche

Vous pouvez modifier le taux de vérification pour la vérification en arrière-plan sur un nœud de stockage :

- Adaptatif : paramètre par défaut. La tâche est conçue pour vérifier à un maximum de 4 Mo/s ou 10 objets/s

(selon la première limite dépassée).

- Élevé : la vérification du stockage s'effectue rapidement, à une vitesse qui peut ralentir les activités ordinaires des systèmes.

Utilisez le taux de vérification élevé uniquement si vous soupçonnez qu'une erreur matérielle ou logicielle pourrait avoir des données d'objet corrompues. Une fois la vérification de l'arrière-plan de priorité élevée terminée, le taux de vérification se réinitialise automatiquement sur Adaptive.

## Étapes

1. Sélectionnez **SUPPORT > Outils > topologie de grille**.
2. Sélectionnez **Storage Node > LDR > Verification**.
3. Sélectionnez **Configuration > main**.
4. Accédez à **LDR > Verification > Configuration > main**.
5. Sous Vérification de l'arrière-plan, sélectionnez **taux de vérification > taux élevé** ou **taux de vérification > adaptatif**.

Overview Alarms Reports Configuration

Main

Configuration: LDR (Storage Node) - Verification  
Updated: 2021-11-11 07:13:00 MST

Reset Missing Objects Count

**Background Verification**

Verification Rate

Reset Corrupt Objects Count

**Quarantined Objects**

Delete Quarantined Objects

Apply Changes

6. Cliquez sur **appliquer les modifications**.
7. Surveiller les résultats de la vérification en arrière-plan des objets répliqués.
  - a. Accédez à **NOEUDS > Storage Node > objets**.
  - b. Dans la section Vérification, surveillez les valeurs de **objets corrompus** et **objets corrompus non identifiés**.

Si la vérification en arrière-plan trouve des données d'objet répliqué corrompues, la mesure **objets corrompus** est incrémentée et StorageGRID tente d'extraire l'identificateur d'objet des données, comme suit :

- Si l'identifiant d'objet peut être extrait, StorageGRID crée automatiquement une nouvelle copie des données de l'objet. La nouvelle copie peut être effectuée à n'importe quel endroit du système

StorageGRID qui respecte les règles ILM actives.

- Si l'identifiant de l'objet ne peut pas être extrait (car il a été corrompu), la mesure **objets corrompus non identifiés** est incrémentée et l'alerte **objet corrompu non identifié détecté** est déclenchée.

c. Si des données d'objet répliqué corrompues sont trouvées, contactez le support technique pour déterminer la cause première de la corruption.

8. Surveillez les résultats de la vérification en arrière-plan des objets avec code d'effacement.

Si la vérification en arrière-plan détecte des fragments corrompus de données d'objet codées par effacement, l'attribut fragments corrompus détectés est incrémenté. StorageGRID restaure en reconstruisant le fragment corrompu sur le même nœud de stockage.

a. Sélectionnez **SUPPORT > Outils > topologie de grille**.

b. Sélectionnez **Storage Node > LDR > codage d'effacement**.

c. Dans le tableau Résultats de la vérification, surveillez l'attribut fragments corrompus détectés (ECCD).

9. Une fois les objets corrompus automatiquement restaurés par le système StorageGRID, réinitialisez le nombre d'objets corrompus.

a. Sélectionnez **SUPPORT > Outils > topologie de grille**.

b. Sélectionnez **Storage Node > LDR > Verification > Configuration**.

c. Sélectionnez **Réinitialiser le nombre d'objets corrompus**.

d. Cliquez sur **appliquer les modifications**.

10. Si vous êtes sûr que les objets mis en quarantaine ne sont pas nécessaires, vous pouvez les supprimer.



Si l'alerte **objets perdus** a été déclenchée, le support technique peut vouloir accéder aux objets mis en quarantaine pour aider à déboguer le problème sous-jacent ou tenter de récupérer les données.

a. Sélectionnez **SUPPORT > Outils > topologie de grille**.

b. Sélectionnez **Storage Node > LDR > Verification > Configuration**.

c. Sélectionnez **Supprimer les objets en quarantaine**.

d. Sélectionnez **appliquer les modifications**.

#### Qu'est-ce que la vérification de l'existence d'objet ?

Le contrôle d'existence d'objet vérifie si toutes les copies répliquées attendues d'objets et de fragments avec code d'effacement existent sur un nœud de stockage. La vérification de l'existence des objets ne vérifie pas les données de l'objet lui-même (la vérification en arrière-plan le fait) ; elle permet plutôt de vérifier l'intégrité des périphériques de stockage, en particulier si un problème matériel récent pouvait affecter l'intégrité des données.

Contrairement à la vérification de l'arrière-plan, qui se produit automatiquement, vous devez démarrer manuellement un travail de vérification de l'existence d'un objet.

Le contrôle d'existence des objets lit les métadonnées de chaque objet stocké dans StorageGRID et vérifie l'existence de copies d'objet répliquées et de fragments d'objet avec code d'effacement. Les données manquantes sont traitées comme suit :

- **Copies répliquées** : si une copie des données d'objet répliqué est manquante, StorageGRID tente

automatiquement de remplacer la copie d'une autre copie stockée dans le système. Le nœud de stockage exécute une copie existante via une évaluation ILM. Elle détermine que la politique ILM actuelle n'est plus respectée pour cet objet, car une autre copie est manquante. Une nouvelle copie est générée et placée pour respecter les règles ILM actives du système. Cette nouvelle copie peut ne pas être placée au même endroit où la copie manquante a été stockée.

- **Fragments codés par effacement** : si un fragment d'un objet codé par effacement est manquant, StorageGRID tente automatiquement de reconstruire le fragment manquant sur le même nœud de stockage en utilisant les fragments restants. Si le fragment manquant ne peut pas être reconstruit (en raison de la perte d'un trop grand nombre de fragments), ILM tente de trouver une autre copie de l'objet, qu'il peut utiliser pour générer un nouveau fragment avec code d'effacement.

## Exécutez la vérification de l'existence d'objet

Vous créez et exécutez un travail de vérification de l'existence d'un objet à la fois. Lorsque vous créez un travail, vous sélectionnez les nœuds de stockage et les volumes à vérifier. Vous sélectionnez également la cohérence du travail.

### Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Maintenance ou autorisation d'accès racine"](#).
- Vous avez vérifié que les nœuds de stockage à vérifier sont en ligne. Sélectionnez **NOEUDS** pour afficher la table des noeuds. Assurez-vous qu'aucune icône d'alerte n'apparaît en regard du nom du nœud pour les nœuds que vous souhaitez vérifier.
- Vous avez vérifié que les procédures suivantes sont **non** exécutées sur les nœuds que vous voulez vérifier :
  - Extension de la grille pour ajouter un nœud de stockage
  - Désaffectation du nœud de stockage
  - Restauration d'un volume de stockage défaillant
  - Récupération d'un nœud de stockage avec un lecteur système défaillant
  - Rééquilibrage EC
  - Clone du nœud d'appliance

Le contrôle d'existence d'objet ne fournit pas d'informations utiles pendant que ces procédures sont en cours.

### Description de la tâche

Une tâche de vérification de l'existence d'un objet peut prendre des jours ou des semaines, selon le nombre d'objets dans la grille, les nœuds et volumes de stockage sélectionnés et la cohérence sélectionnée. Vous ne pouvez exécuter qu'une seule tâche à la fois, mais vous pouvez sélectionner plusieurs nœuds de stockage et volumes en même temps.

### Étapes

1. Sélectionnez **MAINTENANCE > tâches > Vérification d'existence d'objet**.
2. Sélectionnez **Créer un travail**. L'assistant création d'un objet Vérification de l'existence s'affiche.
3. Sélectionnez les nœuds contenant les volumes à vérifier. Pour sélectionner tous les nœuds en ligne, cochez la case **Node name** dans l'en-tête de colonne.

Vous pouvez effectuer vos recherches par nom de nœud ou site.

Vous ne pouvez pas sélectionner de nœuds qui ne sont pas connectés à la grille.

4. Sélectionnez **Continuer**.
5. Sélectionnez un ou plusieurs volumes pour chaque nœud de la liste. Vous pouvez rechercher des volumes à l'aide du numéro du volume de stockage ou du nom du nœud.

Pour sélectionner tous les volumes pour chaque nœud sélectionné, cochez la case **Storage volume** dans l'en-tête de colonne.

6. Sélectionnez **Continuer**.
7. Sélectionnez la cohérence du travail.

La cohérence détermine le nombre de copies des métadonnées d'objet utilisées pour la vérification de l'existence des objets.

- **Site fort** : deux copies de métadonnées sur un seul site.
- **Fort-global**: Deux copies de métadonnées à chaque site.
- **Tout** (par défaut) : les trois copies des métadonnées de chaque site.

Pour plus d'informations sur la cohérence, reportez-vous aux descriptions fournies par l'assistant.

8. Sélectionnez **Continuer**.
9. Vérifiez et vérifiez vos sélections. Vous pouvez sélectionner **Précédent** pour passer à l'étape précédente de l'assistant afin de mettre à jour vos sélections.

Un travail de vérification de l'existence d'un objet est généré et exécuté jusqu'à ce que l'un des événements suivants se produise :

- Le travail se termine.
- Vous mettez en pause ou annulez le travail. Vous pouvez reprendre un travail que vous avez interrompu, mais vous ne pouvez pas reprendre un travail que vous avez annulé.
- Le travail se bloque. L'alerte \* Vérification de l'existence de l'objet a calé\* est déclenchée. Suivez les actions correctives spécifiées pour l'alerte.
- Le travail échoue. L'alerte **échec de la vérification de l'existence de l'objet** est déclenchée. Suivez les actions correctives spécifiées pour l'alerte.
- Un message « Service non disponible » ou « erreur de serveur interne » s'affiche. Au bout d'une minute, actualisez la page pour continuer à surveiller le travail.



Si nécessaire, vous pouvez naviguer hors de la page de vérification de l'existence d'un objet et revenir à la page de suivi du travail.

10. Pendant l'exécution du travail, affichez l'onglet **travail actif** et notez la valeur des copies d'objet manquantes détectées.

Cette valeur représente le nombre total de copies manquantes d'objets répliqués et d'objets avec code d'effacement avec un ou plusieurs fragments manquants.

Si le nombre de copies d'objet manquantes détectées est supérieur à 100, il peut y avoir un problème avec le stockage du nœud de stockage.

# Object existence check

Perform an object existence check if you suspect some storage volumes have been damaged or are corrupt and you want to verify that objects still exist on these volumes.

If you have questions about running object existence check, contact technical support.

**Active job**    Job history

Status: Accepted    Consistency control: All  
Job ID: 2334602652907829302    Start time: 2021-11-10 14:43:02 MST  
Missing object copies detected: 0    Elapsed time: —  
Progress: 0%    Estimated time to completion: —

Pause    Cancel

**Volumes**    Details

Selected node	Selected storage volumes	Site
DC1-S1	0, 1, 2	Data Center 1
DC1-S2	0, 1, 2	Data Center 1
DC1-S3	0, 1, 2	Data Center 1

11. Une fois le travail terminé, prenez les mesures supplémentaires requises :

- Si les copies d'objet manquantes détectées sont nulles, aucun problème n'a été trouvé. Aucune action n'est requise.
- Si les copies d'objet manquantes détectées sont supérieures à zéro et que l'alerte **objets perdus** n'a pas été déclenchée, toutes les copies manquantes ont été réparées par le système. Vérifiez que tout problème matériel a été corrigé pour éviter d'endommager ultérieurement les copies d'objet.
- Si les copies d'objet manquantes détectées sont supérieures à zéro et que l'alerte **objets perdus** a été déclenchée, l'intégrité des données pourrait être affectée. Contactez l'assistance technique.
- Vous pouvez rechercher des copies d'objet perdues en utilisant grep pour extraire les messages d'audit LLST : `grep LLST audit_file_name`.

Cette procédure est similaire à celle de "[analyse des objets perdus](#)", bien que pour les copies d'objet que vous recherchez LLST à la place de OLST .

12. Si vous avez sélectionné une cohérence solide ou globale pour le travail, attendez environ trois semaines avant d'exécuter à nouveau le travail sur les mêmes volumes.

Lorsque StorageGRID a eu le temps d'assurer la cohérence des métadonnées pour les nœuds et les volumes inclus dans le travail, réexécuter ce travail peut effacer les copies d'objet manquantes, ou faire vérifier d'autres copies d'objet si elles ne sont pas prises en compte.

- Sélectionnez **MAINTENANCE > Vérification de l'existence d'objet > Historique du travail**.
- Déterminez les travaux prêts à être réexécutés :

- i. Consultez la colonne **end Time** pour déterminer les tâches qui ont été exécutées il y a plus de trois semaines.
  - ii. Pour ces travaux, scannez la colonne de contrôle de cohérence pour obtenir un site fort ou fort-global.
- c. Cochez la case de chaque travail à repasser, puis sélectionnez **repassage**.

## Object existence check

Perform an object existence check if you suspect some storage volumes have been damaged or are corrupt and you want to verify that objects still exist on these volumes.

If you have questions about running object existence check, contact technical support.

Active job

Job history

Delete

Rerun

Search by Job ID/ node name/ consistency control/ start time

Displaying 4 results

<input type="checkbox"/>	Job ID <span style="font-size: x-small;">?</span>	Status <span style="font-size: x-small;">?</span>	Nodes (volumes) <span style="font-size: x-small;">?</span>	Missing object copies detected <span style="font-size: x-small;">?</span>	Consistency control <span style="font-size: x-small;">?</span>	Start time <span style="font-size: x-small;">?</span>	End time <span style="font-size: x-small;">?</span>
<input checked="" type="checkbox"/>	2334602652907829302	Completed	DC1-S1 (3 volumes) DC1-S2 (3 volumes) DC1-S3 (3 volumes) and <a href="#">7 more</a>	0	All	2021-11-10 14:43:02 MST	2021-11-10 14:43:06 MST (3 weeks ago)
<input type="checkbox"/>	11725651898848823235 (Rerun job)	Completed	DC1-S2 (2 volumes) DC1-S3 (2 volumes) DC1-S4 (2 volumes) and <a href="#">4 more</a>	0	Strong-site	2021-11-10 14:42:10 MST	2021-11-10 14:42:11 MST (17 minutes ago)

- d. Dans l'assistant Réanalyser les travaux, examinez les nœuds et volumes sélectionnés et la cohérence.
- e. Lorsque vous êtes prêt à réexécuter les travaux, sélectionnez **repassage**.

L'onglet travail actif s'affiche. Tous les travaux que vous avez sélectionnés sont réexécutés comme un travail à une cohérence de site fort. Un champ **travaux connexes** de la section Détails répertorie les ID des travaux d'origine.

### Une fois que vous avez terminé

Si vous avez toujours des problèmes d'intégrité des données, accédez à **SUPPORT > Outils > topologie de grille > site > Storage Node > LDR > Verification > Configuration > main** et augmentez le taux de vérification en arrière-plan. La vérification en arrière-plan vérifie l'exactitude de toutes les données d'objet stockées et répare tout problème détecté. Trouver et réparer les problèmes le plus rapidement possible réduit le risque de perte de données.

### Dépannez l'alerte de taille d'objet PUT S3 trop grande

L'alerte S3 PUT Object size too large est déclenchée si un locataire tente une opération PutObject non parties qui dépasse la taille limite S3 de 5 Gio.

### Avant de commencer



- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).

Déterminez les locataires qui utilisent des objets supérieurs à 5 Gio. Vous pouvez donc les informer.

### Étapes

1. Accédez à **CONFIGURATION > surveillance > Audit et serveur syslog**.
2. Si les écritures client sont normales, accédez au journal d'audit :

- a. Entrée `ssh admin@primary_Admin_Node_IP`
- b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
- c. Entrez la commande suivante pour basculer en root : `su -`
- d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

- e. Entrée `cd /var/local/log`



["Découvrez les destinations des informations d'audit"](#).

- f. Identifiez les locataires qui utilisent des objets de plus de 5 Gio.
  - i. Entrée `zgrep SPUT * | egrep "CSIZ\(UI64\) : ([5-9] | [1-9] [0-9]+) [0-9] {9}"`
  - ii. Pour chaque message d'audit dans les résultats, consultez le `S3AI` champ pour déterminer l'ID de compte de locataire. Utilisez les autres champs du message pour déterminer l'adresse IP utilisée par le client, le compartiment et l'objet :

Code	Description
SAIP	Adresse IP source
S3AI	ID locataire
S3BK	Godet
S3KY	Objet
CSIZ	Taille (octets)

### Exemple de résultats du journal d'audit

```
audit.log:2023-01-05T18:47:05.525999
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1672943621106262][TIME(UI64):80431733
3][SAIP(IPAD):"10.96.99.127"][S3AI(CSTR):"93390849266154004343"][SACC(CS
TR):"bhavna"][S3AK(CSTR):"06OX85M40Q90Y280B7YT"][SUSR(CSTR):"urn:sgws:id
entity::93390849266154004343:root"][SBAI(CSTR):"93390849266154004343"][S
BAC(CSTR):"bhavna"][S3BK(CSTR):"test"][S3KY(CSTR):"large-
object"][CBID(UI64):0x077EA25F3B36C69A][UUID(CSTR):"A80219A2-CD1E-466F-
9094-
B9C0FDE2FFA3"][CSIZ(UI64):6040000000][MTME(UI64):1672943621338958][AVER(
UI32):10][ATIM(UI64):1672944425525999][ATYP(FC32):SPUT][ANID(UI32):12220
829][AMID(FC32):S3RQ][ATID(UI64):4333283179807659119]]
```

3. Si les écritures du client ne sont pas normales, utilisez l'ID de locataire de l'alerte pour identifier le locataire :

- a. Accédez à **SUPPORT > Outils > journaux**. Collectez les journaux d'application du nœud de stockage dans l'alerte. Spécifiez 15 minutes avant et après l'alerte.
- b. Extraire le fichier et aller à `bycast.log`:

```
/GID<grid_id>_<time_stamp>/<site_node>/<time_stamp>/grid/bycast.log
```

- c. Recherchez le journal `method=PUT` et identifiez le client dans le `clientIP` champ.

#### Exemple bycast.log

```
Jan  5 18:33:41 BHAVNAJ-DC1-S1-2-65 ADE: |12220829 1870864574 S3RQ %CEA
2023-01-05T18:33:41.208790| NOTICE 1404 af23cb66b7e3efa5 S3RQ:
EVENT_PROCESS_CREATE - connection=1672943621106262 method=PUT
name=</test/4MiB-0> auth=<V4> clientIP=<10.96.99.127>
```

4. Indiquez aux locataires que la taille maximale de `PutObject` est de 5 Gio et que vous devez utiliser des téléchargements partitionnés pour les objets supérieurs à 5 Gio.
5. Ignorez l'alerte pendant une semaine si l'application a été modifiée.

## Dépanner les données d'objet perdues ou manquantes

### Dépanner les données d'objet perdues ou manquantes

Les objets peuvent être récupérés pour plusieurs raisons, y compris les demandes de lecture provenant d'une application client, les vérifications en arrière-plan des données d'objet répliquées, les réévaluations ILM et la restauration des données d'objet lors de la restauration d'un nœud de stockage.

Le système StorageGRID utilise les informations d'emplacement dans les métadonnées d'un objet pour déterminer l'emplacement à partir duquel vous souhaitez récupérer l'objet. Si une copie de l'objet n'est pas trouvée à l'emplacement prévu, le système tente de récupérer une autre copie de l'objet à partir d'un autre emplacement du système, en supposant que la règle ILM contient une règle permettant de créer au moins

deux copies de l'objet.

Si cette récupération réussit, le système StorageGRID remplace la copie manquante de l'objet. Sinon, l'alerte **objets perdus** est déclenchée comme suit :

- Pour les copies répliquées, si une autre copie ne peut pas être récupérée, l'objet est considéré comme perdu et l'alerte est déclenchée.
- Pour les copies avec code d'effacement, si une copie ne peut pas être récupérée à partir de l'emplacement attendu, l'attribut copies corrompues détectées (ECOR) est incrémenté d'une copie avant qu'une tentative de récupération d'une copie ne soit effectuée à partir d'un autre emplacement. Si aucune autre copie n'est trouvée, l'alerte est déclenchée.

Vous devez examiner immédiatement toutes les alertes **objets perdus** pour déterminer la cause première de la perte et déterminer si l'objet peut encore exister dans un noeud de stockage hors ligne ou actuellement indisponible. Voir "[Rechercher les objets perdus](#)".

Dans le cas où les données d'objet sans copie sont perdues, il n'y a pas de solution de récupération. Cependant, vous devez réinitialiser le compteur d'objets perdus pour empêcher les objets perdus connus de masquer les nouveaux objets perdus. Voir "[Réinitialiser le nombre d'objets perdus et manquants](#)".

### Rechercher les objets perdus

Lorsque l'alerte **objets perdus** est déclenchée, vous devez examiner immédiatement. Collectez des informations sur les objets affectés et contactez le support technique.

#### Avant de commencer

- Vous devez être connecté au Gestionnaire de grille à l'aide d'un "[navigateur web pris en charge](#)".
- Vous avez "[autorisations d'accès spécifiques](#)".
- Vous devez avoir le `Passwords.txt` fichier.

#### Description de la tâche

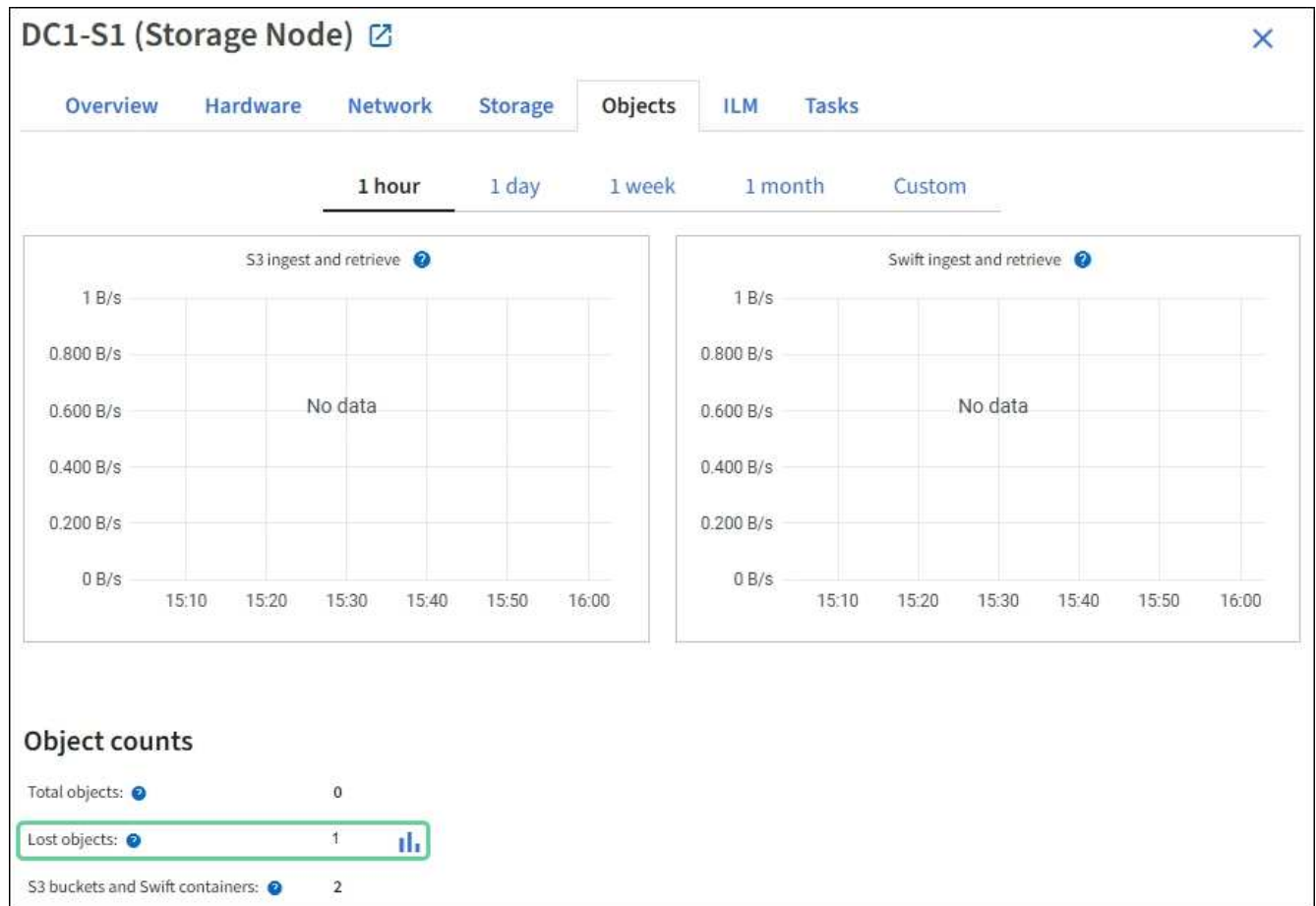
L'alerte **objets perdus** indique que StorageGRID estime qu'il n'y a pas de copie d'un objet dans la grille. Les données ont peut-être été définitivement perdues.

Recherchez immédiatement les alertes relatives à la perte d'objet. Vous devrez peut-être prendre des mesures pour éviter d'autres pertes de données. Dans certains cas, vous pourrez peut-être restaurer un objet perdu si vous prenez une action d'invite.


#### Étapes

1. Sélectionnez **NOEUDS**.
2. Sélectionnez **Storage Node > objets**.
3. Vérifiez le nombre d'objets perdus affichés dans le tableau nombres d'objets.

Ce nombre indique le nombre total d'objets que ce nœud de grille détecte comme manquant dans l'ensemble du système StorageGRID. La valeur est la somme des compteurs d'objets perdus du composant de stockage de données dans les services LDR et DDS.



4. À partir d'un nœud d'administration, "[accédez au journal d'audit](#)" pour déterminer l'identifiant unique (UUID) de l'objet qui a déclenché l'alerte **objets perdus** :
  - a. Connectez-vous au nœud grid :
    - i. Entrez la commande suivante : `ssh admin@grid_node_IP`
    - ii. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
    - iii. Entrez la commande suivante pour basculer en root : `su -`
    - iv. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier. Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.
  - b. Accédez au répertoire dans lequel se trouvent les journaux d'audit. Entrer : `cd /var/local/log/`

 "[Découvrez les destinations des informations d'audit](#)".
  - c. Utilisez `grep` pour extraire les messages d'audit objet perdu (OLST). Entrer : `grep OLST audit_file_name`
  - d. Notez la valeur UUID incluse dans le message.

```
>Admin: # grep OLSM audit.log
2020-02-12T19:18:54.780426
[AUDT:[CBID(UI64):0x38186FE53E3C49A5][UUID(CSTR):926026C4-00A4-449B-
AC72-BCCA72DD1311]
[PATH(CSTR):"source/cats"][NOID(UI32):12288733][VOLI(UI64):3222345986
][RSLT(FC32):NONE][AVER(UI32):10]
[ATIM(UI64):1581535134780426][ATYP(FC32):OLSM][ANID(UI32):12448208][A
MID(FC32):ILMX][ATID(UI64):7729403978647354233]]
```

5. Rechercher les métadonnées de l'objet perdu à l'aide de l'UUID :

- a. Sélectionnez **ILM > Object metadata Lookup**.
- b. Entrez l'UUID et sélectionnez **Rechercher**.
- c. Vérifiez les emplacements dans les métadonnées et prenez les mesures appropriées :

Les métadonnées	Conclusion
<object_identifieur> d'objet introuvable	<p>Si l'objet n'est pas trouvé, le message "ERREUR:" est renvoyé.</p> <p>Si l'objet est introuvable, vous pouvez réinitialiser le nombre d'objets perdus* pour effacer l'alerte. L'absence d'objet indique que l'objet a été supprimé intentionnellement.</p>
Emplacements > 0	<p>Si des emplacements sont répertoriés dans la sortie, l'alerte <b>objets perdus</b> peut être un faux positif.</p> <p>Vérifiez que les objets existent. Utilisez l'ID de nœud et le chemin du fichier indiqués dans la sortie pour confirmer que le fichier objet se trouve à l'emplacement indiqué.</p> <p>(La procédure de "<a href="#">recherche d'objets potentiellement perdus</a>" explique comment utiliser l'ID de nœud pour trouver le nœud de stockage correct.)</p> <p>Si les objets existent, vous pouvez réinitialiser le nombre d'objets perdus* pour effacer l'alerte.</p>
Emplacements = 0	<p>Si aucun emplacement n'est répertorié dans le résultat, l'objet est potentiellement manquant. Vous pouvez essayer "<a href="#">recherchez et restaurez l'objet</a>" par vous-même ou contacter le support technique.</p> <p>L'assistance technique peut vous demander si une procédure de restauration du stockage est en cours. Voir les informations sur "<a href="#">Restauration des données d'objet à l'aide de Grid Manager</a>" et "<a href="#">restauration des données d'objet vers un volume de stockage</a>".</p>

**Recherche et restauration d'objets potentiellement perdus**

Il est possible de trouver et de restaurer des objets qui ont déclenché une alerte **Object**

**Lost** et une alarme héritée Lost Objects (LOST) et que vous avez identifié comme potentiellement perdus.

#### Avant de commencer

- Vous disposez de l'UUID de tout objet perdu, tel qu'identifié dans ["Rechercher les objets perdus"](#).
- Vous avez le `Passwords.txt` fichier.

#### Description de la tâche

Vous pouvez suivre cette procédure pour rechercher les copies répliquées de l'objet perdu ailleurs dans la grille. Dans la plupart des cas, l'objet perdu est introuvable. Toutefois, dans certains cas, vous pouvez trouver et restaurer un objet répliqué perdu si vous prenez une action rapide.



Pour obtenir de l'aide sur cette procédure, contactez le support technique.

#### Étapes

1. À partir d'un nœud d'administration, recherchez dans les journaux d'audit les emplacements d'objets possibles :
  - a. Connectez-vous au nœud grid :
    - i. Entrez la commande suivante : `ssh admin@grid_node_IP`
    - ii. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
    - iii. Entrez la commande suivante pour basculer en root : `su -`
    - iv. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier. Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.
  - b. Accédez au répertoire où se trouvent les journaux d'audit : `cd /var/local/log/`



["Découvrez les destinations des informations d'audit"](#).

- c. Utilisez `grep` pour extraire le ["messages d'audit associés à l'objet potentiellement perdu"](#) et les envoyer à un fichier de sortie. Entrer : `grep uuid-value audit_file_name > output_file_name`

Par exemple :

```
Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
messages_about_lost_object.txt
```

- d. Utilisez `grep` pour extraire les messages d'audit emplacement perdu (LLST) de ce fichier de sortie. Entrer : `grep LLST output_file_name`

Par exemple :

```
Admin: # grep LLST messages_about_lost_objects.txt
```

Un message d'audit LLST ressemble à cet exemple de message.

```
[AUDT:\ [NOID\ (UI32\ ) :12448208\ ] [CBIL (UI64) :0x38186FE53E3C49A5]
[UUID (CSTR) : "926026C4-00A4-449B-AC72-BCCA72DD1311" ] [LTYP (FC32) :CLDI]
[PCLD\ (CSTR\ ) : "/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6"\ ]
[TSRC (FC32) :SYST] [RSLT (FC32) :NONE] [AVER (UI32) :10] [ATIM (UI64) :
1581535134379225] [ATYP (FC32) :LLST] [ANID (UI32) :12448208] [AMID (FC32) :CL
SM]
[ATID (UI64) :7086871083190743409]]
```

e. Recherchez le champ PCLD et LE champ NOID dans le message LLST.

Le cas échéant, la valeur de PCLD correspond au chemin complet du disque vers la copie de l'objet répliqué manquante. La valeur de NOID est l'ID de nœud du LDR dans lequel une copie de l'objet peut être trouvée.

Si vous trouvez un emplacement d'objet, vous pourrez peut-être restaurer l'objet.

a. Recherchez le nœud de stockage associé à cet ID de nœud LDR. Dans le Gestionnaire de grille, sélectionnez **SUPPORT > Outils > topologie de grille**. Sélectionnez ensuite **Data Center > Storage Node > LDR**.

L'ID de nœud du service LDR se trouve dans le tableau informations sur le nœud. Vérifiez les informations pour chaque nœud de stockage jusqu'à ce que vous trouviez celui qui héberge ce LDR.

2. Déterminez si l'objet existe sur le nœud de stockage indiqué dans le message d'audit :

a. Connectez-vous au nœud grid :

- i. Entrez la commande suivante : `ssh admin@grid_node_IP`
- ii. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
- iii. Entrez la commande suivante pour basculer en root : `su -`
- iv. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

b. Déterminez si le chemin du fichier de l'objet existe.

Pour le chemin du fichier de l'objet, utilisez la valeur PCLD du message d'audit LLST.

Par exemple, entrez :

```
ls '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
```



Placez toujours le chemin d'accès au fichier d'objet entre guillemets simples dans des commandes pour échapper à tout caractère spécial.

- Si le chemin d'accès à l'objet est introuvable, l'objet est perdu et ne peut pas être restauré à l'aide de cette procédure. Contactez l'assistance technique.
- Si le chemin d'accès à l'objet est trouvé, passez à l'étape suivante. Vous pouvez essayer de

restaurer à nouveau l'objet trouvé dans StorageGRID.

3. Si le chemin d'accès à l'objet a été trouvé, essayez de restaurer l'objet sur StorageGRID :
  - a. À partir du même nœud de stockage, modifiez la propriété du fichier objet afin qu'il puisse être géré par StorageGRID. Entrer : `chown ldr-user:bycast 'file_path_of_object'`
  - b. Telnet vers localhost 1402 pour accéder à la console LDR. Entrer : `telnet 0 1402`
  - c. Entrer : `cd /proc/STOR`
  - d. Entrer : `Object_Found 'file_path_of_object'`

Par exemple, entrez :

```
Object_Found '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
```

L'exécution `Object_Found` de la commande avertit la grille de l'emplacement de l'objet. Elle déclenche également les règles ILM actives, qui ajoutent des copies supplémentaires comme spécifié dans chaque règle.



Si le nœud de stockage sur lequel vous avez trouvé l'objet est hors ligne, vous pouvez le copier sur n'importe quel nœud de stockage en ligne. Placez l'objet dans un répertoire `/var/local/rangedb` du nœud de stockage en ligne. Ensuite, exécutez la `Object_Found` commande en utilisant ce chemin de fichier vers l'objet.

- Si l'objet ne peut pas être restauré, la `Object_Found` commande échoue. Contactez l'assistance technique.
- Si l'objet a été restauré avec succès dans StorageGRID, un message de réussite s'affiche. Par exemple :

```
ade 12448208: /proc/STOR > Object_Found
'/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'

ade 12448208: /proc/STOR > Object found succeeded.
First packet of file was valid. Extracted key: 38186FE53E3C49A5
Renamed '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6' to
'/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila#3udu'
```

Passez à l'étape suivante.

4. Si l'objet a été restauré dans StorageGRID, vérifiez que les nouveaux emplacements ont été créés :
  - a. Connectez-vous au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
  - b. Sélectionnez **ILM > Object metadata Lookup**.
  - c. Entrez l'UUID et sélectionnez **Rechercher**.
  - d. Examinez les métadonnées et vérifiez les nouveaux emplacements.
5. À partir d'un nœud d'administration, recherchez dans les journaux d'audit le message d'audit ORLM correspondant à cet objet pour vous assurer que la gestion du cycle de vie des informations (ILM) a placé des copies, si nécessaire.



a. Connectez-vous au nœud grid :

- i. Entrez la commande suivante : `ssh admin@grid_node_IP`
- ii. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
- iii. Entrez la commande suivante pour basculer en root : `su -`
- iv. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier. Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

b. Accédez au répertoire où se trouvent les journaux d'audit : `cd /var/local/log/`

c. Utilisez `grep` pour extraire les messages d'audit associés à l'objet dans un fichier de sortie. Entrer :  
`grep uuid-value audit_file_name > output_file_name`

Par exemple :

```
Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
messages_about_restored_object.txt
```

d. Utilisez `grep` pour extraire les messages d'audit règles objet met (ORLM) de ce fichier de sortie. Entrer :  
`grep ORLM output_file_name`

Par exemple :

```
Admin: # grep ORLM messages_about_restored_object.txt
```

Un message d'audit ORLM ressemble à cet exemple de message.

```
[AUDT:[CBID(UI64):0x38186FE53E3C49A5][RULE(CSTR):"Make 2 Copies"]
[STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"926026C4-00A4-449B-AC72-
BCCA72DD1311"]
[LOCS(CSTR):"**CLDI 12828634 2148730112**, CLDI 12745543 2147552014"]
[RSLT(FC32):SUCS][AVER(UI32):10][ATYP(FC32):ORLM][ATIM(UI64):15633982306
69]
[ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID(FC32):BCMS]]
```

a. Recherchez le champ `EMPLACEMENTS` dans le message d'audit.

Le cas échéant, la valeur de `CLDI` dans `LES EMBLEMENTS` est l'ID de nœud et l'ID de volume sur lequel une copie d'objet a été créée. Ce message indique que la ILM a été appliquée et que deux copies d'objet ont été créées à deux emplacements dans la grille.

6. **"Réinitialise le nombre d'objets perdus et manquants"** Dans le Gestionnaire de grille.

#### Réinitialiser le nombre d'objets perdus et manquants

Après avoir examiné le système StorageGRID et vérifié que tous les objets perdus enregistrés sont définitivement perdus ou qu'il s'agit d'une fausse alarme, vous pouvez

réinitialiser la valeur de l'attribut objets perdus sur zéro.

#### Avant de commencer

- Vous devez être connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".
- Vous avez "autorisations d'accès spécifiques".

#### Description de la tâche

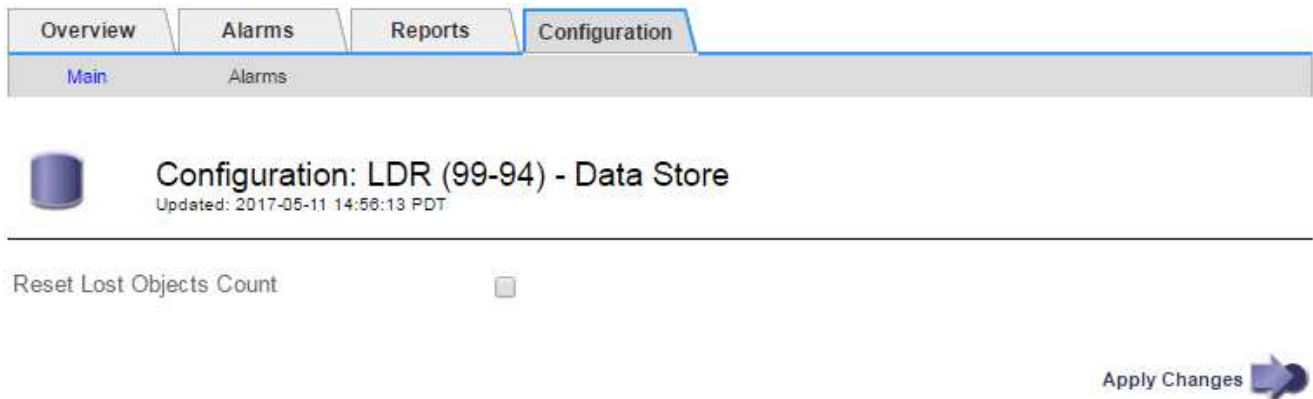
Vous pouvez réinitialiser le compteur objets perdus à partir de l'une des pages suivantes :

- **SUPPORT > Outils > topologie Grid > site > Storage Node > LDR > Data Store > Présentation > main**
- **SUPPORT > Outils > topologie Grid > site > Storage Node > DDS > Data Store > Présentation > main**

Ces instructions montrent la réinitialisation du compteur à partir de la page **LDR > Data Store**.

#### Étapes

1. Sélectionnez **SUPPORT > Outils > topologie de grille**.
2. Sélectionnez **site > Storage Node > LDR > Data Store > Configuration** pour le nœud de stockage qui a l'alerte **objets perdus** ou l'alarme PERDUE.
3. Sélectionnez **Réinitialiser le nombre d'objets perdus**.



4. Cliquez sur **appliquer les modifications**.

L'attribut objets perdus est réinitialisé à 0 et l'alerte **objets perdus** et l'effacement de l'alarme PERDUE, qui peut prendre quelques minutes.

5. Si vous le souhaitez, réinitialisez d'autres valeurs d'attribut associées qui auraient pu être incrémentées en cours d'identification de l'objet perdu.
  - a. Sélectionnez **site > Storage Node > LDR > codage d'effacement > Configuration**.
  - b. Sélectionnez **Réinitialiser les lectures nombre d'échecs** et **Réinitialiser les copies corrompues nombre d'échecs détectés**.
  - c. Cliquez sur **appliquer les modifications**.
  - d. Sélectionnez **site > Storage Node > LDR > Verification > Configuration**.
  - e. Sélectionnez **Réinitialiser le nombre d'objets manquants** et **Réinitialiser le nombre d'objets corrompus**.
  - f. Si vous êtes sûr que les objets mis en quarantaine ne sont pas requis, vous pouvez sélectionner **Supprimer les objets mis en quarantaine**.

Des objets mis en quarantaine sont créés lorsque la vérification en arrière-plan identifie une copie d'objet répliquée corrompue. Dans la plupart des cas, StorageGRID remplace automatiquement l'objet corrompu, et il est sûr de supprimer les objets mis en quarantaine. Cependant, si l'alerte **objets perdus** ou L'alarme PERDUE est déclenchée, le support technique peut vouloir accéder aux objets mis en quarantaine.

g. Cliquez sur **appliquer les modifications**.

La réinitialisation des attributs peut prendre quelques instants après avoir cliqué sur **appliquer les modifications**.

## Dépanner l'alerte de stockage de données d'objet faible

L'alerte **mémoire de données d'objet faible** surveille la quantité d'espace disponible pour le stockage de données d'objet sur chaque nœud de stockage.

### Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).

### Description de la tâche

L'alerte **Low Object Data Storage** est déclenchée lorsque la quantité totale de données d'objet répliquées et codées par effacement sur un nœud de stockage remplit l'une des conditions configurées dans la règle d'alerte.

Par défaut, une alerte majeure est déclenchée lorsque cette condition est évaluée comme vrai :

```
(storagegrid_storage_utilization_data_bytes/  
(storagegrid_storage_utilization_data_bytes +  
storagegrid_storage_utilization_usable_space_bytes)) >=0.90
```

Dans cette condition :

- `storagegrid_storage_utilization_data_bytes` Est une estimation de la taille totale des données d'objet répliquées et codées d'effacement pour un nœud de stockage.
- `storagegrid_storage_utilization_usable_space_bytes` Quantité totale d'espace de stockage objet restant pour un nœud de stockage.

Si une alerte majeure ou mineure **stockage de données d'objet bas** est déclenchée, vous devez exécuter une procédure d'extension dès que possible.

### Étapes

1. Sélectionnez **ALERTE** > **actuel**.

La page alertes s'affiche.

2. Dans le tableau des alertes, développez le groupe d'alertes **stockage de données d'objet bas**, si nécessaire, et sélectionnez l'alerte que vous souhaitez afficher.

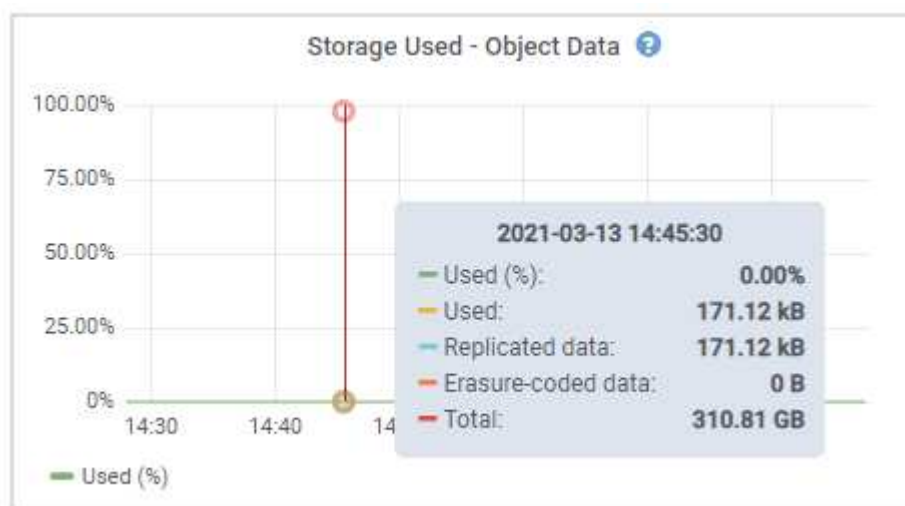


Sélectionnez l'alerte, et non l'en-tête d'un groupe d'alertes.

3. Vérifiez les détails dans la boîte de dialogue et notez ce qui suit :
  - Temps déclenché
  - Le nom du site et du noeud
  - Valeurs actuelles des mesures de cette alerte
4. Sélectionnez **NOEUDS > Storage Node ou site > Storage**.
5. Positionnez le curseur sur le graphique stockage utilisé - données d'objet.

Les valeurs suivantes sont affichées :

- **Utilisé (%)** : pourcentage de l'espace utilisable total qui a été utilisé pour les données d'objet.
- **Used** : quantité de l'espace utilisable total qui a été utilisé pour les données d'objet.
- **Données répliquées** : estimation de la quantité de données d'objet répliqué sur ce nœud, site ou grille.
- **Données avec code d'effacement** : estimation de la quantité de données d'objet avec code d'effacement sur ce nœud, ce site ou ce grid.
- **Total** : la quantité totale d'espace utilisable sur ce nœud, site ou grille. La valeur utilisée est la `storagegrid_storage_utilization_data_bytes` mesure.



6. Sélectionnez les commandes de temps au-dessus du graphique pour afficher l'utilisation du stockage sur différentes périodes.

Pour mieux comprendre la quantité de stockage utilisée auparavant et après le déclenchement de l'alerte, vous pouvez estimer le temps nécessaire pour que l'espace restant du nœud devienne complet.

7. Dès que possible, "[ajouter de la capacité de stockage](#)" à votre grille.

Vous pouvez ajouter des volumes de stockage (LUN) à des nœuds de stockage existants ou ajouter de nouveaux nœuds de stockage.



Pour plus d'informations, voir "[Gérer des nœuds de stockage complets](#)".

## Dépanner les alertes de remplacement de filigrane en lecture seule faible

Si vous utilisez des valeurs personnalisées pour les filigranes de volume de stockage, vous devrez peut-être résoudre l'alerte **dépassement de filigrane en lecture seule faible**. Si possible, vous devez mettre à jour votre système pour commencer à utiliser les valeurs optimisées.

Dans les versions précédentes, les trois "filigranes de volume de stockage" paramètres étaient globaux et la référence 8212 ; les mêmes valeurs étaient appliquées à chaque volume de stockage sur chaque nœud de stockage. À partir de StorageGRID 11.6, le logiciel peut optimiser ces filigranes pour chaque volume de stockage, en fonction de la taille du nœud de stockage et de la capacité relative du volume.

Lorsque vous effectuez une mise à niveau vers StorageGRID 11.6 ou une version ultérieure, des filigranes optimisés en lecture seule et en lecture-écriture sont automatiquement appliqués à tous les volumes de stockage, sauf si l'une des conditions suivantes est vraie :

- Votre système est proche de sa capacité et ne pourra pas accepter de nouvelles données si des filigranes optimisés ont été appliqués. Dans ce cas, StorageGRID ne modifie pas les paramètres du filigrane.
- Vous avez précédemment défini n'importe laquelle des filigranes du volume de stockage sur une valeur personnalisée. StorageGRID ne remplacera pas les paramètres de filigrane personnalisés avec des valeurs optimisées. Cependant, StorageGRID peut déclencher l'alerte **Low read-only filigrane override** si votre valeur personnalisée pour le filigrane soft read-only du volume de stockage est trop petite.

### Description de l'alerte

Si vous utilisez des valeurs personnalisées pour les filigranes du volume de stockage, l'alerte **valeur de remplacement du filigrane en lecture seule faible** peut être déclenchée pour un ou plusieurs nœuds de stockage.

Chaque instance de l'alerte indique que la valeur personnalisée du filigrane en lecture seule souple du volume de stockage est inférieure à la valeur minimale optimisée pour ce nœud de stockage. Si vous continuez à utiliser le paramètre personnalisé, le nœud de stockage risque d'être extrêmement faible sur l'espace avant qu'il ne puisse passer en mode lecture seule en toute sécurité. Certains volumes de stockage peuvent devenir inaccessibles (lorsqu'ils sont démontés automatiquement) lorsqu'ils atteignent la capacité.

Par exemple, supposons que vous avez défini précédemment le filigrane en lecture seule souple du volume de stockage sur 5 Go. Supposons maintenant que StorageGRID a calculé les valeurs optimisées suivantes pour les quatre volumes de stockage du nœud A :

Volume 0	12 GO
Volume 1	12 GO
Volume 2	11 GO
Volume 3	15 GO

L'alerte **dépassement de seuil en lecture seule faible** est déclenchée pour le nœud de stockage A car votre filigrane personnalisé (5 Go) est inférieur à la valeur minimale optimisée pour tous les volumes de ce nœud (11 Go). Si vous continuez à utiliser le paramètre personnalisé, le nœud risque d'avoir un espace insuffisant avant de passer en mode lecture seule en toute sécurité.

## Résolution de l'alerte

Suivez ces étapes si une ou plusieurs alertes **prioritaire de filigrane en lecture seule basse** ont été déclenchées. Vous pouvez également utiliser ces instructions si vous utilisez actuellement des paramètres de filigrane personnalisés et souhaitez commencer à utiliser des paramètres optimisés, même si aucune alerte n'a été déclenchée.

### Avant de commencer

- Vous avez terminé la mise à niveau vers StorageGRID 11.6 ou une version ultérieure.
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Autorisation d'accès racine"](#).

### Description de la tâche

Vous pouvez résoudre l'alerte **dépassement de filigrane en lecture seule** en mettant à jour les paramètres de filigrane personnalisés vers les nouveaux remplacements de filigrane. Toutefois, si un ou plusieurs nœuds de stockage sont proches de leur emplacement complet ou si vous avez des exigences ILM spécifiques, vous devez d'abord consulter les filigranes de stockage optimisés et déterminer s'il est sûr de les utiliser.

## Évaluer l'utilisation des données d'objet pour l'ensemble de la grille

### Étapes

1. Sélectionnez **NOEUDS**.
2. Pour chaque site de la grille, développez la liste des nœuds.
3. Examinez les valeurs de pourcentage affichées dans la colonne **données objet utilisées** pour chaque nœud de stockage de chaque site.

# Nodes

View the list and status of sites and grid nodes.

Search... Total node count: 13

Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID	Grid	61%	4%	—
▲ Data Center 1	Site	56%	3%	—
DC1-ADM	Primary Admin Node	—	—	6%
DC1-GW	Gateway Node	—	—	1%
! DC1-SN1	Storage Node	71%	3%	30%
! DC1-SN2	Storage Node	25%	3%	42%
! DC1-SN3	Storage Node	63%	3%	42%
! DC1-SN4	Storage Node	65%	3%	41%

4. Suivez l'étape appropriée :

- Si aucun des nœuds de stockage n'est presque plein (par exemple, toutes les valeurs **données objet utilisées** sont inférieures à 80 %), vous pouvez commencer à utiliser les paramètres de remplacement. Allez à [Utilisez des filigranes optimisés](#).
- Si les règles ILM utilisent un comportement d'ingestion strict ou si des pools de stockage spécifiques sont proches de leur saturation, effectuez les étapes décrites dans [Afficher des filigranes de stockage optimisés](#) et [Déterminez si vous pouvez utiliser des filigranes optimisés](#).

### Afficher les filigranes de stockage optimisés

StorageGRID utilise deux metrics Prometheus pour afficher les valeurs optimisées qu'il a calculées pour le seuil en lecture seule souple du volume de stockage. Vous pouvez afficher les valeurs minimale et maximale optimisées pour chaque nœud de stockage de la grille.

#### Étapes

- Sélectionnez **SUPPORT > Outils > métriques**.
- Dans la section Prometheus, sélectionnez le lien permettant d'accéder à l'interface utilisateur Prometheus.
- Pour afficher le filigrane minimum en lecture seule programmable recommandé, entrez la mesure Prometheus suivante et sélectionnez **Exécute** :

```
storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
```

La dernière colonne affiche la valeur minimale optimisée du filigrane en lecture seule pour tous les

volumes de stockage de chaque nœud de stockage. Si cette valeur est supérieure au paramètre personnalisé du filigrane en lecture seule du volume de stockage, l'alerte **Low read-only filigrane override** est déclenchée pour le nœud de stockage.

4. Pour afficher le filigrane maximal en lecture seule programmable recommandé, entrez la mesure Prometheus suivante et sélectionnez **Execute** :

```
storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
```

La dernière colonne affiche la valeur maximale optimisée du filigrane en lecture seule pour tous les volumes de stockage de chaque nœud de stockage.

5. Notez la valeur maximale optimisée pour chaque nœud de stockage.

### Déterminez si vous pouvez utiliser des filigranes optimisés

#### Étapes

1. Sélectionnez **NOEUDS**.
2. Répétez la procédure suivante pour chaque nœud de stockage en ligne :
  - a. Sélectionnez **Storage Node > Storage**.
  - b. Faites défiler jusqu'au tableau magasins d'objets.
  - c. Comparez la valeur **disponible** pour chaque magasin d'objets (volume) au filigrane optimisé maximum que vous avez indiqué pour ce nœud de stockage.
3. Si au moins un volume sur chaque nœud de stockage en ligne dispose de plus d'espace disponible que le filigrane maximum optimisé pour ce nœud, reportez-vous à la section [Utilisez des filigranes optimisés](#) pour commencer à utiliser les filigranes optimisés.

Sinon, développez la grille dès que possible. ["ajout de volumes de stockage"](#) Vers un nœud existant ou ["Ajout de nœuds de stockage"](#). Ensuite, accédez à [Utilisez des filigranes optimisés](#) pour mettre à jour les paramètres du filigrane.

4. Si vous devez continuer à utiliser des valeurs personnalisées pour les filigranes du volume de stockage ["silence"](#) ou ["désactiver"](#) l'alerte **Low read-only filigrane override**.



Les mêmes valeurs de filigrane personnalisées sont appliquées à chaque volume de stockage sur chaque nœud de stockage. L'utilisation de valeurs inférieures aux valeurs recommandées pour les filigranes du volume de stockage peut rendre certains volumes de stockage inaccessibles (démontés automatiquement) lorsque le nœud atteint sa capacité.

### utiliser des filigranes optimisés

#### Étapes

1. Accédez à **SUPPORT > autre > filigranes de stockage**.
2. Cochez la case **utiliser les valeurs optimisées**.
3. Sélectionnez **Enregistrer**.

Les paramètres de filigrane du volume de stockage optimisé sont désormais en vigueur pour chaque volume de stockage, en fonction de la taille du nœud de stockage et de la capacité relative du volume.



## Diagnostiquez les problèmes liés aux métadonnées

En cas de problèmes liés aux métadonnées, des alertes vous informeront de la source des problèmes et des mesures recommandées à prendre. En particulier, vous devez ajouter de nouveaux nœuds de stockage si l'alerte de faible stockage des métadonnées est déclenchée.

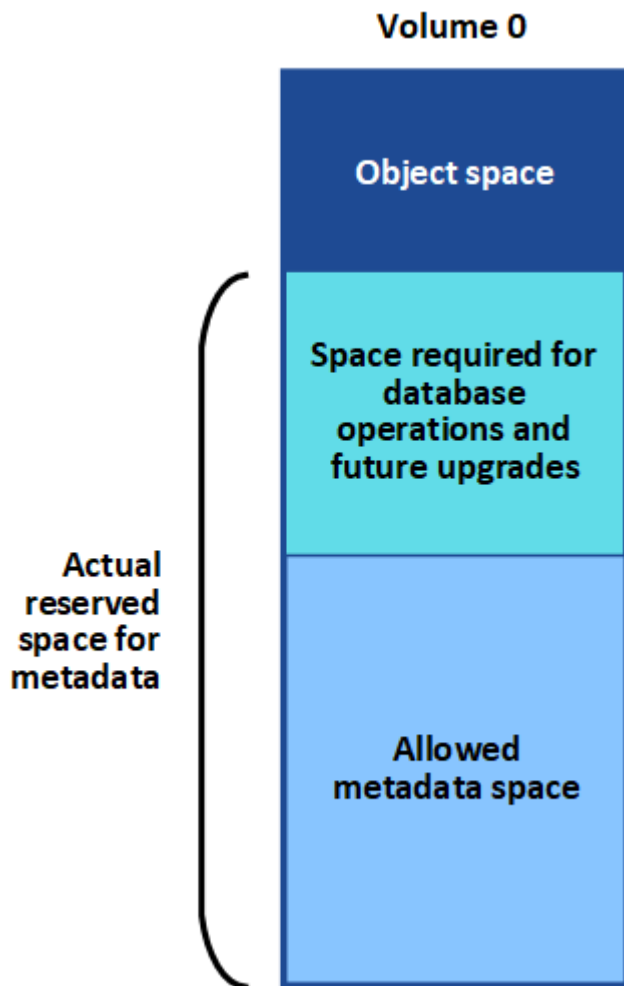
### Avant de commencer

Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).

### Description de la tâche

Suivez les actions recommandées pour chaque alerte liée aux métadonnées qui est déclenchée. Si l'alerte **stockage de métadonnées faible** est déclenchée, vous devez ajouter de nouveaux nœuds de stockage.

StorageGRID réserve un certain espace sur le volume 0 de chaque nœud de stockage pour les métadonnées de l'objet. Cet espace, appelé *espace réservé réel*, est subdivisé en l'espace autorisé pour les métadonnées de l'objet (espace de métadonnées autorisé) et l'espace requis pour les opérations de base de données essentielles, telles que la compaction et la réparation. L'espace de métadonnées autorisé régit la capacité globale des objets.



Si les métadonnées d'objet consomment plus de 100 % de l'espace autorisé pour les métadonnées, les opérations de base de données ne peuvent pas s'exécuter efficacement et des erreurs se produisent.

Vous pouvez "[Surveillez la capacité des métadonnées d'objet pour chaque nœud de stockage](#)" vous aider à anticiper les erreurs et à les corriger avant qu'elles ne se produisent.

StorageGRID utilise la métrique Prometheus suivante pour mesurer la totalité de l'espace de métadonnées autorisé :

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utilization_metadata_allowed_bytes
```

Lorsque cette expression Prometheus atteint certains seuils, l'alerte **stockage de métadonnées faible** est déclenchée.

- **Mineure** : les métadonnées d'objet utilisent au moins 70 % de l'espace autorisé pour les métadonnées. Vous devez ajouter des nœuds de stockage dès que possible.
- **Majeur** : les métadonnées d'objet utilisent au moins 90 % de l'espace autorisé pour les métadonnées. Vous devez immédiatement ajouter de nouveaux nœuds de stockage.



Lorsque les métadonnées d'objet utilisent au moins 90 % de l'espace de métadonnées autorisé, un avertissement s'affiche sur le tableau de bord. Si cet avertissement s'affiche, vous devez immédiatement ajouter de nouveaux nœuds de stockage. Vous ne devez jamais autoriser les métadonnées objet à utiliser plus de 100 % de l'espace autorisé.

- **Critique** : les métadonnées d'objet utilisent au moins 100 % de l'espace de métadonnées autorisé et commencent à consommer l'espace requis pour les opérations essentielles de la base de données. Vous devez arrêter l'ingestion des nouveaux objets et vous devez immédiatement ajouter de nouveaux nœuds de stockage.



Si la taille du volume 0 est inférieure à celle de l'option de stockage de l'espace réservé aux métadonnées (par exemple, dans un environnement non productif), le calcul de l'alerte **stockage de métadonnées faible** peut être inexact.

## Étapes

1. Sélectionnez **ALERTES > actuel**.
2. Dans le tableau des alertes, développez le groupe d'alertes **stockage de métadonnées faible**, si nécessaire, et sélectionnez l'alerte spécifique que vous souhaitez afficher.
3. Vérifiez les détails dans la boîte de dialogue d'alerte.
4. Si une alerte majeure ou critique **stockage de métadonnées faible** a été déclenchée, effectuez immédiatement une extension pour ajouter des nœuds de stockage.



Dans la mesure où StorageGRID conserve des copies complètes de toutes les métadonnées d'objet sur chaque site, la capacité de métadonnées de l'ensemble de la grille est limitée par la capacité des métadonnées du site le plus petit. Si vous devez ajouter de la capacité de métadonnées à un site, vous devez également "[développez n'importe quel autre site](#)" utiliser le même nombre de nœuds de stockage.

Une fois l'extension effectuée, StorageGRID redistribue les métadonnées de l'objet existantes vers les nouveaux nœuds, qui augmentent la capacité globale des métadonnées de la grille. Aucune action de l'utilisateur n'est requise. L'alerte **stockage de métadonnées faible** est effacée.

## Résoudre les erreurs de certificat

Si vous rencontrez un problème de sécurité ou de certificat lorsque vous tentez de vous connecter à StorageGRID à l'aide d'un navigateur Web, d'un client S3 ou d'un outil de surveillance externe, vous devez vérifier le certificat.

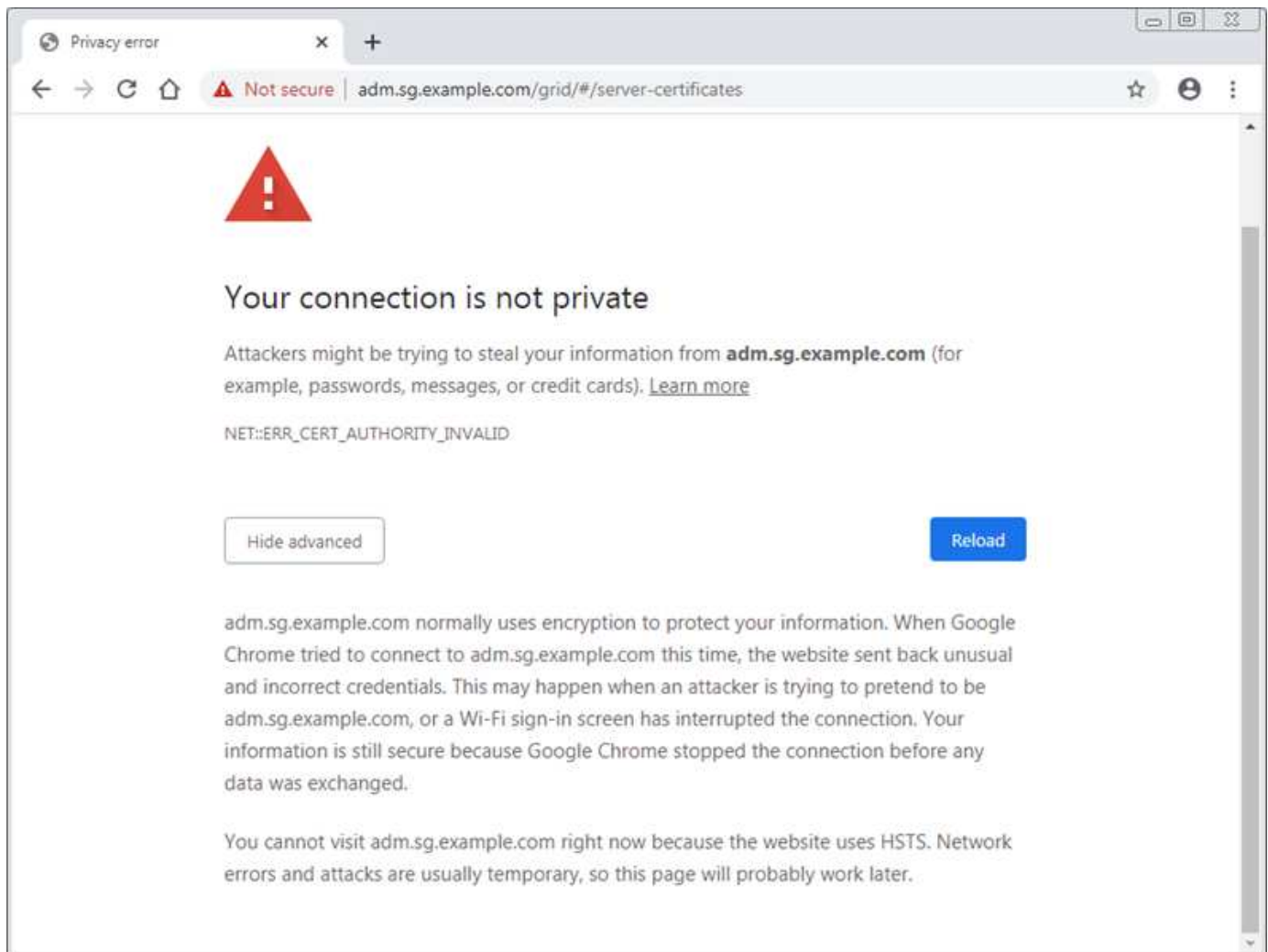
### Description de la tâche

Les erreurs de certificat peuvent entraîner des problèmes lors de votre tentative de connexion à StorageGRID à l'aide de Grid Manager, de l'API de gestion du grid, du gestionnaire de locataires ou de l'API de gestion des locataires. Des erreurs de certificat peuvent également se produire lorsque vous tentez de vous connecter à un client S3 ou à un outil de surveillance externe.

Si vous accédez à Grid Manager ou au Gestionnaire de locataires à l'aide d'un nom de domaine au lieu d'une adresse IP, le navigateur affiche une erreur de certificat sans option de contournement si l'un des cas suivants se produit :

- Votre certificat d'interface de gestion personnalisée expire.
- Vous restaurez un certificat d'interface de gestion personnalisée vers le certificat de serveur par défaut.

L'exemple suivant montre une erreur de certificat lorsque le certificat de l'interface de gestion personnalisée a expiré :



Pour garantir que les opérations ne sont pas interrompues par un certificat de serveur défaillant, l'alerte **expiration du certificat de serveur pour l'interface de gestion** est déclenchée lorsque le certificat de serveur est sur le point d'expirer.

Lorsque vous utilisez des certificats client pour l'intégration avec Prometheus externe, les erreurs de certificat peuvent être dues au certificat de l'interface de gestion StorageGRID ou aux certificats client. L'alerte **expiration des certificats client configurés sur la page certificats** est déclenchée lorsqu'un certificat client arrive à expiration.

## Étapes

Si vous avez reçu une notification d'alerte concernant un certificat expiré, accédez aux détails du certificat : . Sélectionnez **CONFIGURATION > sécurité > certificats**, puis "[sélectionnez l'onglet certificat approprié](#)".

1. Vérifiez la période de validité du certificat. + certains navigateurs Web et clients S3 n'acceptent pas les certificats dont la période de validité est supérieure à 398 jours.
2. Si le certificat a expiré ou expire bientôt, téléchargez ou générez un nouveau certificat.
  - Pour un certificat de serveur, reportez-vous aux étapes de "[Configuration d'un certificat de serveur personnalisé pour le Grid Manager et le tenant Manager](#)".
  - Pour un certificat client, reportez-vous aux étapes de "[configuration d'un certificat client](#)".
3. Pour les erreurs de certificat de serveur, essayez l'une des options suivantes ou les deux :
  - Assurez-vous que le nom d'alternative de l'objet (SAN) du certificat est renseigné et que le SAN correspond à l'adresse IP ou au nom d'hôte du nœud auquel vous vous connectez.
  - Si vous tentez de vous connecter à StorageGRID à l'aide d'un nom de domaine :
    - i. Entrez l'adresse IP du nœud d'administration au lieu du nom de domaine pour contourner l'erreur de connexion et accéder à Grid Manager.
    - ii. Dans le Gestionnaire de grille, sélectionnez **CONFIGURATION > sécurité > certificats**, puis "[sélectionnez l'onglet certificat approprié](#)" pour installer un nouveau certificat personnalisé ou continuer avec le certificat par défaut.
    - iii. Dans les instructions d'administration de StorageGRID, reportez-vous aux étapes de "[Configuration d'un certificat de serveur personnalisé pour le Grid Manager et le tenant Manager](#)".

## Résolution des problèmes liés au nœud d'administration et à l'interface utilisateur

Vous pouvez effectuer plusieurs tâches pour déterminer la source des problèmes liés aux nœuds d'administration et à l'interface utilisateur de StorageGRID.

### Erreurs de connexion au nœud d'administration

Si vous rencontrez une erreur lorsque vous vous connectez à un nœud d'administration StorageGRID, votre système peut avoir un problème avec ou, un "[la mise en réseau](#)" problème avec ou "[matériel](#)" "[Services de nœuds d'administration](#)" "[Problème avec la base de données Cassandra](#)" sur les nœuds de stockage connectés.

### Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur web pris en charge](#)".
- Vous avez le `Passwords.txt` fichier.
- Vous avez "[autorisations d'accès spécifiques](#)".

## Description de la tâche

Suivez ces instructions de dépannage si vous voyez l'un des messages d'erreur suivants lorsque vous tentez de vous connecter à un nœud d'administration :

- Your credentials for this account were invalid. Please try again.
- Waiting for services to start...
- Internal server error. The server encountered an error and could not complete your request. Please try again. If the problem persists, contact Technical Support.
- Unable to communicate with server. Reloading page..

## Étapes

1. Attendez 10 minutes et essayez à nouveau de vous connecter.

Si l'erreur n'est pas résolue automatiquement, passez à l'étape suivante.

2. Si votre système StorageGRID comporte plusieurs nœuds d'administration, essayez de vous connecter au Gestionnaire de grille à partir d'un autre nœud d'administration pour vérifier l'état d'un nœud d'administration non disponible.
  - Si vous pouvez vous connecter, vous pouvez utiliser les options **Dashboard**, **NODES**, **Alerts** et **SUPPORT** pour déterminer la cause de l'erreur.
  - Si vous n'avez qu'un seul nœud d'administration ou si vous ne pouvez toujours pas vous connecter, passez à l'étape suivante.
3. Déterminez si le matériel du nœud est hors ligne.
4. Si l'authentification unique (SSO) est activée pour votre système StorageGRID, reportez-vous aux étapes pour "[configuration de l'authentification unique](#)".

Pour résoudre ces problèmes, il peut être nécessaire de désactiver et de réactiver temporairement l'authentification SSO pour un nœud d'administration unique.



Si SSO est activé, vous ne pouvez pas vous connecter à l'aide d'un port restreint. Vous devez utiliser le port 443.

5. Déterminez si le compte que vous utilisez appartient à un utilisateur fédéré.

Si le compte d'utilisateur fédéré ne fonctionne pas, essayez de vous connecter à Grid Manager en tant qu'utilisateur local, tel que root.

- Si l'utilisateur local peut se connecter :
  - i. Consultez les alertes.
  - ii. Sélectionnez **CONFIGURATION** > **contrôle d'accès** > **fédération d'identités**.
  - iii. Cliquez sur **Tester la connexion** pour valider vos paramètres de connexion pour le serveur LDAP.
  - iv. Si le test échoue, corrigez toute erreur de configuration.
- Si l'utilisateur local ne peut pas se connecter et que vous êtes sûr que les informations d'identification sont correctes, passez à l'étape suivante.

6. Utilisez SSH (Secure Shell) pour vous connecter au nœud d'administration :

- a. Entrez la commande suivante : `ssh admin@Admin_Node_IP`

- b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
- c. Entrez la commande suivante pour basculer en root : `su -`
- d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

7. Afficher l'état de tous les services exécutés sur le nœud de grille : `storagegrid-status`

Assurez-vous que les services nms, mi, nginx et api de gestion sont tous en cours d'exécution.

La sortie est immédiatement mise à jour si l'état d'un service change.

```
$ storagegrid-status
Host Name                99-211
IP Address               10.96.99.211
Operating System Kernel  4.19.0                 Verified
Operating System Environment Debian 10.1             Verified
StorageGRID Webscale Release 11.4.0                 Verified
Networking                Verified
Storage Subsystem        Verified
Database Engine          5.5.9999+default      Running
Network Monitoring       11.4.0                 Running
Time Synchronization     1:4.2.8p10+dfsg      Running
ams                      11.4.0                 Running
cmn                      11.4.0                 Running
nms                      11.4.0                 Running
ssm                      11.4.0                 Running
mi                      11.4.0                 Running
dynip                   11.4.0                 Running
nginx                   1.10.3                 Running
tomcat                  9.0.27                 Running
grafana                 6.4.3                 Running
mgmt api                11.4.0                 Running
prometheus              11.4.0                 Running
persistence             11.4.0                 Running
ade exporter            11.4.0                 Running
alertmanager            11.4.0                 Running
attrDownPurge           11.4.0                 Running
attrDownSamp1           11.4.0                 Running
attrDownSamp2           11.4.0                 Running
node exporter           0.17.0+ds              Running
sg snmp agent           11.4.0                 Running
```

8. Vérifiez que le service nginx-gw est en cours d'exécution # `service nginx-gw status`
9. utilisez Lumberjack pour collecter les journaux : # `/usr/local/sbin/lumberjack.rb`

Si l'authentification a échoué par le passé, vous pouvez utiliser les options de script `--start` et `--end` Lumberjack pour spécifier la plage horaire appropriée. Utilisez `lumberjack -h` pour plus de détails sur ces options.

La sortie vers le terminal indique l'emplacement où l'archive de journal a été copiée.

10. consultez les journaux suivants :

- `/var/local/log/bycast.log`
- `/var/local/log/bycast-err.log`
- `/var/local/log/nms.log`
- `**/*commands.txt`

11. Si vous n'avez pas pu identifier de problèmes avec le nœud d'administration, exécutez l'une ou l'autre des commandes suivantes pour déterminer les adresses IP des trois nœuds de stockage exécutant le service ADC sur votre site. Il s'agit généralement des trois premiers nœuds de stockage installés sur le site.

```
# cat /etc/hosts
```

```
# gpt-list-services adc
```

Les nœuds Admin utilisent le service ADC pendant le processus d'authentification.

12. À partir du nœud d'administration, utilisez `ssh` pour vous connecter à chacun des nœuds de stockage ADC, en utilisant les adresses IP que vous avez identifiées.

13. Afficher l'état de tous les services exécutés sur le nœud de grille : `storagegrid-status`

Assurez-vous que tous les services `idnt`, `acct`, `nginx` et `cassandra` fonctionnent.

14. Répétez les étapes [Utilisez Lumberjack pour récupérer les journaux](#) et [Journaux de révision](#) pour consulter les journaux sur les nœuds de stockage.

15. Si vous ne parvenez pas à résoudre le problème, contactez le support technique.

Fournissez les journaux que vous avez collectés au support technique. Voir aussi "[Référence des fichiers journaux](#)".

## Problèmes liés à l'interface utilisateur

L'interface utilisateur du Gestionnaire de grille ou du Gestionnaire de locataires peut ne pas répondre comme prévu après la mise à niveau du logiciel StorageGRID.

### Étapes

1. Assurez-vous que vous utilisez un "[navigateur web pris en charge](#)".
2. Effacez le cache de votre navigateur Web.

L'effacement du cache supprime les ressources obsolètes utilisées par la version précédente du logiciel StorageGRID et permet à l'interface utilisateur de fonctionner de nouveau correctement. Pour obtenir des instructions, reportez-vous à la documentation de votre navigateur Web.

## Résolution des problèmes de réseau, de matériel et de plateforme

Vous pouvez effectuer plusieurs tâches pour déterminer la source des problèmes liés au réseau, au matériel et à la plateforme StorageGRID.

### Erreurs « 422 : entité non traitable »

L'erreur 422 : entité détraitable peut se produire pour différentes raisons. Consultez le message d'erreur pour déterminer la cause de votre problème.

Si l'un des messages d'erreur répertoriés s'affiche, effectuez l'action recommandée.

Message d'erreur	Cause première et action corrective
<pre>422: Unprocessable Entity  Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration. Unable to authenticate, please verify your username and password: LDAP Result Code 8 "Strong Auth Required": 00002028: LdapErr: DSID-0C090256, comment: The server requires binds to turn on integrity checking if SSL\TLS are not already active on the connection, data 0, v3839</pre>	<p>Ce message peut se produire si vous sélectionnez l'option <b>ne pas utiliser TLS</b> pour transport Layer Security (TLS) lors de la configuration de la fédération d'identités à l'aide de Windows Active Directory (AD).</p> <p>L'utilisation de l'option <b>ne pas utiliser TLS</b> n'est pas prise en charge pour les serveurs AD qui appliquent la signature LDAP. Vous devez sélectionner l'option <b>Use STARTTLS</b> ou l'option <b>use LDAPS</b> pour TLS.</p>



Message d'erreur	Cause première et action corrective
<pre>422: Unprocessable Entity  Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration.Unable to begin TLS, verify your certificate and TLS configuration: LDAP Result Code 200 "Network Error": TLS handshake failed (EOF)</pre>	<p>Ce message s'affiche si vous essayez d'utiliser un chiffrement non pris en charge pour établir une connexion TLS (transport Layer Security) entre StorageGRID et un système externe utilisé pour identifier la fédération ou les pools de stockage dans le cloud.</p> <p>Vérifiez les chiffrements proposés par le système externe. Le système doit utiliser l'un des <a href="#">"Chiffrements pris en charge par StorageGRID"</a> pour les connexions TLS sortantes, comme indiqué dans les instructions d'administration de StorageGRID.</p>

### alerte de non-concordance MTU du réseau de la grille

L'alerte **Grid Network MTU mismatch** est déclenchée lorsque le paramètre MTU (maximum transmission Unit) de l'interface réseau Grid (eth0) diffère considérablement sur les nœuds de la grille.

#### Description de la tâche

Les différences dans les paramètres MTU peuvent indiquer que certains réseaux eth0, mais pas tous, sont configurés pour les trames jumbo. Une différence de taille de MTU supérieure à 1000 peut entraîner des problèmes de performances du réseau.

#### Étapes

- Répertorie les paramètres MTU pour eth0 sur tous les nœuds.
  - Utilisez la requête fournie dans Grid Manager.
  - Accédez à `primary Admin Node IP address/metrics/graph` et entrez la requête suivante : `node_network_mtu_bytes{device="eth0"}`
- "Modifiez les paramètres MTU"** Si nécessaire, pour s'assurer qu'ils sont identiques pour l'interface réseau Grid (eth0) sur tous les nœuds.
  - Pour les nœuds basés sur Linux et VMware, utilisez la commande suivante : `/usr/sbin/change-ip.py [-h] [-n node] mtu network [network...]`

**Exemple** : `change-ip.py -n node 1500 grid admin`

**Remarque** : sur les nœuds Linux, si la valeur MTU souhaitée pour le réseau dans le conteneur dépasse la valeur déjà configurée sur l'interface hôte, vous devez d'abord configurer l'interface hôte pour qu'elle ait la valeur MTU souhaitée, puis utiliser le `change-ip.py` script pour modifier la valeur MTU du réseau dans le conteneur.

Utilisez les arguments suivants pour modifier la MTU sur les nœuds Linux ou VMware.

Arguments de position	Description
mtu	La MTU à définir. Doit être compris entre 1280 et 9216.
network	Réseaux auxquels appliquer la MTU. Incluez un ou plusieurs des types de réseau suivants : <ul style="list-style-type: none"> <li>• grille</li> <li>• admin</li> <li>• client</li> </ul>

+

Arguments facultatifs	Description
-h, - help	Afficher le message d'aide et quitter.
-n node, --node node	Le nœud. La valeur par défaut est le nœud local.

### Alerte d'erreur de trame de réception réseau de nœud

**Erreur de trame de réception réseau de nœud** les alertes peuvent être causées par des problèmes de connectivité entre StorageGRID et votre matériel réseau. Cette alerte disparaît toute seule une fois le problème sous-jacent résolu.

#### Description de la tâche

**Erreur de trame de réception réseau de nœud** les alertes peuvent être causées par les problèmes suivants avec le matériel réseau qui se connecte à StorageGRID :

- La correction d'erreur de marche avant (FEC) est requise et n'est pas utilisée
- Le port du commutateur et la MTU de la carte réseau ne correspondent pas
- Taux d'erreur de liaison élevés
- Dépassement de la mémoire tampon de la sonnerie NIC

#### Étapes

1. Suivez les étapes de dépannage pour toutes les causes potentielles de cette alerte en fonction de la configuration de votre réseau.
2. Effectuez les étapes suivantes en fonction de la cause de l'erreur :

## Non-concordance FEC



Ces étapes s'appliquent uniquement aux alertes **erreur de trame de réception réseau de nœud** causées par une incompatibilité FEC sur les appareils StorageGRID.

- a. Vérifiez l'état FEC du port du commutateur connecté à votre appliance StorageGRID.
- b. Vérifiez l'intégrité physique des câbles entre l'appareil et le commutateur.
- c. Si vous souhaitez modifier les paramètres FEC pour essayer de résoudre l'alerte, assurez-vous d'abord que l'appareil est configuré pour le mode **Auto** sur la page Configuration de la liaison du programme d'installation de l'appareil StorageGRID (reportez-vous aux instructions relatives à votre appareil :
  - "SG6160"
  - "SGF6112"
  - "SG6000"
  - "SG5800"
  - "SG5700"
  - "SG110 et SG1100"
  - "SG100 et SG1000"
- d. Modifiez les paramètres FEC sur les ports du commutateur. Si possible, les ports de l'appliance StorageGRID ajustent leurs paramètres FEC.

Vous ne pouvez pas configurer les paramètres FEC sur les appliances StorageGRID. Au lieu de cela, les appareils tentent de détecter et de mettre en miroir les paramètres FEC sur les ports de commutateur auxquels ils sont connectés. Si les liaisons sont forcées à des vitesses de réseau 25 GbE ou 100 GbE, le commutateur et la carte réseau peuvent ne pas négocier un paramètre FEC commun. Sans paramètre FEC commun, le réseau revient en mode « no-FEC ». Lorsque le mode FEC n'est pas activé, les connexions sont plus susceptibles d'erreurs causées par le bruit électrique.



Les appareils StorageGRID prennent en charge les FEC Firecode (FC) et Reed Solomon (RS), ainsi qu'aucun FEC.

### Le port du commutateur et la MTU de la carte réseau ne correspondent pas

Si l'alerte est causée par une incompatibilité de port de commutateur et de MTU de carte réseau, vérifiez que la taille MTU configurée sur le nœud est identique au paramètre MTU du port de commutateur.

La taille de MTU configurée sur le nœud peut être inférieure à celle définie sur le port de commutateur auquel le nœud est connecté. Si un nœud StorageGRID reçoit une trame Ethernet supérieure à sa MTU, ce qui est possible avec cette configuration, l'alerte **erreur de trame de réception réseau de nœud** peut être signalée. Si vous pensez que c'est ce qui se passe, modifiez la MTU du port du switch pour qu'il corresponde à la MTU de l'interface réseau StorageGRID, ou modifiez la MTU de l'interface réseau StorageGRID pour qu'elle corresponde au port du switch, en fonction de vos objectifs ou de vos exigences MTU de bout en bout.



Pour des performances réseau optimales, tous les nœuds doivent être configurés avec des valeurs MTU similaires sur leurs interfaces réseau Grid. L'alerte **Grid Network MTU mismatch** est déclenchée en cas de différence importante dans les paramètres MTU pour le réseau Grid sur les nœuds individuels. Les valeurs MTU ne doivent pas nécessairement être identiques pour tous les types de réseau. Voir [Dépanner l'alerte de non-concordance de MTU du réseau Grid](#) pour plus d'informations.



Voir aussi "[Modifier le paramètre MTU](#)".

#### Taux d'erreur de liaison élevés

- a. Activez FEC, si ce n'est déjà fait.
- b. Vérifiez que le câblage réseau est de bonne qualité et qu'il n'est pas endommagé ou mal connecté.
- c. Si les câbles ne semblent pas être à l'origine du problème, contactez le support technique.



Vous remarquerez peut-être des taux d'erreur élevés dans un environnement présentant un bruit électrique élevé.

#### Dépassement de la mémoire tampon de la sonnerie NIC

Si l'erreur est un dépassement de la mémoire tampon de la sonnerie de la carte réseau, contactez le support technique.

La mémoire tampon annulaire peut être surchargée lorsque le système StorageGRID est surchargé et ne peut pas traiter les événements réseau en temps opportun.

3. Surveillez le problème et contactez le support technique si l'alerte ne résout pas le problème.

### Erreurs de synchronisation de l'heure

Des problèmes de synchronisation de l'heure peuvent s'afficher dans votre grille.

Si vous rencontrez des problèmes de synchronisation du temps, vérifiez que vous avez spécifié au moins quatre sources NTP externes, chacune fournissant une référence Stratum 3 ou supérieure, et que toutes les sources NTP externes fonctionnent normalement et sont accessibles par vos nœuds StorageGRID.



Lorsqu'"[Spécification de la source NTP externe](#)" il s'agit d'une installation StorageGRID de niveau production, n'utilisez pas le service Windows Time (W32Time) sur une version de Windows antérieure à Windows Server 2016. Le service de temps des versions antérieures de Windows n'est pas suffisamment précis et n'est pas pris en charge par Microsoft pour une utilisation dans des environnements à haute précision, tels que StorageGRID.

### Linux : problèmes de connectivité réseau

Des problèmes de connectivité réseau peuvent survenir pour les nœuds StorageGRID hébergés sur des hôtes Linux.

#### Clonage d'adresses MAC

Dans certains cas, les problèmes de réseau peuvent être résolus en utilisant le clonage d'adresses MAC. Si vous utilisez des hôtes virtuels, définissez la valeur de la clé de clonage d'adresse MAC de chacun de vos

réseaux sur « true » dans le fichier de configuration de nœud. Ce paramètre entraîne l'utilisation de l'adresse MAC du conteneur StorageGRID de l'hôte. Pour créer des fichiers de configuration de nœud, reportez-vous aux instructions de ["Red Hat Enterprise Linux"](#) ou ["Ubuntu ou Debian"](#).



Créez des interfaces réseau virtuelles distinctes pour le système d'exploitation hôte Linux. L'utilisation des mêmes interfaces réseau pour le système d'exploitation hôte Linux et le conteneur StorageGRID peut rendre le système d'exploitation hôte inaccessible si le mode promiscuous n'a pas été activé sur l'hyperviseur.

Pour plus d'informations sur l'activation du clonage MAC, reportez-vous aux instructions de ["Red Hat Enterprise Linux"](#) ou ["Ubuntu ou Debian"](#).

### Mode promiscueux

Si vous ne souhaitez pas utiliser le clonage d'adresses MAC et que vous préférez autoriser toutes les interfaces à recevoir et transmettre des données pour les adresses MAC autres que celles attribuées par l'hyperviseur, assurez-vous que les propriétés de sécurité au niveau du commutateur virtuel et du groupe de ports sont définies sur **Accept** pour le mode promiscuous, les modifications d'adresse MAC et les transmissions forgées. Les valeurs définies sur le commutateur virtuel peuvent être remplacées par les valeurs au niveau du groupe de ports, de sorte que les paramètres soient les mêmes aux deux endroits.

Pour plus d'informations sur l'utilisation du mode promiscuous, reportez-vous aux instructions de ["Red Hat Enterprise Linux"](#) ou ["Ubuntu ou Debian"](#).

### Linux : l'état du nœud est « orphelin »

Un nœud Linux à l'état orphelin indique généralement que le service StorageGRID ou le démon du nœud StorageGRID contrôlant le conteneur du nœud est décédé de façon inattendue.

#### Description de la tâche

Si un nœud Linux signale qu'il est dans un état orphelin, vous devez :

- Vérifiez les journaux à la recherche d'erreurs et de messages.
- Tentative de démarrage du nœud.
- Si nécessaire, utiliser des commandes moteur de conteneur pour arrêter le conteneur de nœuds existant.
- Redémarrez le nœud.

#### Étapes

1. Vérifiez les journaux du démon du service et du nœud orphelin pour voir si des erreurs évidentes et des messages relatifs à la fermeture inopinée.
2. Connectez-vous à l'hôte en tant que root ou en utilisant un compte avec l'autorisation sudo.
3. Essayez de redémarrer le nœud en exécutant la commande suivante : `$ sudo storagegrid node start node-name`

```
$ sudo storagegrid node start DC1-S1-172-16-1-172
```

Si le nœud est orphelin, la réponse est

```
Not starting ORPHANED node DC1-S1-172-16-1-172
```

4. Depuis Linux, arrêtez le moteur de conteneur et tous les processus de nœud StorageGRID qui contrôlent. Par exemple :`sudo docker stop --time secondscontainer-name`

Pour `seconds`, entrez le nombre de secondes que vous souhaitez attendre pour que le conteneur s'arrête (généralement 15 minutes ou moins). Par exemple :

```
sudo docker stop --time 900 storagegrid-DC1-S1-172-16-1-172
```

5. Redémarrez le nœud : `storagegrid node start node-name`

```
storagegrid node start DC1-S1-172-16-1-172
```

## Linux : dépannage de la prise en charge IPv6

Vous devrez peut-être activer la prise en charge IPv6 dans le noyau si vous avez installé des nœuds StorageGRID sur des hôtes Linux et que vous remarquez que les adresses IPv6 n'ont pas été attribuées aux conteneurs de nœuds comme prévu.

### Description de la tâche

Pour afficher l'adresse IPv6 qui a été attribuée à un nœud de grille :

1. Sélectionnez **NODES** et sélectionnez le nœud.
2. Sélectionnez **Afficher les adresses IP supplémentaires** en regard de **adresses IP** dans l'onglet vue d'ensemble.

Si l'adresse IPv6 n'est pas affichée et que le nœud est installé sur un hôte Linux, procédez comme suit pour activer la prise en charge IPv6 dans le noyau.

### Étapes

1. Connectez-vous à l'hôte en tant que `root` ou en utilisant un compte avec l'autorisation `sudo`.
2. Exécutez la commande suivante : `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@SG:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

Le résultat doit être 0.

```
net.ipv6.conf.all.disable_ipv6 = 0
```



Si le résultat n'est pas 0, consultez la documentation de votre système d'exploitation pour modifier les `sysctl` paramètres. Ensuite, définissez la valeur sur 0 avant de continuer.

3. Entrez le conteneur de nœuds StorageGRID : `storagegrid node enter node-name`

4. Exécutez la commande suivante : `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@DC1-S1:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

Le résultat doit être 1.

```
net.ipv6.conf.all.disable_ipv6 = 1
```



Si le résultat n'est pas 1, cette procédure ne s'applique pas. Contactez l'assistance technique.

5. Sortir du conteneur : `exit`

```
root@DC1-S1:~ # exit
```

6. En tant que root, éditez le fichier suivant : `/var/lib/storagegrid/settings/sysctl.d/net.conf`.

```
sudo vi /var/lib/storagegrid/settings/sysctl.d/net.conf
```

7. Localisez les deux lignes suivantes et supprimez les balises de commentaire. Ensuite, enregistrez et fermez le fichier.

```
net.ipv6.conf.all.disable_ipv6 = 0
```

```
net.ipv6.conf.default.disable_ipv6 = 0
```

8. Exécutez ces commandes pour redémarrer le conteneur StorageGRID :

```
storagegrid node stop node-name
```

```
storagegrid node start node-name
```

## Dépanner un serveur syslog externe

Le tableau suivant décrit les messages d'erreur pouvant être liés à un serveur syslog externe et répertorie les actions correctives.

Pour plus d'informations sur l'envoi d'informations d'audit à un serveur syslog externe, reportez-vous à la section :

- ["Considérations relatives à l'utilisation d'un serveur syslog externe"](#)
- ["Configurer les messages d'audit et le serveur syslog externe"](#)

Message d'erreur	Description et actions recommandées
Impossible de résoudre le nom d'hôte	<p>Le FQDN que vous avez saisi pour le serveur syslog n'a pas pu être résolu en adresse IP.</p> <ol style="list-style-type: none"><li>1. Vérifiez le nom d'hôte que vous avez saisi. Si vous avez saisi une adresse IP, assurez-vous qu'elle est valide en notation W.X.Y.Z (« décimale à points »).</li><li>2. Vérifier que les serveurs DNS sont configurés correctement.</li><li>3. Vérifiez que chaque nœud peut accéder aux adresses IP du serveur DNS.</li></ol>
Connexion refusée	<p>Une connexion TCP ou TLS au serveur syslog a été refusée. Il se peut qu'il n'y ait pas d'écoute de service sur le port TCP ou TLS de l'hôte, ou qu'un pare-feu bloque l'accès.</p> <ol style="list-style-type: none"><li>1. Vérifiez que vous avez saisi le nom de domaine complet ou l'adresse IP, le port et le protocole corrects pour le serveur syslog.</li><li>2. Vérifiez que l'hôte du service syslog exécute un démon syslog écouté sur le port spécifié.</li><li>3. Vérifiez qu'un pare-feu ne bloque pas l'accès aux connexions TCP/TLS depuis les nœuds vers l'adresse IP et le port du serveur syslog.</li></ol>
Réseau inaccessible	<p>Le serveur syslog ne se trouve pas sur un sous-réseau directement connecté. Un routeur a renvoyé un message d'échec ICMP pour indiquer qu'il n'a pas pu transférer les messages de test des nœuds répertoriés vers le serveur syslog.</p> <ol style="list-style-type: none"><li>1. Vérifiez que vous avez saisi le nom de domaine complet ou l'adresse IP correct pour le serveur syslog.</li><li>2. Pour chaque nœud répertorié, vérifiez la liste de sous-réseaux du réseau Grid, les listes de sous-réseaux des réseaux Admin et les passerelles réseau client. Confirmez que ces éléments sont configurés pour acheminer le trafic vers le serveur syslog via l'interface réseau et la passerelle prévues (grille, Admin ou client).</li></ol>
Hôte inaccessible	<p>Le serveur syslog se trouve sur un sous-réseau directement connecté (sous-réseau utilisé par les nœuds répertoriés pour leurs adresses IP Grid, Admin ou client). Les nœuds ont tenté d'envoyer des messages de test, mais n'ont pas reçu de réponses aux requêtes ARP pour l'adresse MAC du serveur syslog.</p> <ol style="list-style-type: none"><li>1. Vérifiez que vous avez saisi le nom de domaine complet ou l'adresse IP correct pour le serveur syslog.</li><li>2. Vérifiez que l'hôte exécutant le service syslog est actif.</li></ol>



Message d'erreur	Description et actions recommandées
La connexion a expiré	<p>Une tentative de connexion TCP/TLS a été effectuée, mais aucune réponse n'a été reçue depuis longtemps du serveur syslog. Il peut y avoir une mauvaise configuration de routage ou un pare-feu peut tomber du trafic sans envoyer de réponse (configuration commune).</p> <ol style="list-style-type: none"> <li>1. Vérifiez que vous avez saisi le nom de domaine complet ou l'adresse IP correct pour le serveur syslog.</li> <li>2. Pour chaque nœud répertorié, vérifiez la liste de sous-réseaux du réseau Grid, les listes de sous-réseaux des réseaux Admin et les passerelles réseau client. Vérifiez qu'ils sont configurés pour acheminer le trafic vers le serveur syslog à l'aide de l'interface réseau et de la passerelle (Grid, Admin ou client) sur lesquelles vous vous attendez à ce que le serveur syslog soit atteint.</li> <li>3. Vérifiez qu'un pare-feu ne bloque pas l'accès aux connexions TCP/TLS à partir des nœuds répertoriés sur l'IP et le port du serveur syslog.</li> </ol>
Connexion fermée par le partenaire	<p>Une connexion TCP au serveur syslog a été établie avec succès, mais elle a été fermée ultérieurement. Plusieurs raisons peuvent expliquer ce phénomène :</p> <ul style="list-style-type: none"> <li>• Le serveur syslog a peut-être été redémarré ou redémarré.</li> <li>• Le nœud et le serveur syslog peuvent avoir des paramètres TCP/TLS différents.</li> <li>• Un pare-feu intermédiaire pourrait fermer les connexions TCP inactives.</li> <li>• Un serveur non syslog qui écoute sur le port du serveur syslog a peut-être fermé la connexion.</li> </ul> <p>Pour résoudre ce problème :</p> <ol style="list-style-type: none"> <li>1. Vérifiez que vous avez saisi le nom de domaine complet ou l'adresse IP, le port et le protocole corrects pour le serveur syslog.</li> <li>2. Si vous utilisez TLS, vérifiez que le serveur syslog utilise également TLS. Si vous utilisez TCP, vérifiez que le serveur syslog utilise également TCP.</li> <li>3. Vérifiez qu'un pare-feu intermédiaire n'est pas configuré pour fermer les connexions TCP inactives.</li> </ol>
Erreur de certificat TLS	<p>Le certificat de serveur reçu du serveur syslog n'était pas compatible avec le bundle de certificats CA et le certificat client que vous avez fournis.</p> <ol style="list-style-type: none"> <li>1. Vérifiez que le groupe de certificats de l'autorité de certification et le certificat client (le cas échéant) sont compatibles avec le certificat de serveur sur le serveur syslog.</li> <li>2. Vérifiez que les identités du certificat de serveur du serveur syslog incluent les valeurs IP ou FQDN attendues.</li> </ol>

Message d'erreur	Description et actions recommandées
Transfert suspendu	<p>Les enregistrements syslog ne sont plus transférés vers le serveur syslog et StorageGRID ne peut pas détecter la raison.</p> <p>Examinez les journaux de débogage fournis avec cette erreur pour tenter de déterminer la cause principale.</p>
Session TLS interrompue	<p>Le serveur syslog a mis fin à la session TLS et StorageGRID ne parvient pas à détecter la raison.</p> <ol style="list-style-type: none"> <li>1. Examinez les journaux de débogage fournis avec cette erreur pour tenter de déterminer la cause principale.</li> <li>2. Vérifiez que vous avez saisi le nom de domaine complet ou l'adresse IP, le port et le protocole corrects pour le serveur syslog.</li> <li>3. Si vous utilisez TLS, vérifiez que le serveur syslog utilise également TLS. Si vous utilisez TCP, vérifiez que le serveur syslog utilise également TCP.</li> <li>4. Vérifiez que le groupe de certificats de l'autorité de certification et le certificat client (le cas échéant) sont compatibles avec le certificat de serveur du serveur syslog.</li> <li>5. Vérifiez que les identités du certificat de serveur du serveur syslog incluent les valeurs IP ou FQDN attendues.</li> </ol>
Échec de la requête de résultats	<p>Le nœud d'administration utilisé pour la configuration et le test du serveur syslog ne peut pas demander les résultats de test à partir des nœuds répertoriés. Un ou plusieurs nœuds sont peut-être en panne.</p> <ol style="list-style-type: none"> <li>1. Suivez les étapes de dépannage standard pour vous assurer que les nœuds sont en ligne et que tous les services attendus sont en cours d'exécution.</li> <li>2. Redémarrez le service ETCD sur les nœuds répertoriés.</li> </ol>

## Examiner les journaux d'audit

### Journaux et messages d'audit

Ces instructions contiennent des informations sur la structure et le contenu des messages d'audit StorageGRID et des journaux d'audit. Vous pouvez utiliser ces informations pour lire et analyser la piste d'audit de l'activité du système.

Ces instructions s'adresse aux administrateurs responsables de la production de rapports d'activité et d'utilisation du système qui nécessitent une analyse des messages d'audit du système StorageGRID.

Pour utiliser le fichier journal texte, vous devez avoir accès au partage d'audit configuré sur le nœud d'administration.

Pour plus d'informations sur la configuration des niveaux de messages d'audit et l'utilisation d'un serveur syslog externe, reportez-vous à la section "[Configurez les messages d'audit et les destinations des journaux](#)".

## Flux et conservation des messages d'audit

Tous les services StorageGRID génèrent des messages d'audit pendant le fonctionnement normal du système. Vous devez comprendre comment ces messages d'audit se déplacent dans le fichier via le système StorageGRID `audit.log`.

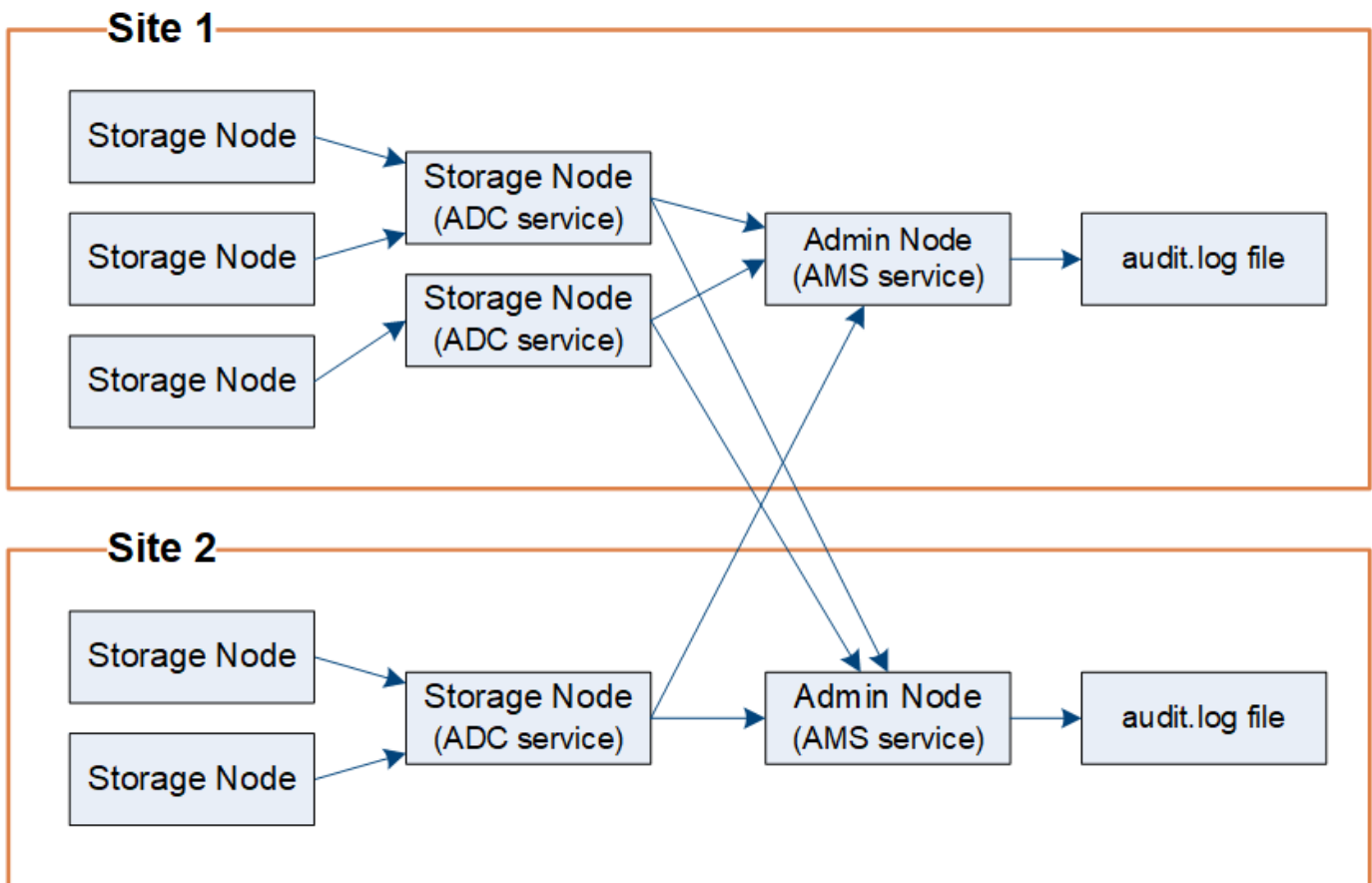
### Flux de message d'audit

Les messages d'audit sont traités par des nœuds d'administration et par les nœuds de stockage disposant d'un service ADC (administrative Domain Controller).

Comme indiqué dans le schéma de flux des messages d'audit, chaque nœud StorageGRID envoie ses messages d'audit à l'un des services ADC du site du centre de données. Le service ADC est automatiquement activé pour les trois premiers nœuds de stockage installés sur chaque site.

De son tour, chaque service ADC agit comme un relais et envoie sa collection de messages d'audit à chaque nœud d'administration du système StorageGRID, ce qui donne à chaque nœud d'administration un enregistrement complet de l'activité du système.

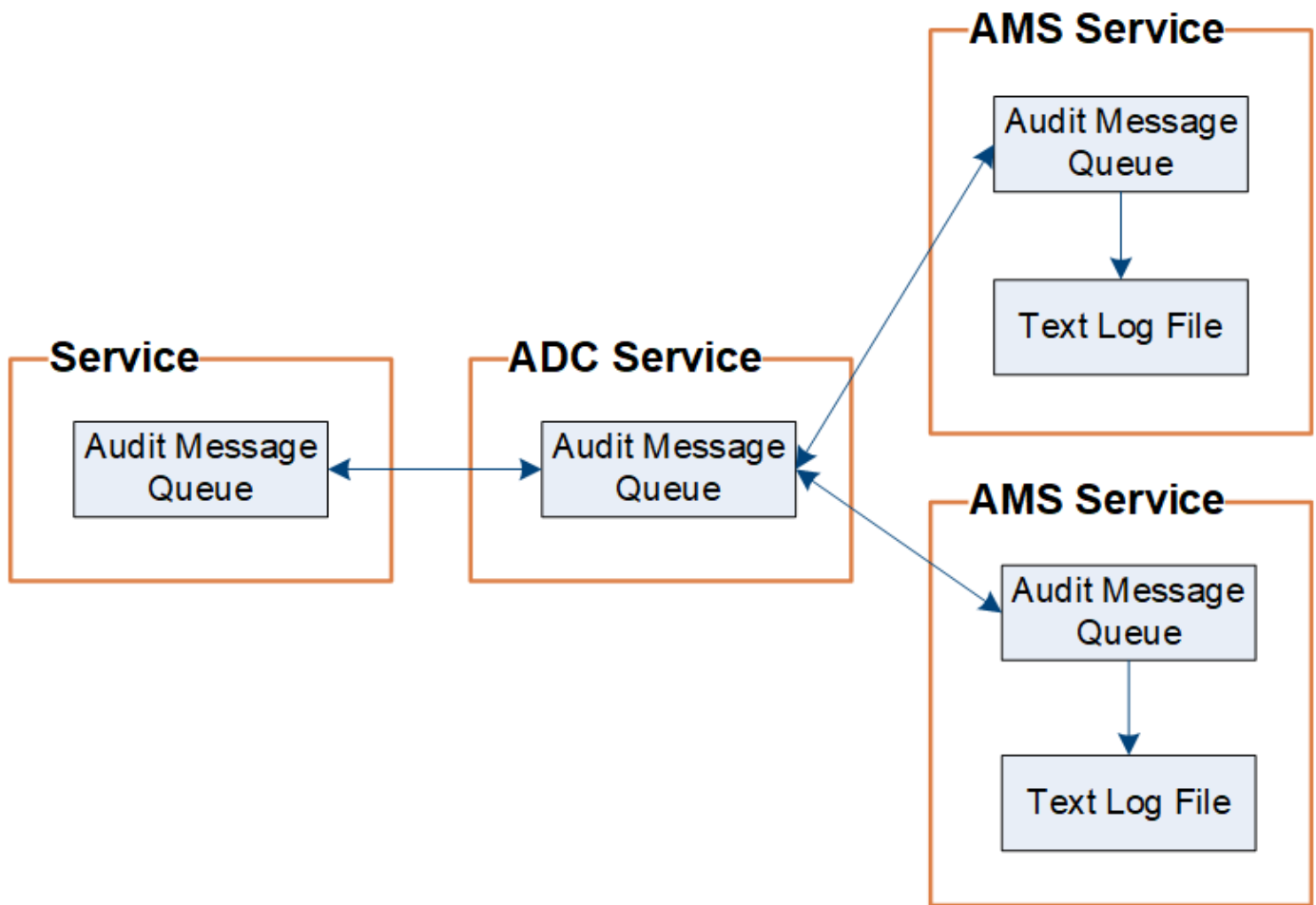
Chaque nœud d'administration stocke les messages d'audit dans des fichiers journaux texte ; le fichier journal actif est nommé `audit.log`.



### Conservation des messages d'audit

StorageGRID utilise un processus de copie et de suppression pour garantir qu'aucun message d'audit ne soit perdu avant d'être écrit dans le journal d'audit.

Lorsqu'un nœud génère ou transmet un message d'audit, celui-ci est stocké dans une file d'attente de messages d'audit sur le disque système du nœud de la grille. Une copie du message est toujours conservée dans une file d'attente de messages d'audit jusqu'à ce que le message soit écrit dans le fichier journal d'audit dans le répertoire du nœud d'administration `/var/local/log`. Cela permet d'éviter la perte d'un message d'audit pendant le transport.



La file d'attente des messages d'audit peut augmenter temporairement en raison de problèmes de connectivité réseau ou d'une capacité d'audit insuffisante. Au fur et à mesure que les files d'attente augmentent, elles consomment davantage d'espace disponible dans le répertoire de chaque nœud `/var/local/`. Si le problème persiste et que le répertoire des messages d'audit d'un nœud devient trop plein, les nœuds individuels priorisent le traitement de leur carnet de commandes et deviennent temporairement indisponibles pour les nouveaux messages.

Plus précisément, vous pouvez voir les comportements suivants :

- Si le `/var/local/log` répertoire utilisé par un nœud d'administration est plein, le nœud d'administration est signalé comme indisponible pour les nouveaux messages d'audit jusqu'à ce que le répertoire ne soit plus plein. Les requêtes des clients S3 ne sont pas affectées. L'alarme XAMS (Unreable Audit Revers) est déclenchée lorsqu'un référentiel d'audit est inaccessible.
- Si le `/var/local/` répertoire utilisé par un nœud de stockage avec le service ADC devient plein à 92 %, le nœud sera signalé comme indisponible pour vérifier les messages jusqu'à ce que le répertoire soit rempli à 87 % seulement. Les requêtes des clients S3 vers d'autres nœuds ne sont pas affectées. L'alarme NRLY (relais d'audit disponibles) est déclenchée lorsque les relais d'audit sont inaccessibles.



S'il n'y a pas de nœuds de stockage disponibles avec le service ADC, les nœuds de stockage stockent les messages d'audit localement dans `/var/local/log/localaudit.log` le fichier.

- Si le `/var/local/` répertoire utilisé par un nœud de stockage est rempli à 85 %, le nœud commence à refuser les requêtes du client S3 avec `503 Service Unavailable`.

Les types de problèmes suivants peuvent entraîner une augmentation très importante des files d'attente de messages d'audit :

- Panne d'un nœud d'administration ou d'un nœud de stockage avec le service ADC. Si l'un des nœuds du système est en panne, les nœuds restants peuvent devenir connectés à un nœud défaillant.
- Un taux d'activité soutenu qui dépasse la capacité d'audit du système.
- L'``/var/local/``espace sur un nœud de stockage ADC devient saturé pour des raisons sans rapport avec les messages d'audit. Dans ce cas, le nœud n'accepte plus de nouveaux messages d'audit et hiérarchise son carnet de commandes actuel, ce qui peut entraîner des arriérés sur les autres nœuds.

#### Alerte de file d'attente d'audit et alarme de messages d'audit en file d'attente (AMQS)

Pour vous aider à surveiller la taille des files d'attente de messages d'audit dans le temps, l'alerte **grande file d'attente d'audit** et l'alarme AMQS héritée sont déclenchées lorsque le nombre de messages dans une file d'attente de nœud de stockage ou une file d'attente de nœud d'administration atteint certains seuils.

Si l'alerte **grande file d'attente d'audit** ou l'alarme AMQS héritée est déclenchée, commencez par vérifier la charge sur le système—s'il y a eu un nombre important de transactions récentes, l'alerte et l'alarme doivent être résolus au fil du temps et peuvent être ignorées.

Si l'alerte ou l'alarme persiste et augmente la gravité, affichez un graphique de la taille de la file d'attente. Si ce chiffre augmente régulièrement au fil des heures ou des jours, la charge d'audit a probablement dépassé la capacité d'audit du système. Réduisez le taux de fonctionnement du client ou diminuez le nombre de messages d'audit consignés en modifiant le niveau d'audit pour les écritures du client et les lectures du client sur erreur ou Désactivé. Voir "[Configurez les messages d'audit et les destinations des journaux](#)".

#### Dupliquer les messages

Le système StorageGRID adopte une approche prudente en cas de panne sur un réseau ou un nœud. Pour cette raison, des messages en double peuvent exister dans le journal d'audit.

### Accéder au fichier journal d'audit

Le partage d'audit contient le fichier actif `audit.log` et tous les fichiers journaux d'audit compressés. Vous pouvez accéder aux fichiers journaux d'audit directement à partir de la ligne de commande du nœud d'administration.

#### Avant de commencer

- Vous avez "[autorisations d'accès spécifiques](#)".
- Vous devez avoir le `Passwords.txt` fichier.
- Vous devez connaître l'adresse IP d'un nœud d'administration.

#### Étapes

1. Connectez-vous à un nœud d'administration :
  - a. Entrez la commande suivante : `ssh admin@primary_Admin_Node_IP`
  - b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
  - c. Entrez la commande suivante pour basculer en root : `su -`
  - d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Accédez au répertoire contenant les fichiers journaux d'audit :

```
cd /var/local/log
```

3. Afficher le fichier journal d'audit actuel ou enregistré, selon les besoins.

## Rotation du fichier journal d'audit

Les fichiers journaux d'audit sont enregistrés dans le répertoire d'un nœud d'administration `/var/local/log`. Les fichiers journaux d'audit actifs sont nommés `audit.log`.



Vous pouvez également modifier la destination des journaux d'audit et envoyer des informations d'audit à un serveur syslog externe. Les journaux locaux des enregistrements d'audit continuent à être générés et stockés lorsqu'un serveur syslog externe est configuré. Voir "[Configurez les messages d'audit et les destinations des journaux](#)".

Une fois par jour, le fichier actif `audit.log` est enregistré et un nouveau `audit.log` fichier démarre. Le nom du fichier enregistré indique quand il a été enregistré, au format `yyyy-mm-dd.txt`. Si plusieurs journaux d'audit sont créés en une seule journée, les noms de fichier utilisent la date à laquelle le fichier a été enregistré, ajoutée par un nombre, au format `yyyy-mm-dd.txt.n`. Par exemple, `2018-04-15.txt` et `2018-04-15.txt.1` sont les premier et deuxième fichiers journaux créés et enregistrés le 15 avril 2018.

Après un jour, le fichier enregistré est compressé et renommé, au format `yyyy-mm-dd.txt.gz`, qui conserve la date d'origine. Avec le temps, cela entraîne la consommation du stockage alloué aux journaux d'audit sur le nœud d'administration. Un script surveille la consommation d'espace du journal d'audit et supprime les fichiers journaux si nécessaire pour libérer de l'espace dans le `/var/local/log` répertoire. Les journaux d'audit sont supprimés en fonction de la date de création, le plus ancien étant supprimé en premier. Vous pouvez contrôler les actions du script dans le fichier suivant : `/var/local/log/manage-audit.log`.

Cet exemple montre le fichier actif `audit.log`, le fichier du jour précédent (`2018-04-15.txt`) et le fichier compressé du jour précédent (`2018-04-14.txt.gz`).

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

## Format du fichier journal d'audit

### Format du fichier journal d'audit

Les fichiers journaux d'audit se trouvent sur chaque nœud d'administration et contiennent un ensemble de messages d'audit individuels.

Chaque message d'audit contient les éléments suivants :

- Temps universel coordonné (UTC) de l'événement qui a déclenché le message d'audit (ATIM) au format ISO 8601, suivi d'un espace :

*YYYY-MM-DDTHH:MM:SS.UUUUUU*, où *UUUUUU* sont des microsecondes.

- Le message d'audit lui-même, entre crochets et commençant par AUDT.

L'exemple suivant montre trois messages d'audit dans un fichier journal d'audit (sauts de ligne ajoutés pour la lisibilité). Ces messages ont été générés lorsqu'un locataire a créé un compartiment S3 et a ajouté deux objets dans ce compartiment.

```
2019-08-07T18:43:30.247711
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][SAI
P(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWnt-
PhoTDwB9Jok7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][AVER(UI32):10][ATIM(UI64):1565203410247711]
[ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):7074142
142472611085]]
```

```
2019-08-07T18:43:30.783597
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991696][TIME(UI64):120713][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWnt-
PhoTDwB9Jok7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-0"]
[CBID(UI64):0x779557A069B2C037][UUID(CSTR):"94BA6949-38E1-4B0C-BC80-
EB44FB4FCC7F"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410783597][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):8439606722108456022]]
```

```
2019-08-07T18:43:30.784558
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991693][TIME(UI64):121666][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWnt-
PhoTDwB9Jok7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-2000"]
[CBID(UI64):0x180CBD8E678EED17][UUID(CSTR):"19CE06D0-D2CF-4B03-9C38-
E578D66F7ADD"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410784558][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):13489590586043706682]]
```

Dans leur format par défaut, les messages d'audit dans les fichiers journaux d'audit ne sont pas faciles à lire ou à interpréter. Vous pouvez utiliser le ["outil d'audit-explication"](#) pour obtenir des résumés simplifiés des messages d'audit dans le journal d'audit. Vous pouvez utiliser le ["outil de somme d'audit"](#) pour résumer le nombre d'opérations d'écriture, de lecture et de suppression consignées, ainsi que la durée de ces opérations.

### Utiliser l'outil d'explication d'audit

Vous pouvez utiliser `audit-explain` l'outil pour traduire les messages d'audit dans le journal d'audit dans un format facile à lire.



## Avant de commencer

- Vous avez "[autorisations d'accès spécifiques](#)".
- Vous devez avoir le `Passwords.txt` fichier.
- Vous devez connaître l'adresse IP du nœud d'administration principal.

## Description de la tâche

L' `audit-explain` outil, disponible sur le nœud d'administration principal, fournit des résumés simplifiés des messages d'audit dans un journal d'audit.



Cet `audit-explain` outil est principalement destiné au support technique lors des opérations de dépannage. Le traitement des `audit-explain` requêtes peut consommer une grande quantité de puissance CPU, ce qui peut avoir un impact sur les opérations StorageGRID.

Cet exemple montre les résultats typiques de l' `audit-explain` outil. Ces quatre "**SPUT**" messages d'audit ont été générés lorsque le locataire S3 associé à l'ID de compte 92484777680322627870 a utilisé des demandes PUT S3 pour créer un compartiment nommé « bucket1 » et ajouter trois objets à ce compartiment.

```
SPUT S3 PUT bucket bucket1 account:92484777680322627870 usec:124673
SPUT S3 PUT object bucket1/part1.txt tenant:92484777680322627870
cbid:9DCB157394F99FE5 usec:101485
SPUT S3 PUT object bucket1/part2.txt tenant:92484777680322627870
cbid:3CFBB07AB3D32CA9 usec:102804
SPUT S3 PUT object bucket1/part3.txt tenant:92484777680322627870
cbid:5373D73831ECC743 usec:93874
```

L' `audit-explain` outil peut effectuer les opérations suivantes :

- Traiter les journaux d'audit bruts ou compressés. Par exemple :

```
audit-explain audit.log
```

```
audit-explain 2019-08-12.txt.gz
```

- Traitez plusieurs fichiers simultanément. Par exemple :

```
audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-explain /var/local/log/*
```

- Acceptez l'entrée d'un canal, qui vous permet de filtrer et de prétraiter l'entrée à l'aide de la `grep` commande ou d'autres moyens. Par exemple :

```
grep SPUT audit.log | audit-explain
```

```
grep bucket-name audit.log | audit-explain
```

Comme les journaux d'audit peuvent être très volumineux et lents à analyser, vous gagnez du temps en filtrant les parties que vous souhaitez consulter et exécuter `audit-explain` sur les pièces, au lieu du fichier entier.



``audit-explain``L'outil n'accepte pas les fichiers compressés en tant qu'entrée de tuyauterie. Pour traiter des fichiers compressés, indiquez leurs noms de fichiers en tant qu'arguments de ligne de commande ou utilisez l' ``zcat``outil pour décompresser d'abord les fichiers. Par exemple :

```
zcat audit.log.gz | audit-explain
```

Utilisez l' ``help (-h)``option pour voir les options disponibles. Par exemple :

```
$ audit-explain -h
```

## Étapes

1. Connectez-vous au nœud d'administration principal :

- Entrez la commande suivante : `ssh admin@primary_Admin_Node_IP`
- Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
- Entrez la commande suivante pour basculer en root : `su -`
- Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

2. Entrez la commande suivante, où `/var/local/log/audit.log` représente le nom et l'emplacement du ou des fichiers à analyser :

```
$ audit-explain /var/local/log/audit.log
```

L' ``audit-explain``outil imprime des interprétations lisibles de tous les messages du ou des fichiers spécifiés.



Pour réduire la longueur des lignes et faciliter la lisibilité, les horodatages ne sont pas affichés par défaut. Si vous voulez voir les horodatages, utilisez l' ``-t``option horodatage ).

## Utiliser l'outil audit-sum

Vous pouvez utiliser `audit-sum` l'outil pour compter les messages d'audit d'écriture, de lecture, de tête et de suppression et pour afficher le temps minimal, maximal et moyen (ou la taille) pour chaque type d'opération.

### Avant de commencer

- Vous avez "[autorisations d'accès spécifiques](#)".
- Vous devez avoir le `Passwords.txt` fichier.
- Vous devez connaître l'adresse IP du nœud d'administration principal.

### Description de la tâche

L' ``audit-sum``outil, disponible sur le nœud d'administration principal, récapitule le nombre d'opérations d'écriture, de lecture et de suppression consignées, ainsi que la durée de ces opérations.



Cet `audit-sum` outil est principalement destiné au support technique lors des opérations de dépannage. Le traitement des `audit-sum` requêtes peut consommer une grande quantité de puissance CPU, ce qui peut avoir un impact sur les opérations StorageGRID.

Cet exemple montre les résultats typiques de l' `audit-sum` outil. Cet exemple montre la durée des opérations de protocoles.

message group average (sec)	count	min (sec)	max (sec)
=====	=====	=====	=====
=====			
IDEL	274		
SDEL	213371	0.004	20.934
0.352			
SGET	201906	0.010	1740.290
1.132			
SHEA	22716	0.005	2.349
0.272			
SPUT	1771398	0.011	1770.563
0.487			

`audit-sum` L'outil fournit le nombre et l'heure des messages d'audit S3, Swift et ILM suivants dans un journal d'audit.



Les codes d'audit sont supprimés du produit et de la documentation, car les fonctionnalités sont obsolètes. Si vous rencontrez un code d'audit qui n'est pas répertorié ici, consultez les versions précédentes de cette rubrique pour connaître les versions antérieures de SG. Par exemple "[StorageGRID 11.8 à l'aide de la documentation de l'outil de somme d'audit](#)", .

Code	Description	Reportez-vous à la section
IDEL	ILM initialisée – journaux lorsque l'ILM démarre le processus de suppression d'un objet.	<a href="#">"IDEL : suppression initiée ILM"</a>
SDEL	SUPPRESSION S3 : journal une transaction réussie pour supprimer un objet ou un compartiment.	<a href="#">"SDEL : SUPPRESSION S3"</a>
SGET	S3 GET : log une transaction réussie pour récupérer un objet ou répertorier les objets dans un compartiment.	<a href="#">"SGET : OBTENEZ S3"</a>
SHEA	TÊTE S3 : consigne une transaction réussie pour vérifier l'existence d'un objet ou d'un compartiment.	<a href="#">"SHEA : TÊTE S3"</a>

Code	Description	Reportez-vous à la section
SPUT	S3 PUT : enregistre la réussite d'une transaction pour créer un nouvel objet ou un compartiment.	"SPUT : PUT S3"
WDEL	SUPPRESSION Swift : enregistre une transaction réussie pour supprimer un objet ou un conteneur.	"WDEL : SUPPRESSION rapide"
C'EST PARTI	SWIFT GET : log une transaction réussie pour récupérer un objet ou répertorier les objets dans un conteneur.	"WGET: SWIFT GET"
WHEA	SWIFT HEAD : consigne une transaction réussie afin de vérifier l'existence d'un objet ou d'un conteneur.	"WHEA: TÊTE SWIFT"
WPUT	SWIFT PUT : consigne une transaction réussie pour créer un nouvel objet ou conteneur.	"WPUT : PUT SWIFT"

L'`audit-sum`outil peut effectuer les opérations suivantes :

- Traiter les journaux d'audit bruts ou compressés. Par exemple :

```
audit-sum audit.log
```

```
audit-sum 2019-08-12.txt.gz
```

- Traitez plusieurs fichiers simultanément. Par exemple :

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-sum /var/local/log/*
```

- Acceptez l'entrée d'un canal, qui vous permet de filtrer et de prétraiter l'entrée à l'aide de la `grep` commande ou d'autres moyens. Par exemple :

```
grep WGET audit.log | audit-sum
```

```
grep bucket1 audit.log | audit-sum
```

```
grep SPUT audit.log | grep bucket1 | audit-sum
```



Cet outil n'accepte pas les fichiers compressés comme entrée de pipettes. Pour traiter des fichiers compressés, indiquez leurs noms de fichiers en tant qu'arguments de ligne de commande ou utilisez l'`zcat`outil pour décompresser d'abord les fichiers. Par exemple :

```
audit-sum audit.log.gz
```

```
zcat audit.log.gz | audit-sum
```

Vous pouvez utiliser les options de ligne de commande pour résumer les opérations sur des compartiments

séparément des opérations sur des objets ou pour regrouper les résumés de messages par nom de compartiment, par période ou par type de cible. Par défaut, les résumés affichent le temps de fonctionnement minimal, maximal et moyen, mais vous pouvez utiliser l' `size (-s)` option pour examiner la taille de l'objet à la place.

Utilisez l' `help (-h)` option pour voir les options disponibles. Par exemple :

```
$ audit-sum -h
```

## Étapes

1. Connectez-vous au nœud d'administration principal :

- a. Entrez la commande suivante : `ssh admin@primary_Admin_Node_IP`
- b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
- c. Entrez la commande suivante pour basculer en root : `su -`
- d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

2. Pour analyser tous les messages liés aux opérations d'écriture, de lecture, de tête et de suppression, procédez comme suit :

- a. Entrez la commande suivante, où `/var/local/log/audit.log` représente le nom et l'emplacement du ou des fichiers à analyser :

```
$ audit-sum /var/local/log/audit.log
```

Cet exemple montre les résultats typiques de l' `audit-sum` outil. Cet exemple montre la durée des opérations de protocoles.

message group	count	min(sec)	max(sec)
average(sec)			
=====	=====	=====	=====
=====			
IDEL	274		
SDEL	213371	0.004	20.934
0.352			
SGET	201906	0.010	1740.290
1.132			
SHEA	22716	0.005	2.349
0.272			
SPUT	1771398	0.011	1770.563
0.487			

Dans cet exemple, les opérations SGET (S3 GET) sont les opérations les plus lentes en moyenne à 1.13 secondes, mais les opérations SGET et SPUT (S3 PUT) affichent toutes les deux de longues périodes de pire des cas d'environ 1,770 secondes.

- b. Pour afficher les opérations de récupération 10 les plus lentes, utilisez la commande `grep` pour

sélectionner uniquement les messages SGET et ajouter l'option de sortie longue (-l) pour inclure les chemins d'objet :

```
grep SGET audit.log | audit-sum -l
```

Les résultats incluent le type (objet ou compartiment) et le chemin, ce qui vous permet d'afficher le journal d'audit pour les autres messages relatifs à ces objets particuliers.

```
Total:          201906 operations
Slowest:        1740.290 sec
Average:        1.132 sec
Fastest:        0.010 sec
Slowest operations:
      time(usec)      source ip      type      size(B) path
      =====      =====
      1740289662     10.96.101.125      object     5663711385
backup/r9010aQ8JB-1566861764-4519.iso
      1624414429     10.96.101.125      object     5375001556
backup/r9010aQ8JB-1566861764-6618.iso
      1533143793     10.96.101.125      object     5183661466
backup/r9010aQ8JB-1566861764-4518.iso
      70839          10.96.101.125      object           28338
bucket3/dat.1566861764-6619
      68487          10.96.101.125      object           27890
bucket3/dat.1566861764-6615
      67798          10.96.101.125      object           27671
bucket5/dat.1566861764-6617
      67027          10.96.101.125      object           27230
bucket5/dat.1566861764-4517
      60922          10.96.101.125      object           26118
bucket3/dat.1566861764-4520
      35588          10.96.101.125      object           11311
bucket3/dat.1566861764-6616
      23897          10.96.101.125      object           10692
bucket3/dat.1566861764-4516
```

+

Dans cet exemple de sortie, vous pouvez constater que les trois demandes GET S3 les plus lentes étaient celles des objets d'une taille d'environ 5 Go (ce qui est beaucoup plus important que les autres objets). La grande taille tient compte des délais de récupération lents les moins importants.

3. Si vous voulez déterminer la taille des objets qui sont ingérés et récupérés à partir de votre grille, utilisez l'option taille (-s) :

```
audit-sum -s audit.log
```

message group average (MB)	count	min (MB)	max (MB)
=====	=====	=====	=====
IDEL 1654.502	274	0.004	5000.000
SDEL 1.695	213371	0.000	10.504
SGET 14.920	201906	0.000	5000.000
SHEA 2.967	22716	0.001	10.504
SPUT 2.495	1771398	0.000	5000.000

Dans cet exemple, la taille moyenne des objets pour SPUT est inférieure à 2.5 Mo, mais la taille moyenne pour SGET est beaucoup plus grande. Le nombre de messages SPUT est beaucoup plus élevé que le nombre de messages SGET, ce qui indique que la plupart des objets ne sont jamais récupérés.

4. Si vous voulez déterminer si les récupérations étaient lentes hier :
  - a. Exécutez la commande dans le journal d'audit approprié et utilisez l'option Group-by-time (-gt(groupe par heure), suivie de la période (par exemple, 15M, 1H, 10S) :

```
grep SGET audit.log | audit-sum -gt 1H
```

message group average(sec)	count	min(sec)	max(sec)
=====	=====	=====	=====
2019-09-05T00 1.254	7591	0.010	1481.867
2019-09-05T01 1.115	4173	0.011	1740.290
2019-09-05T02 1.562	20142	0.011	1274.961
2019-09-05T03 1.254	57591	0.010	1383.867
2019-09-05T04 1.405	124171	0.013	1740.290
2019-09-05T05 1.562	420182	0.021	1274.511
2019-09-05T06 5.562	1220371	0.015	6274.961
2019-09-05T07 2.002	527142	0.011	1974.228
2019-09-05T08 1.105	384173	0.012	1740.290
2019-09-05T09 1.354	27591	0.010	1481.867

Ces résultats montrent que S3 GÉNÈRE un trafic entre 06:00 et 07:00. Les temps maximum et moyen sont à la fois considérablement plus élevés à ces moments aussi, et ils n'ont pas augmenté progressivement à mesure que le comptage a augmenté. Cela suggère que la capacité a été dépassée quelque part, peut-être dans le réseau ou que la grille peut traiter les demandes.

- b. Pour déterminer la taille des objets récupérés chaque heure d'hier, ajoutez l'option size (-s) à la commande :

```
grep SGET audit.log | audit-sum -gt 1H -s
```



message group average (B)	count	min (B)	max (B)
=====	=====	=====	=====
2019-09-05T00 1.976	7591	0.040	1481.867
2019-09-05T01 2.062	4173	0.043	1740.290
2019-09-05T02 2.303	20142	0.083	1274.961
2019-09-05T03 1.182	57591	0.912	1383.867
2019-09-05T04 1.528	124171	0.730	1740.290
2019-09-05T05 2.398	420182	0.875	4274.511
2019-09-05T06 51.328	1220371	0.691	5663711385.961
2019-09-05T07 2.147	527142	0.130	1974.228
2019-09-05T08 1.878	384173	0.625	1740.290
2019-09-05T09 1.354	27591	0.689	1481.867

Ces résultats indiquent que des récupérations très importantes se sont produites lorsque le trafic global de récupération était à son maximum.

c. Pour plus de détails, utilisez le ["outil d'audit-explication"](#) pour revoir toutes les opérations SGET pendant cette heure :

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

Si la sortie de la commande `grep` doit être de plusieurs lignes, ajoutez la `less` commande pour afficher le contenu du fichier journal d'audit, une page (un écran) à la fois.

5. Si vous souhaitez déterminer si les opérations SPUT sur les godets sont plus lentes que les opérations SPUT pour les objets :

a. Commencez par utiliser l' ``-go`` option, qui regroupe les messages pour les opérations d'objet et de compartiment séparément :

```
grep SPUT sample.log | audit-sum -go
```

message group	count	min(sec)	max(sec)
average(sec)			
=====	=====	=====	=====
=====			
SPUT.bucket	1	0.125	0.125
0.125			
SPUT.object	12	0.025	1.019
0.236			

Les résultats montrent que les opérations SPUT pour les compartiments ont des caractéristiques de performances différentes de celles des opérations SPUT pour les objets.

b. Pour déterminer les compartiments ayant les opérations SPUT les plus lentes, utilisez l'`-gb`option, qui regroupe les messages par compartiment :

```
grep SPUT audit.log | audit-sum -gb
```

message group	count	min(sec)	max(sec)
average(sec)			
=====	=====	=====	=====
=====			
SPUT.cho-non-versioning	71943	0.046	1770.563
1.571			
SPUT.cho-versioning	54277	0.047	1736.633
1.415			
SPUT.cho-west-region	80615	0.040	55.557
1.329			
SPUT.ldt002	1564563	0.011	51.569
0.361			

c. Pour déterminer quels compartiments ont la taille d'objet SPUT la plus élevée, utilisez les`-gb`options et`-s` :

```
grep SPUT audit.log | audit-sum -gb -s
```

message group average (B)	count	min (B)	max (B)
=====	=====	=====	=====
SPUT.cho-non-versioning 21.672	71943	2.097	5000.000
SPUT.cho-versioning 21.120	54277	2.097	5000.000
SPUT.cho-west-region 14.433	80615	2.097	800.000
SPUT.ldt002 0.352	1564563	0.000	999.972

## Format du message d'audit

### Format du message d'audit

Les messages d'audit échangés dans le système StorageGRID incluent des informations standard communes à tous les messages et du contenu spécifique décrivant l'événement ou l'activité signalé.

Si les informations récapitulatives fournies par les ["audit - expliquer"](#) outils et ["somme-audit"](#) sont insuffisantes, reportez-vous à cette section pour comprendre le format général de tous les messages d'audit.

Voici un exemple de message d'audit tel qu'il peut apparaître dans le fichier journal d'audit :

```
2014-07-17T03:50:47.484627
[AUDT: [RSLT (FC32) :VRGN] [AVER (UI32) :10] [ATIM (UI64) :1405569047484627] [ATYP (FC32) :SYSU] [ANID (UI32) :11627225] [AMID (FC32) :ARNI] [ATID (UI64) :9445736326500603516]]
```

Chaque message d'audit contient une chaîne d'éléments d'attribut. La chaîne entière est entre parenthèses ( [ ] ) et chaque élément d'attribut de la chaîne possède les caractéristiques suivantes :

- Entre parenthèses [ ]
- Introduit par la chaîne `AUDT`, qui indique un message d'audit
- Sans délimiteurs (pas de virgules ni d'espaces) avant ou après
- Terminé par un caractère de saut de ligne `\n`

Chaque élément inclut un code d'attribut, un type de données et une valeur qui sont rapportées dans ce format :

```
[ATTR (type) :value] [ATTR (type) :value] ...  
[ATTR (type) :value] \n
```

Le nombre d'éléments d'attribut dans le message dépend du type d'événement du message. Les éléments d'attribut ne sont pas répertoriés dans un ordre particulier.

La liste suivante décrit les éléments d'attribut :

- `ATTR` est un code à quatre caractères pour l'attribut signalé. Certains attributs sont communs à tous les messages d'audit et à d'autres, qui sont spécifiques à un événement.
- `type` Est un identificateur à quatre caractères du type de données de programmation de la valeur, comme `UI64`, `FC32`, etc. Le type est entre parenthèses ( ).
- `value` est le contenu de l'attribut, généralement une valeur numérique ou textuelle. Les valeurs suivent toujours deux points (:). Les valeurs du type de données `CSTR` sont entourées de guillemets doubles " ".

## Types de données

Différents types de données sont utilisés pour stocker les informations dans les messages d'audit.

Type	Description
UI32	Entier long non signé (32 bits) ; il peut stocker les nombres 0 à 4,294,967,295.
UI64	Entier double non signé (64 bits) ; il peut stocker les nombres 0 à 18,446,744,073,709,551,615.
FC32	Constante de quatre caractères ; valeur entière non signée de 32 bits représentée par quatre caractères ASCII tels que « ABCD ».
IPAD	Utilisé pour les adresses IP.
REST	Tableau de caractères UTF-8 de longueur variable. Les caractères peuvent être échappé avec les conventions suivantes : <ul style="list-style-type: none"><li>• La barre oblique inverse est <code>\\</code>.</li><li>• Le retour chariot est <code>\r</code>.</li><li>• Les guillemets sont <code>\"</code>.</li><li>• La ligne d'alimentation (nouvelle ligne) est <code>\n</code>.</li><li>• Les caractères peuvent être remplacés par leurs équivalents hexadécimaux (au format <code>\XHH</code>, où <code>HH</code> est la valeur hexadécimale représentant le caractère).</li></ul>

## Données spécifiques à un événement

Chaque message d'audit du journal d'audit enregistre les données spécifiques à un événement système.

Après le conteneur d'ouverture [AUDT : qui identifie le message lui-même, l'ensemble d'attributs suivant fournit des informations sur l'événement ou l'action décrit par le message d'audit. Ces attributs sont mis en évidence dans l'exemple suivant :

```
2018-12-05T08:24 10.224.0 60025621595611246499:45.921845 100 60025621595611246499
[AUDT:*[RSLT(FC32):SUCS] [TIME(UI64):11454][SAIP(IPAD)][S3AI(CSTR)](CSTR)
60025621595611246499\« STU3S\ »\« STC\ »\« STC\ »\[STC\ » :[S6S][STC\STC\STC\« STC\ »
:[STE][STC\STC\STC\STC\STE][STC*[STC\STC\STC\STC*[STC\« S\ » :[STC\« STE\ » :[STC\« STE\
» :[STE\« S\ » :[STE\ »\ » :[STE\S3S\ » :*[STC\STC\STC\S37 30720 10 1543998285921845
12281045 15552417629170647261
```

L'`ATYP`élément (souligné dans l'exemple) identifie l'événement qui a généré le message. Cet exemple de message inclut le "**SHEA**"code de message ([ATYP(FC32):SHEA]), indiquant qu'il a été généré par une demande S3 HEAD réussie.

### Éléments communs dans les messages d'audit

Tous les messages d'audit contiennent les éléments communs.

Code	Type	Description
AU MILIEU	FC32	ID de module : identificateur à quatre caractères de l'ID de module qui a généré le message. Ceci indique le segment de code dans lequel le message d'audit a été généré.
ANID	UI32	ID de nœud : ID de nœud de la grille attribué au service qui a généré le message. Un identifiant unique est attribué à chaque service au moment de la configuration et de l'installation du système StorageGRID. Cet ID ne peut pas être modifié.
ASE	UI64	Identifiant de session d'audit : dans les versions précédentes, cet élément indique l'heure à laquelle le système d'audit a été initialisé après le démarrage du service. Cette valeur temporelle a été mesurée en microsecondes depuis l'époque du système d'exploitation (00:00:00 UTC le 1er janvier 1970).  <b>Remarque</b> : cet élément est obsolète et n'apparaît plus dans les messages d'audit.
ASQN	UI64	Nombre de séquences : dans les versions précédentes, ce compteur a été incrémenté pour chaque message d'audit généré sur le nœud de la grille (ANID) et remis à zéro au redémarrage du service.  <b>Remarque</b> : cet élément est obsolète et n'apparaît plus dans les messages d'audit.
ATID	UI64	Trace ID : identifiant partagé par l'ensemble de messages déclenchés par un seul événement.

Code	Type	Description
ATIM	UI64	<p>Timestamp: Heure à laquelle l'événement a été généré le message d'audit, mesuré en microsecondes depuis l'époque du système d'exploitation (00:00:00 UTC le 1er janvier 1970). Notez que la plupart des outils disponibles pour convertir l'horodatage en date et heure locales sont basés sur des millisecondes.</p> <p>Il peut être nécessaire d'arrondir ou de tronquer l'horodatage enregistré. Le temps lisible par l'utilisateur qui apparaît au début du message d'audit dans le <code>audit.log</code> fichier est l'attribut ATIM au format ISO 8601. La date et l'heure sont représentées par <code>YYYY-MMDDTHH:MM:SS.UUUUUU</code>, où le <code>T</code> est un caractère de chaîne littérale indiquant le début du segment de temps de la date. <code>UUUUUU</code> sont des microsecondes.</p>
ATYP	FC32	Type d'événement : identificateur à quatre caractères de l'événement en cours de consignation. Cela régit le contenu « charge utile » du message : les attributs inclus.
FINISSEUR	UI32	Version : version du message d'audit. À mesure que le logiciel StorageGRID évolue, les nouvelles versions de services peuvent intégrer de nouvelles fonctionnalités dans les rapports d'audit. Ce champ permet une rétrocompatibilité dans le service AMS pour traiter les messages provenant de versions antérieures de services.
RSLT	FC32	Résultat : résultat de l'événement, du processus ou de la transaction. Si n'est pas pertinent pour un message, AUCUN n'est utilisé plutôt que LES CMC pour que le message ne soit pas filtré accidentellement.

### Exemples de messages d'audit

Vous trouverez des informations détaillées dans chaque message d'audit. Tous les messages d'audit utilisent le même format.

Voici un exemple de message d'audit tel qu'il peut apparaître dans `audit.log` le fichier :

```
2014-07-17T21:17:58.959669
[AUDT: [RSLT (FC32) :SUCS] [TIME (UI64) :246979] [S3AI (CSTR) : "bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"] [
S3AK (CSTR) : "UJXDKKQOXB7YARDS71Q2"] [S3BK (CSTR) : "s3small11"] [S3K
Y (CSTR) : "hello1"] [CBID (UI64) :0x50C4F7AC2BC8EDF7] [CSIZ (UI64) :0
] [AVER (UI32) :10] [ATIM (UI64) :1405631878959669] [ATYP (FC32) :SPUT
] [ANID (UI32) :12872812] [AMID (FC32) :S3RQ] [ATID (UI64) :1579224144
102530435]]
```

Le message d'audit contient des informations sur l'événement en cours d'enregistrement, ainsi que des informations sur le message d'audit lui-même.

Pour identifier l'événement enregistré par le message d'audit, recherchez l'attribut ATYP (mis en évidence ci-dessous) :

```
2014-07-17T21:17:58.959669
[AUDT: [RSLT (FC32) :SUCS] [TIME (UI64) :246979] [S3AI (CSTR) : "bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f" ] [
S3AK (CSTR) : "UJXDKKQOXB7YARDS71Q2" ] [S3BK (CSTR) : "s3small11" ] [S3K
Y (CSTR) : "hello1" ] [CBID (UI64) :0x50C4F7AC2BC8EDF7] [CSIZ (UI64) :0
] [AVER (UI32) :10] [ATIM (UI64) :1405631878959669] [ATYP (FC32) :SP
UT] [ANID (UI32) :12872812] [AMID (FC32) :S3RQ] [ATID (UI64) :1579224
144102530435]]
```

La valeur de l'attribut ATYP est SPUT. "SPUT" Représente une transaction PUT S3, qui consigne l'ingestion d'un objet dans un compartiment.

Le message d'audit suivant indique également le compartiment à partir duquel l'objet est associé :

```
2014-07-17T21:17:58.959669
[AUDT: [RSLT (FC32) :SUCS] [TIME (UI64) :246979] [S3AI (CSTR) : "bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f" ] [
S3AK (CSTR) : "UJXDKKQOXB7YARDS71Q2" ] [S3BK\ (CSTR\ ) : "s3small11"] [S3
KY (CSTR) : "hello1" ] [CBID (UI64) :0x50C4F7AC2BC8EDF7] [CSIZ (UI64) :
0] [AVER (UI32) :10] [ATIM (UI64) :1405631878959669] [ATYP (FC32) :SPU
T] [ANID (UI32) :12872812] [AMID (FC32) :S3RQ] [ATID (UI64) :157922414
4102530435]]
```

Pour savoir quand l'événement PUT s'est produit, notez l'horodatage universel coordonné (UTC) au début du message d'audit. Cette valeur est une version lisible par l'utilisateur de l'attribut ATIM du message d'audit lui-même :

```
2014-07-17T21:17:58.959669
[AUDT: [RSLT (FC32) :SUCS] [TIME (UI64) :246979] [S3AI (CSTR) : "bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f" ] [
S3AK (CSTR) : "UJXDKKQOXB7YARDS71Q2" ] [S3BK (CSTR) : "s3small11" ] [S3K
Y (CSTR) : "hello1" ] [CBID (UI64) :0x50C4F7AC2BC8EDF7] [CSIZ (UI64) :0
] [AVER (UI32) :10] [ATIM\ (UI64\ ) :1405631878959669] [ATYP (FC32) :SP
UT] [ANID (UI32) :12872812] [AMID (FC32) :S3RQ] [ATID (UI64) :15792241
44102530435]]
```

ATIM enregistre le temps, en microsecondes, depuis le début de l'époque UNIX. Dans l'exemple, la valeur 1405631878959669 se traduit par jeudi, 17-Jul-2014 21:17:59 UTC.

## Messages d'audit et cycle de vie de l'objet

## Quand un message d'audit est-il généré ?

Des messages d'audit sont générés à chaque ingestion, récupération ou suppression d'un objet. Vous pouvez identifier ces transactions dans le journal d'audit en localisant les messages d'audit spécifiques à l'API S3.

Les messages d'audit sont liés par des identificateurs spécifiques à chaque protocole.

Protocole	Code
Liaison des opérations S3	S3BK (godet), S3KY (clé), ou les deux
Liaison d'opérations Swift	WCON (conteneur), WOBJ (objet) ou les deux
Liaison des opérations internes	CBID (identifiant interne de l'objet)

### Calendrier des messages d'audit

En raison de facteurs tels que les différences de synchronisation entre les nœuds de la grille, la taille de l'objet et les retards réseau, l'ordre des messages d'audit générés par les différents services peut varier de celui présenté dans les exemples de cette section.

### Transactions d'ingestion d'objets

Vous pouvez identifier les transactions d'ingestion de clients dans le journal d'audit en localisant les messages d'audit spécifiques à l'API S3.

Tous les messages d'audit générés lors d'une transaction d'entrée ne sont pas répertoriés dans les tableaux suivants. Seuls les messages nécessaires au suivi de la transaction d'acquisition sont inclus.

#### Ingestion des messages d'audit S3

Code	Nom	Description	Tracé	Voir
SPUT	Transaction PUT S3	Une transaction d'entrée DE PUT S3 a été effectuée avec succès.	CBID, S3BK, S3KY	"SPUT : PUT S3"
ORLM	Règles d'objet respectées	La politique ILM a été satisfaite pour cet objet.	CBID	"ORLM : règles d'objet respectées"

#### Ingestion des messages d'audit Swift

Code	Nom	Description	Tracé	Voir
WPUT	EFFECTUER la transaction Swift	Une transaction d'entrée DE PUT Swift a été effectuée avec succès.	CBID, WCON, WOBJ	"WPUT : PUT SWIFT"



Code	Nom	Description	Tracé	Voir
ORLM	Règles d'objet respectées	La politique ILM a été satisfaite pour cet objet.	CBID	"ORLM : règles d'objet respectées"

### Exemple : ingestion d'objet S3

La série de messages d'audit ci-dessous est un exemple des messages d'audit générés et enregistrés dans le journal d'audit lorsqu'un client S3 ingère un objet à un nœud de stockage (LDR).

Dans cet exemple, la règle ILM active inclut la règle ILM Make 2 copies.



Tous les messages d'audit générés pendant une transaction ne sont pas répertoriés dans l'exemple ci-dessous. Seules les personnes liées à la transaction de transfert S3 (SPUT) sont répertoriées.

Dans cet exemple, un compartiment S3 a déjà été créé.

### SPUT : PUT S3

Le message SPUT est généré pour indiquer qu'une transaction PUT S3 a été émise pour créer un objet dans un compartiment spécifique.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):25771][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHya1RU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"][S3BK(CSTR):"example"][S3KY(CSTR):"testobject-0-
3"][CBID(UI64):0x8EF52DF8025E63A8][CSIZ(UI64):30720][AVER(UI32):10][ATIM
(UI64):150032627859669][ATYP(FC32):SPUT][ANID(UI32):12086324][AMID(FC32)
:S3RQ][ATID(UI64):14399932238768197038]]
```

### ORLM : règles d'objet respectées

Le message ORLM indique que la politique ILM a été satisfaite pour cet objet. Le message inclut le CBID de l'objet et le nom de la règle ILM appliquée.

Pour les objets répliqués, le champ EMBLEMENTS inclut l'ID de nœud LDR et l'ID de volume des emplacements d'objets.

2019-07-

```
17T21:18:31.230669[AUDT:[CBID(UI64):0x50C4F7AC2BC8EDF7][RULE(CSTR):"Make
2 Copies"][STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"0B344E18-98ED-4F22-
A6C8-A93ED68F8D3F"][LOCS(CSTR):"CLDI 12828634 2148730112, CLDI 12745543
2147552014"][RSLT(FC32):SUCS][AVER(UI32):10][ATYP(FC32):ORLM][ATIM(UI64)
:1563398230669][ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID
(FC32):BCMS]]
```

Pour les objets avec code d'effacement, le champ EMLACEMENTS inclut l'ID du profil de code d'effacement et l'ID du groupe de codes d'effacement

2019-02-23T01:52:54.647537

```
[AUDT:[CBID(UI64):0xFA8ABE5B5001F7E2][RULE(CSTR):"EC_2_plus_1"][STAT(FC32)
:DONE][CSIZ(UI64):10000][UUID(CSTR):"E291E456-D11A-4701-8F51-
D2F7CC9AFECA"][LOCS(CSTR):"CLEC 1 A471E45D-A400-47C7-86AC-
12E77F229831"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1550929974537]\[
ATYP(FC32):ORLM][ANID(UI32):12355278][AMID(FC32):ILMX][ATID(UI64):41685
59046473725560]]
```

Le champ CHEMIN d'ACCÈS inclut des informations clés et un compartiment S3 ou des informations sur le conteneur Swift et l'objet, selon l'API utilisée.

2019-09-15.txt:2018-01-24T13:52:54.131559

```
[AUDT:[CBID(UI64):0x82704DFA4C9674F4][RULE(CSTR):"Make 2
Copies"][STAT(FC32):DONE][CSIZ(UI64):3145729][UUID(CSTR):"8C1C9CAC-22BB-
4880-9115-
CE604F8CE687"][PATH(CSTR):"frisbee_Bucket1/GridDataTests151683676324774_1_
1vf9d"][LOCS(CSTR):"CLDI 12525468, CLDI
12222978"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1568555574559][ATYP(
FC32):ORLM][ANID(UI32):12525468][AMID(FC32):OBDI][ATID(UI64):3448338865383
69336]]
```

### Transactions de suppression d'objet

Vous pouvez identifier les transactions de suppression d'objets dans le journal d'audit en localisant les messages d'audit spécifiques à l'API S3.

Tous les messages d'audit générés lors d'une opération de suppression ne sont pas répertoriés dans les tableaux suivants. Seuls les messages requis pour suivre la transaction de suppression sont inclus.

#### S3 supprime les messages d'audit

Code	Nom	Description	Tracé	Voir
SDEL	Suppression S3	Demande de suppression de l'objet d'un compartiment.	CBID, S3KY	"SDEL : SUPPRESSION S3"

#### Supprimez les messages d'audit Swift

Code	Nom	Description	Tracé	Voir
WDEL	Suppression Swift	Demande de suppression de l'objet d'un conteneur ou du conteneur.	CBID, WOBJ	"WDEL : SUPPRESSION rapide"

#### Exemple : suppression d'objet S3

Lorsqu'un client S3 supprime un objet d'un nœud de stockage (service LDR), un message d'audit est généré et enregistré dans le journal des audits.



Tous les messages d'audit générés lors d'une opération de suppression ne sont pas répertoriés dans l'exemple ci-dessous. Seules les personnes liées à la transaction de suppression S3 (SDEL) sont répertoriées.

#### SDEL : suppression S3

La suppression d'objet commence lorsque le client envoie une requête DeleteObject à un service LDR. Le message contient le compartiment à partir duquel vous souhaitez supprimer l'objet ainsi que la clé S3 de l'objet, qui permet d'identifier l'objet.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):14316][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHya1RU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity:70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SBA
AC(CSTR):"test"]\[S3BK\CSTR\):"example"\\[S3KY\CSTR\):"testobject-0-
7"\][CBID(UI64):0x339F21C5A6964D89][CSIZ(UI64):30720][AVER(UI32):10][ATI
M(UI64):150032627859669][ATYP(FC32):SDEL][ANID(UI32):12086324][AMID(FC32
):S3RQ][ATID(UI64):4727861330952970593]]
```

#### Transactions de récupération d'objet

Vous pouvez identifier les transactions de récupération d'objets dans le journal d'audit en localisant les messages d'audit spécifiques à l'API S3.

Tous les messages d'audit générés lors d'une transaction de récupération ne sont pas répertoriés dans les tableaux suivants. Seuls les messages requis pour suivre la transaction de récupération sont inclus.

### Messages d'audit de récupération S3

Code	Nom	Description	Tracé	Voir
SGET	OBTENTION S3	Demande de récupération d'un objet à partir d'un compartiment.	CBID, S3BK, S3KY	"SGET : OBTENEZ S3"

### Messages d'audit de récupération Swift

Code	Nom	Description	Tracé	Voir
C'EST PARTI	PROFITEZ-en rapidement	Demande de récupération d'un objet à partir d'un conteneur.	CBID, WCON, WOBJ	"WGET: SWIFT GET"

### Exemple : récupération d'objets S3

Lorsqu'un client S3 récupère un objet à partir d'un nœud de stockage (service LDR), un message d'audit est généré et enregistré dans le journal d'audit.

Notez que tous les messages d'audit générés pendant une transaction ne sont pas répertoriés dans l'exemple ci-dessous. Seules les transactions liées à la transaction de récupération S3 (SGET) sont répertoriées.

### SGET : OBTENEZ S3

La récupération d'objet commence lorsque le client envoie une requête GetObject à un service LDR. Le message contient le compartiment à partir duquel vous pouvez récupérer l'objet ainsi que la clé S3 de l'objet, qui permet d'identifier l'objet.

```
2017-09-20T22:53:08.782605
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):47807][SAIP(IPAD):"10.96.112.26"][S3AI(CSTR):"43979298178977966408"][SACC(CSTR):"s3-account-a"][S3AK(CSTR):"SGKHt7GzEcu0yXhFhT_rL5mep4nJt1w75GBh-O_FEW=="][SUSR(CSTR):"urn:sgws:identity::43979298178977966408:root"][SBAI(CSTR):"43979298178977966408"][SBAC(CSTR):"s3-account-a"]\[S3BK\CSTR\):"bucket-anonymous"\]\[S3KY\CSTR\):"Hello.txt"\][CBID(UI64):0x83D70C6F1F662B02][CSIZ(UI64):12][AVER(UI32):10][ATIM(UI64):1505947988782605]\[ATYP\ (FC32\):SGET\][ANID(UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):17742374343649889669]
]
```

Si la règle de compartiment le permet, un client peut récupérer des objets de façon anonyme ou récupérer des objets à partir d'un compartiment qui est détenu par un autre compte de locataire. Le message d'audit contient des informations sur le compte du propriétaire du compartiment afin que vous puissiez suivre ces demandes anonymes et inter-comptes.

Dans l'exemple de message suivant, le client envoie une requête GetObject pour un objet stocké dans un compartiment dont il n'est pas propriétaire. Les valeurs de SBAI et SBAC enregistrent l'ID et le nom de compte du propriétaire du compartiment, qui diffèrent de l'ID et du nom du compte du locataire enregistré dans S3AI et SACC.

```
2017-09-20T22:53:15.876415
```

```
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):53244][SAIP(IPAD):"10.96.112.26"]\[S3AI\n(CSTR):"17915054115450519830"\]\[SACC(CSTR):"s3-account-b"\][S3AK(CSTR):"SGKHpoblWlP_kBkqSCbTi754Ls8lBUog67I2LlSiUg=="][SUSR(CSTR):"urn:sgws:identity::17915054115450519830:root"]\[SBAI\n(CSTR):"43979298178977966408"\]\[SBAC(CSTR):"s3-account-a"\][S3BK(CSTR):"bucket-anonymous"][S3KY(CSTR):"Hello.txt"][CBID(UI64):0x83D70C6F1F662B02][CSIZ(UI64):12][AVER(UI32):10][ATIM(UI64):1505947995876415][ATYP(FC32):SGET][ANID(UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):6888780247515624902]]
```

### Exemple : S3 Select sur un objet

Lorsqu'un client S3 émet une requête S3 Select sur un objet, des messages d'audit sont générés et enregistrés dans le journal d'audit.

Notez que tous les messages d'audit générés pendant une transaction ne sont pas répertoriés dans l'exemple ci-dessous. Seules les transactions liées à la transaction S3 Select (SelectObjectContent) sont répertoriées.

Chaque requête génère deux messages d'audit : un qui effectue l'autorisation de la requête S3 Select (le champ S3SR est défini sur « SELECT ») et une opération GET standard qui récupère les données du stockage pendant le traitement.

```
2021-11-08T15:35:30.750038
```

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636385730715700][TIME(UI64):29173][SAIP(IPAD):"192.168.7.44"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Tenant1636027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:identity::63147909414576125820:root"]\[SBAI(CSTR):"63147909414576125820"\][SBAC(CSTR):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-05064f74126d"][S3KY(CSTR):"SUB-EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-9F01-4EE7-B133-08842A099628"][CSIZ(UI64):0][S3SR(CSTR):"select"][AVER(UI32):10][ATIM(UI64):1636385730750038][ATYP(FC32):SPOS][ANID(UI32):12601166][AMID(FC32):S3RQ][ATID(UI64):1363009709396895985]]
```

2021-11-08T15:35:32.604886

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636383069486504][TIME(UI64):430690][SAIP(IPAD):"192.168.7.44"][HTRH(CSTR):"{\"x-forwarded-for\": \"unix:\"}"] [S3AI(CSTR):"63147909414576125820"] [SACC(CSTR):"Tenant1636027116"] [S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"] [SUSR(CSTR):"urn:sgws:identity:63147909414576125820:root"] [SBAI(CSTR):"63147909414576125820"] [SBAC(CSTR):"Tenant1636027116"] [S3BK(CSTR):"619c0755-9e38-42e0-a614-05064f74126d"] [S3KY(CSTR):"SUB-EST2020_ALL.csv"] [CBID(UI64):0x0496F0408A721171] [UUID(CSTR):"D64B1A4A-9F01-4EE7-B133-08842A099628"] [CSIZ(UI64):10185581] [MTME(UI64):1636380348695262] [AVER(UI32):10] [ATIM(UI64):1636385732604886] [ATYP(FC32):SGET] [ANID(UI32):12733063] [AMID(FC32):S3RQ] [ATID(UI64):16562288121152341130]]
```

## Messages de mise à jour des métadonnées

Des messages d'audit sont générés lorsqu'un client S3 met à jour les métadonnées d'un objet.

### Messages d'audit de la mise à jour des métadonnées S3

Code	Nom	Description	Tracé	Voir
SUPD	Métadonnées S3 mises à jour	Générées lorsqu'un client S3 met à jour les métadonnées d'un objet ingéré.	CBID, S3KY, HTRH	<a href="#">"SUPD : métadonnées S3 mises à jour"</a>

### Exemple : mise à jour des métadonnées S3

L'exemple illustre la réussite d'une transaction permettant de mettre à jour les métadonnées d'un objet S3 existant.

### SUPD : mise à jour des métadonnées S3

Le client S3 demande (SUPD) de mettre à jour les métadonnées spécifiées (`x-amz-meta-*`) pour l'objet S3 (S3KY). Dans cet exemple, les en-têtes de requête sont inclus dans le champ HTRH car ils ont été configurés comme en-tête de protocole d'audit (**CONFIGURATION > surveillance > Audit et serveur syslog**). Voir ["Configurez les messages d'audit et les destinations des journaux"](#).

```

2017-07-11T21:54:03.157462
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):17631][SAIP(IPAD):"10.96.100.254"]
[HTRH(CSTR):"{\"accept-encoding\": \"identity\", \"authorization\": \"AWS
LIUF17FGJARQHPY2E761:jul/hnZs/uNY+aVvV0lTSYhEGts=\",
\"content-length\": \"0\", \"date\": \"Tue, 11 Jul 2017 21:54:03
GMT\", \"host\": \"10.96.99.163:18082\",
\"user-agent\": \"aws-cli/1.9.20 Python/2.7.6 Linux/3.13.0-119-generic
botocore/1.3.20\",
\"x-amz-copy-source\": \"/testbkt1/testobj1\", \"x-amz-metadata-
directive\": \"REPLACE\", \"x-amz-meta-city\": \"Vancouver\"}"]
[S3AI(CSTR):"20956855414285633225"][SACC(CSTR):"acct1"][S3AK(CSTR):"SGKHyy
v9ZQqWRbJSQc5vI7mgioJwrDplShE02AUaww=="]
[SUSR(CSTR):"urn:sgws:identity::20956855414285633225:root"]
[SBAI(CSTR):"20956855414285633225"][SBAC(CSTR):"acct1"][S3BK(CSTR):"testbk
t1"]
[S3KY(CSTR):"testobj1"][CBID(UI64):0xCB1D5C213434DD48][CSIZ(UI64):10][AVER
(UI32):10]
[ATIM(UI64):1499810043157462][ATYP(FC32):SUPD][ANID(UI32):12258396][AMID(F
C32):S3RQ]
[ATID(UI64):8987436599021955788]]

```

## Messages d'audit

### Descriptions des messages d'audit

Les descriptions détaillées des messages d'audit renvoyés par le système sont répertoriées dans les sections suivantes. Chaque message d'audit est d'abord répertorié dans un tableau qui regroupe les messages associés en fonction de la classe d'activité que le message représente. Ces regroupements sont utiles à la fois pour comprendre les types d'activités auditées et pour sélectionner le type souhaité de filtrage des messages d'audit.

Les messages d'audit sont également répertoriés par ordre alphabétique par leur code à quatre caractères. Cette liste alphabétique vous permet de trouver des informations sur des messages spécifiques.

Les codes à quatre caractères utilisés tout au long de ce chapitre sont les valeurs ATYP trouvées dans les messages d'audit, comme indiqué dans l'exemple de message suivant :

```

2014-07-17T03:50:47.484627
\[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP\
(FC32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265
00603516]]

```

Pour plus d'informations sur la définition des niveaux de messages d'audit, la modification des destinations des journaux et l'utilisation d'un serveur syslog externe pour vos informations d'audit, reportez-vous à la

## Catégories de messages d'audit

### Messages d'audit système

Les messages d'audit appartenant à la catégorie d'audit du système sont utilisés pour les événements liés au système d'audit lui-même, aux États des nœuds de la grille, à l'activité des tâches à l'échelle du système (tâches de la grille) et aux opérations de sauvegarde des services.

Code	Titre et description du message	Voir
ECMC	Fragment de données manquant avec code d'effacement : indique qu'un fragment de données manquant avec code d'effacement a été détecté.	"ECMC : fragment de données avec code d'effacement manquant"
ECOC	Fragment de données avec code d'effacement corrompu : indique qu'un fragment de données avec code d'effacement corrompu a été détecté.	"ECOC : fragment de données avec code d'effacement corrompu"
EN	Échec de l'authentification de sécurité : une tentative de connexion à l'aide du protocole TLS (transport Layer Security) a échoué.	"ETAF : échec de l'authentification de sécurité"
GNRG	Enregistrement GNDS : service mis à jour ou enregistré des informations sur lui-même dans le système StorageGRID.	"GNRG : enregistrement GNDS"
GNUR	Annulation de l'enregistrement du GNDS : un service s'est désinscrit du système StorageGRID.	"GNUR : non-inscription du GNDS"
GTED	Tâche de grille terminée : le service CMN a terminé le traitement de la tâche de grille.	"GTED : tâche de grille terminée"
GTST	Tâche de grille démarrée : le service CMN a commencé à traiter la tâche de grille.	"GTST : tâche de grille démarrée"
GTSU	Tâche de grille soumise : une tâche de grille a été envoyée au service CMN.	"GTSU : tâche de grille soumise"
LLST	Emplacement perdu : ce message d'audit est généré en cas de perte d'un emplacement.	"LLST : emplacement perdu"
OLST	Objet perdu : un objet demandé ne peut pas se trouver dans le système StorageGRID.	"OLST : le système a détecté un objet perdu"
AJOUTER	Désactivation de l'audit de sécurité : l'enregistrement des messages d'audit a été désactivé.	"SADD : désactivation de l'audit de sécurité"



Code	Titre et description du message	Voir
SADE	Activation de l'audit de sécurité : la journalisation des messages d'audit a été restaurée.	"SADE : activation de l'audit de sécurité"
SVRF	Échec de la vérification du magasin d'objets : échec de la vérification d'un bloc de contenu.	"SVRF : échec de la vérification du magasin d'objets"
SVRU	Vérification du magasin d'objets Inconnu : données d'objet inattendues détectées dans le magasin d'objets.	"SVRU : Vérification du magasin d'objets inconnue"
SYSD	Arrêt du nœud : un arrêt a été demandé.	"SYSD : arrêt du nœud"
SYST	Arrêt du nœud : un service a démarré un arrêt normal.	"SYST : arrêt du nœud"
SYSU	Node Start : service démarré, la nature de l'arrêt précédent est indiquée dans le message.	"SYSU : démarrage du nœud"

#### Messages d'audit du stockage objet

Les messages d'audit appartenant à la catégorie d'audit du stockage objet sont utilisés pour les événements liés au stockage et à la gestion d'objets au sein du système StorageGRID. Il s'agit notamment du stockage objet et des récupérations, des transferts entre nœuds grid et nœuds.



Les codes d'audit sont supprimés du produit et de la documentation, car les fonctionnalités sont obsolètes. Si vous rencontrez un code d'audit qui n'est pas répertorié ici, consultez les versions précédentes de cette rubrique pour connaître les versions antérieures de SG. Par exemple "[Messages d'audit du stockage objet StorageGRID 11.8](#)", .

Code	Description	Voir
BROR	Demande de lecture seule du compartiment : un compartiment est entré ou a quitté le mode lecture seule.	"BROR : demande en lecture seule du compartiment"
CBSE	Objet Envoyer fin : l'entité source a terminé une opération de transfert des données nœud-grille vers nœud-grille.	"CBSE : fin de l'envoi de l'objet"
CBRE	Fin de réception de l'objet : l'entité de destination a terminé une opération de transfert des données nœud-grille vers nœud-grille.	"CBRE : fin de la réception de l'objet"

Code	Description	Voir
CGRR	Demande de réplication multigrille : StorageGRID a tenté une opération de réplication multigrille pour répliquer des objets entre des compartiments dans une connexion de fédération de grille.	"CGRR : demande de réplication croisée"
EBDL	Suppression d'un compartiment vide : l'analyse ILM a supprimé un objet d'un compartiment qui supprime tous les objets (opération de compartiment vide).	"EBDL : suppression du compartiment vide"
EBKR	Demande de compartiment vide : un utilisateur a envoyé une demande d'activation ou de désactivation de compartiment vide (c'est-à-dire de supprimer des objets de compartiment ou d'arrêter la suppression d'objets).	"EBKR : demande de godet vide"
BALAYAGE	Validation d'un magasin d'objets : un bloc de contenu a été entièrement stocké et vérifié, et peut désormais être demandé.	"SCMT : demande de validation de magasin d'objets"
SREM	Suppression du magasin d'objets : un bloc de contenu a été supprimé d'un nœud de grille et ne peut plus être demandé directement.	"SREM : Suppression du magasin d'objets"

#### Messages d'audit de lecture du client

Les messages d'audit de lecture du client sont consignés lorsqu'une application client S3 demande la récupération d'un objet.

Code	Description	Utilisé par	Voir
S3SL	Demande S3 Select : enregistre une fin d'étude après le renvoi d'une demande S3 Select au client. Le message S3SL peut inclure des détails de message d'erreur et de code d'erreur. La demande n'a peut-être pas abouti.	Client S3	"S3SL: Demande S3 Select"
SGET	S3 GET : log une transaction réussie pour récupérer un objet ou répertorier les objets dans un compartiment.  <b>Remarque</b> : si la transaction fonctionne sur une sous-ressource, le message d'audit inclura le champ S3SR.	Client S3	"SGET : OBTENEZ S3"
SHEA	TÊTE S3 : consigne une transaction réussie pour vérifier l'existence d'un objet ou d'un compartiment.	Client S3	"SHEA : TÊTE S3"

Code	Description	Utilisé par	Voir
C'EST PARTI	SWIFT GET : log une transaction réussie pour récupérer un objet ou répertorier les objets dans un conteneur.	Client Swift	"WGET: SWIFT GET"
WHEA	SWIFT HEAD : consigne une transaction réussie afin de vérifier l'existence d'un objet ou d'un conteneur.	Client Swift	"WHEA: TÊTE SWIFT"

#### Écrire des messages d'audit client

Les messages d'audit d'écriture du client sont consignés lorsqu'une application client S3 demande de créer ou de modifier un objet.

Code	Description	Utilisé par	Voir
OVWR	Remplacement d'objet : consigne une transaction afin de remplacer un objet par un autre.	Clients S3 et Swift	"OVWR : remplacement d'objet"
SDEL	SUPPRESSION S3 : journal une transaction réussie pour supprimer un objet ou un compartiment.  <b>Remarque</b> : si la transaction fonctionne sur une sous-ressource, le message d'audit inclura le champ S3SR.	Client S3	"SDEL : SUPPRESSION S3"
SPR	POST S3 : consigne une transaction réussie pour restaurer un objet à partir du stockage AWS Glacier vers un pool de stockage cloud.	Client S3	"SPO : BORNE S3"
SPUT	S3 PUT : enregistre la réussite d'une transaction pour créer un nouvel objet ou un compartiment.  <b>Remarque</b> : si la transaction fonctionne sur une sous-ressource, le message d'audit inclura le champ S3SR.	Client S3	"SPUT : PUT S3"
SUPD	Métadonnées S3 mises à jour : enregistre une transaction réussie pour mettre à jour les métadonnées d'un objet ou d'un compartiment.	Client S3	"SUPD : métadonnées S3 mises à jour"
WDEL	SUPPRESSION Swift : enregistre une transaction réussie pour supprimer un objet ou un conteneur.	Client Swift	"WDEL : SUPPRESSION rapide"
WPUT	SWIFT PUT : consigne une transaction réussie pour créer un nouvel objet ou conteneur.	Client Swift	"WPUT : PUT SWIFT"

## Message d'audit de gestion

La catégorie gestion consigne les requêtes utilisateur dans l'API de gestion.

Code	Titre et description du message	Voir
MGAU	Message d'audit de l'API de gestion : journal des demandes utilisateur.	"MGAU : message d'audit de gestion"

## Messages d'audit ILM

Les messages d'audit appartenant à la catégorie d'audit ILM sont utilisés pour les événements liés aux opérations de gestion du cycle de vie des informations (ILM).

Code	Titre et description du message	Voir
IDEL	Suppression initiée de l'ILM : ce message d'audit est généré lorsque l'ILM démarre le processus de suppression d'un objet.	"IDEL : suppression initiée ILM"
LKCU	Nettoyage d'objet écrasé. Ce message d'audit est généré lorsqu'un objet écrasé est automatiquement supprimé pour libérer de l'espace de stockage.	"LKCU : nettoyage d'objet écrasé"
ORLM	Règles objet respectées : ce message d'audit est généré lorsque les données objet sont stockées comme spécifié par les règles ILM.	"ORLM : règles d'objet respectées"

## Référence du message d'audit

### BROR : demande en lecture seule du compartiment

Le service LDR génère ce message d'audit lorsqu'un compartiment passe en mode lecture seule ou quitte ce mode. Par exemple, un compartiment passe en mode lecture seule tandis que tous les objets sont en cours de suppression.

Code	Champ	Description
BKHD	UUID de compartiment	ID du compartiment.
BROV	Valeur de demande de lecture seule du compartiment	Que le compartiment soit en lecture seule ou qu'il quitte l'état en lecture seule (1 = lecture seule, 0 = non-lecture seule).
BROS	Motif de compartiment en lecture seule	Raison pour laquelle le compartiment est en lecture seule ou quitte l'état en lecture seule. Par exemple, emptyBucket.

Code	Champ	Description
S3AI	ID de compte locataire S3	ID du compte de locataire qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Compartiment S3	Nom du compartiment S3.

**CBRB : début de la réception de l'objet**

Dans le cadre d'opérations normales, les blocs de contenu sont transférés en continu entre différents nœuds lorsque des données sont accessibles, répliquées et conservées. Lorsque le transfert d'un bloc de contenu d'un nœud à un autre est lancé, ce message est émis par l'entité de destination.

Code	Champ	Description
CNID	Identificateur de connexion	Identifiant unique de la session/connexion nœud à nœud.
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu en cours de transfert.
CTDR	Direction de transfert	Indique si le transfert CBID a été initié par Push ou par Pull :  PUSH : l'opération de transfert a été demandée par l'entité émettrice.  EXTRACTION : l'opération de transfert a été demandée par l'entité destinataire.
CTSR	Entité source	ID de nœud de la source (expéditeur) du transfert CBID.
CTD	Entité de destination	ID de nœud de la destination (récepteur) du transfert CBID.
CTSS	Nombre de séquences de début	Indique le premier nombre de séquences demandé. En cas de réussite, le transfert commence à partir de ce nombre de séquences.
CTE	Nombre de séquences de fin prévu	Indique le dernier nombre de séquences demandé. En cas de réussite, le transfert est considéré comme terminé lorsque ce nombre de séquences a été reçu.
RSLT	Statut de début du transfert	État au moment du démarrage du transfert :  CMC : le transfert a démarré avec succès.

Ce message d'audit signifie qu'une opération de transfert de données nœud à nœud a été lancée sur un seul élément de contenu, tel qu'identifié par son identificateur de bloc de contenu. L'opération demande des

données de « nombre de séquences de début » à « nombre de séquences de fin attendu ». Les nœuds d'envoi et de réception sont identifiés par leurs ID de nœud. Ces informations peuvent être utilisées pour suivre le flux de données du système et lorsqu'elles sont associées à des messages d'audit de stockage, pour vérifier le nombre de répliques.

**CBRE : fin de la réception de l'objet**

Lorsque le transfert d'un bloc de contenu d'un nœud à un autre est terminé, ce message est émis par l'entité de destination.

Code	Champ	Description
CNID	Identificateur de connexion	Identifiant unique de la session/connexion nœud à nœud.
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu en cours de transfert.
CTDR	Direction de transfert	Indique si le transfert CBID a été initié par Push ou par Pull :  PUSH : l'opération de transfert a été demandée par l'entité émettrice.  EXTRACTION : l'opération de transfert a été demandée par l'entité destinataire.
CTSR	Entité source	ID de nœud de la source (expéditeur) du transfert CBID.
CTD	Entité de destination	ID de nœud de la destination (récepteur) du transfert CBID.
CTSS	Nombre de séquences de début	Indique le nombre de séquences sur lesquelles le transfert a démarré.
CTAS	Nombre de séquences de fin réelles	Indique que le dernier nombre de séquences a été transféré avec succès. Si le nombre de séquences de fin réelles est le même que le nombre de séquences de début et que le résultat du transfert n'a pas réussi, aucune donnée n'a été échangée.

Code	Champ	Description
RSLT	Résultat du transfert	Résultat de l'opération de transfert (du point de vue de l'entité émettrice) :  SUC : transfert terminé avec succès ; tous les comptes de séquence demandés ont été envoyés.  CONL : connexion perdue pendant le transfert  CTMO : expiration de la connexion pendant l'établissement ou le transfert  UNRE : ID de nœud de destination inaccessible  CRPT : transfert terminé en raison de la réception de données corrompues ou non valides

Ce message d'audit signifie qu'une opération de transfert des données nœud à nœud est terminée. Si le résultat du transfert a réussi, l'opération a transféré les données de « nombre de séquences de début » à « nombre de séquences de fin réelles ». Les nœuds d'envoi et de réception sont identifiés par leurs ID de nœud. Ces informations peuvent être utilisées pour suivre le flux de données système et pour localiser, tabuler et analyser les erreurs. Lorsqu'il est associé à des messages d'audit du stockage, il peut également être utilisé pour vérifier le nombre de répliques.

#### **CBSB : début de l'envoi de l'objet**

Dans le cadre d'opérations normales, les blocs de contenu sont transférés en continu entre différents nœuds lorsque des données sont accessibles, répliquées et conservées. Lorsque le transfert d'un bloc de contenu d'un nœud à un autre est lancé, ce message est émis par l'entité source.

Code	Champ	Description
CNID	Identificateur de connexion	Identifiant unique de la session/connexion nœud à nœud.
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu en cours de transfert.
CTDR	Direction de transfert	Indique si le transfert CBID a été initié par Push ou par Pull :  PUSH : l'opération de transfert a été demandée par l'entité émettrice.  EXTRACTION : l'opération de transfert a été demandée par l'entité destinataire.
CTSR	Entité source	ID de nœud de la source (expéditeur) du transfert CBID.
CTD	Entité de destination	ID de nœud de la destination (récepteur) du transfert CBID.

Code	Champ	Description
CTSS	Nombre de séquences de début	Indique le premier nombre de séquences demandé. En cas de réussite, le transfert commence à partir de ce nombre de séquences.
CTE	Nombre de séquences de fin prévu	Indique le dernier nombre de séquences demandé. En cas de réussite, le transfert est considéré comme terminé lorsque ce nombre de séquences a été reçu.
RSLT	Statut de début du transfert	État au moment du démarrage du transfert :  CMC : le transfert a démarré avec succès.

Ce message d'audit signifie qu'une opération de transfert de données nœud à nœud a été lancée sur un seul élément de contenu, tel qu'identifié par son identificateur de bloc de contenu. L'opération demande des données de « nombre de séquences de début » à « nombre de séquences de fin attendu ». Les nœuds d'envoi et de réception sont identifiés par leurs ID de nœud. Ces informations peuvent être utilisées pour suivre le flux de données du système et lorsqu'elles sont associées à des messages d'audit de stockage, pour vérifier le nombre de répliques.

#### CBSE : fin de l'envoi de l'objet

Lorsque le transfert d'un bloc de contenu d'un nœud à un autre est terminé, ce message est émis par l'entité source.

Code	Champ	Description
CNID	Identificateur de connexion	Identifiant unique de la session/connexion nœud à nœud.
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu en cours de transfert.
CTDR	Direction de transfert	Indique si le transfert CBID a été initié par Push ou par Pull :  PUSH : l'opération de transfert a été demandée par l'entité émettrice.  EXTRACTION : l'opération de transfert a été demandée par l'entité destinataire.
CTSR	Entité source	ID de nœud de la source (expéditeur) du transfert CBID.
CTD	Entité de destination	ID de nœud de la destination (récepteur) du transfert CBID.
CTSS	Nombre de séquences de début	Indique le nombre de séquences sur lesquelles le transfert a démarré.



Code	Champ	Description
CTAS	Nombre de séquences de fin réelles	Indique que le dernier nombre de séquences a été transféré avec succès. Si le nombre de séquences de fin réelles est le même que le nombre de séquences de début et que le résultat du transfert n'a pas réussi, aucune donnée n'a été échangée.
RSLT	Résultat du transfert	Résultat de l'opération de transfert (du point de vue de l'entité émettrice) :  SUC : transfert terminé avec succès ; tous les comptes de séquence demandés ont été envoyés.  CONL : connexion perdue pendant le transfert  CTMO : expiration de la connexion pendant l'établissement ou le transfert  UNRE : ID de nœud de destination inaccessible  CRPT : transfert terminé en raison de la réception de données corrompues ou non valides

Ce message d'audit signifie qu'une opération de transfert des données nœud à nœud est terminée. Si le résultat du transfert a réussi, l'opération a transféré les données de « nombre de séquences de début » à « nombre de séquences de fin réelles ». Les nœuds d'envoi et de réception sont identifiés par leurs ID de nœud. Ces informations peuvent être utilisées pour suivre le flux de données système et pour localiser, tabuler et analyser les erreurs. Lorsqu'il est associé à des messages d'audit du stockage, il peut également être utilisé pour vérifier le nombre de répliques.

#### **CGRR : demande de réplication croisée**

Ce message est généré lorsque StorageGRID tente une opération de réplication multigrille pour répliquer des objets entre des compartiments dans une connexion de fédération de grille.

Code	Champ	Description
CSIZ	Taille de l'objet	Taille de l'objet en octets.  L'attribut CSIZ a été introduit dans StorageGRID 11.8. Par conséquent, les requêtes de réplication multigrille couvrant une mise à niveau StorageGRID 11.7 à 11.8 peuvent avoir une taille d'objet totale inexacte.
S3AI	ID de compte locataire S3	ID du compte de locataire qui détient le compartiment à partir duquel l'objet est répliqué.
GFID	ID de connexion de fédération de grille	ID de la connexion de fédération de grille utilisée pour la réplication inter-grille.

Code	Champ	Description
OPER	Opération CGR	Type d'opération de réplication inter-grille qui a été tentée : <ul style="list-style-type: none"> <li>• 0 = objet répliqué</li> <li>• 1 = objet multi pièce répliqué</li> <li>• 2 = marqueur de suppression répliqué</li> </ul>
S3BK	Compartiment S3	Nom du compartiment S3.
S3KY	Clé S3	Le nom de la clé S3 n'inclut pas le nom du compartiment.
VSID	ID de version	ID de version de la version spécifique d'un objet en cours de réplication.
RSLT	Code de résultat	Renvoie réussi (SUCS) ou erreur générale (GERR).

#### EBDL : suppression du compartiment vide

Le scanner ILM a supprimé un objet d'un compartiment qui supprime tous les objets (en cours d'exécution d'une opération de compartiment vide).

Code	Champ	Description
CSIZ	Taille de l'objet	Taille de l'objet en octets.
CHEMIN	Compartiment/clé S3	Nom du compartiment S3 et nom de la clé S3.
SEGC	UUID du conteneur	UUID du conteneur pour l'objet segmenté. Cette valeur n'est disponible que si l'objet est segmenté.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
RSLT	Résultat de l'opération de suppression	Résultat de l'événement, du processus ou de la transaction. Si n'est pas pertinent pour un message, AUCUN n'est utilisé plutôt que LES CMC pour que le message ne soit pas filtré accidentellement.

#### EBKR : demande de godet vide

Ce message indique qu'un utilisateur a envoyé une demande d'activation ou de désactivation de compartiment vide (c'est-à-dire de supprimer des objets de compartiment ou d'arrêter de supprimer des objets).

Code	Champ	Description
BUID	UUID de compartiment	ID du compartiment.
EBJS	Configuration JSON de compartiment vide	Contient le fichier JSON représentant la configuration de compartiment vide actuelle.
S3AI	ID de compte locataire S3	ID de compte de locataire de l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Compartiment S3	Nom du compartiment S3.

**ECMC : fragment de données avec code d'effacement manquant**

Ce message d'audit indique que le système a détecté un fragment de données avec code d'effacement manquant.

Code	Champ	Description
VCMC	ID VCS	Nom du VCS contenant le bloc manquant.
CODE DE DIAGNOSTIC	ID de bloc	Identifiant du fragment avec code d'effacement manquant.
RSLT	Résultat	Ce champ a la valeur 'NONE'. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message particulier. 'AUCUN' est utilisé plutôt que 'UCS' pour que ce message ne soit pas filtré.

**ECOC : fragment de données avec code d'effacement corrompu**

Ce message d'audit indique que le système a détecté un fragment de données codé par effacement corrompu.

Code	Champ	Description
VCCO	ID VCS	Nom du VCS contenant le bloc corrompu.
VLID	ID du volume	Volume RangeDB contenant le fragment codé d'effacement corrompu.
CCID	ID de bloc	Identificateur du fragment codé d'effacement corrompu.

Code	Champ	Description
RSLT	Résultat	Ce champ a la valeur 'NONE'. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message particulier. 'AUCUN' est utilisé plutôt que 'UCS' pour que ce message ne soit pas filtré.

**ETAF : échec de l'authentification de sécurité**

Ce message est généré lorsqu'une tentative de connexion avec TLS (transport Layer Security) a échoué.

Code	Champ	Description
CNID	Identificateur de connexion	Identifiant système unique pour la connexion TCP/IP sur laquelle l'authentification a échoué.
RUID	Identité de l'utilisateur	Identifiant dépendant du service représentant l'identité de l'utilisateur distant.
RSLT	Code de motif	<p>La raison de l'échec :</p> <p>SCNI : échec de l'établissement de connexion sécurisée.</p> <p>CERM : certificat manquant.</p> <p>CERT : le certificat n'était pas valide.</p> <p>CERE: Le certificat a expiré.</p> <p>CERR : le certificat a été révoqué.</p> <p>CSGN : la signature du certificat n'est pas valide.</p> <p>CSGU : le signataire de certificat était inconnu.</p> <p>UCRM : les informations d'identification de l'utilisateur étaient manquantes.</p> <p>UCRI : les informations d'identification de l'utilisateur étaient incorrectes.</p> <p>UCRU : les informations d'identification de l'utilisateur ont été interdites.</p> <p>TOUT : expiration du délai d'authentification.</p>

Lorsqu'une connexion est établie à un service sécurisé qui utilise TLS, les informations d'identification de l'entité distante sont vérifiées à l'aide du profil TLS et de la logique supplémentaire intégrée au service. Si cette authentification échoue en raison de certificats ou d'informations d'identification non valides, inattendus ou interdits, un message d'audit est consigné. Cela permet de rechercher des tentatives d'accès non autorisées et d'autres problèmes de connexion liés à la sécurité.

Le message peut être dû à une entité distante ayant une configuration incorrecte ou à des tentatives de

présentation d'informations d'identification non valides ou interdites au système. Ce message d'audit doit être surveillé pour détecter les tentatives d'accès non autorisé au système.

#### **GNRG : enregistrement GNDS**

Le service CMN génère ce message d'audit lorsqu'un service a mis à jour ou enregistré des informations sur lui-même dans le système StorageGRID.

<b>Code</b>	<b>Champ</b>	<b>Description</b>
RSLT	Résultat	Résultat de la demande de mise à jour : <ul style="list-style-type: none"><li>• CMC : réussi</li><li>• SUNV : service non disponible</li><li>• GERR : autre panne</li></ul>
GNID	ID du nœud	ID de nœud du service qui a lancé la demande de mise à jour.
Gntp	Type de périphérique	Type de périphérique du nœud de grid (par exemple BLDR pour un service LDR).
GNDV	Version du modèle de périphérique	Chaîne identifiant la version du modèle de terminal du nœud de grille dans le bundle DMDL.
GNP	Groupe	Groupe auquel appartient le nœud de la grille (dans le contexte des coûts de lien et du classement des requêtes de service).
GNIA	Adresse IP	Adresse IP du nœud de la grille.

Ce message est généré chaque fois qu'un nœud de la grille met à jour son entrée dans le pack Grid Nodes.

#### **GNUR : non-inscription du GNDS**

Le service CMN génère ce message d'audit lorsqu'un service a des informations non enregistrées sur lui-même à partir du système StorageGRID.

<b>Code</b>	<b>Champ</b>	<b>Description</b>
RSLT	Résultat	Résultat de la demande de mise à jour : <ul style="list-style-type: none"><li>• CMC : réussi</li><li>• SUNV : service non disponible</li><li>• GERR : autre panne</li></ul>
GNID	ID du nœud	ID de nœud du service qui a lancé la demande de mise à jour.

**GTED : tâche de grille terminée**

Ce message d'audit indique que le service CMN a terminé le traitement de la tâche de grille spécifiée et a déplacé la tâche vers la table Historique. Si le résultat est SUC, ABRT ou ROLF, un message d'audit correspondant à la tâche de grille démarrée sera affiché. Les autres résultats indiquent que le traitement de cette tâche de grille n'a jamais démarré.

Code	Champ	Description
2	ID de tâche	<p>Ce champ identifie de manière unique une tâche de grille générée et permet de gérer la tâche de grille tout au long de son cycle de vie.</p> <p><b>Remarque :</b> l'ID de tâche est attribué au moment où une tâche de grille est générée, et non au moment où elle est soumise. Une tâche de grille donnée peut être soumise plusieurs fois. Dans ce cas, le champ ID tâche n'est pas suffisant pour lier de manière unique les messages d'audit soumis, lancés et terminés.</p>
RSLT	Résultat	<p>Résultat de l'état final de la tâche de grille :</p> <ul style="list-style-type: none"><li>• SUC : la tâche de grille s'est terminée avec succès.</li><li>• ABRT : la tâche de grille a été interrompue sans erreur de retour arrière.</li><li>• ROLF : la tâche de grille a été interrompue et n'a pas pu terminer le processus de restauration.</li><li>• ANNUL : la tâche de grille a été annulée par l'utilisateur avant son démarrage.</li><li>• EXPR : la tâche de grille a expiré avant son démarrage.</li><li>• IVLD : la tâche de grille n'était pas valide.</li><li>• AUTH : la tâche de grille n'était pas autorisée.</li><li>• DUPL : la tâche de grille a été rejetée en double.</li></ul>

**GTST : tâche de grille démarrée**

Ce message d'audit indique que le service CMN a commencé à traiter la tâche de grille spécifiée. Le message d'audit suit immédiatement le message de la tâche de grille soumise pour les tâches de grille initiées par le service interne Grid Task Submission et sélectionnées pour l'activation automatique. Pour les tâches de grille soumises dans la table en attente, ce message est généré lorsque l'utilisateur démarre la tâche de grille.

Code	Champ	Description
2	ID de tâche	Ce champ identifie de manière unique une tâche de grille générée et permet de gérer la tâche tout au long de son cycle de vie.  <b>Remarque</b> : l'ID de tâche est attribué au moment où une tâche de grille est générée, et non au moment où elle est soumise. Une tâche de grille donnée peut être soumise plusieurs fois. Dans ce cas, le champ ID tâche n'est pas suffisant pour lier de manière unique les messages d'audit soumis, lancés et terminés.
RSLT	Résultat	Résultat. Ce champ n'a qu'une seule valeur :  • SUC : la tâche de grille a été démarrée avec succès.

#### GTSU : tâche de grille soumise

Ce message d'audit indique qu'une tâche de grille a été envoyée au service CMN.

Code	Champ	Description
2	ID de tâche	Identifie de manière unique une tâche de grille générée et permet de gérer la tâche tout au long de son cycle de vie.  <b>Remarque</b> : l'ID de tâche est attribué au moment où une tâche de grille est générée, et non au moment où elle est soumise. Une tâche de grille donnée peut être soumise plusieurs fois. Dans ce cas, le champ ID tâche n'est pas suffisant pour lier de manière unique les messages d'audit soumis, lancés et terminés.
TTYP	Type de tâche	Type de tâche de grille.
VER	Version de la tâche	Numéro indiquant la version de la tâche de grille.
TDSC	Description de la tâche	Description lisible par l'homme de la tâche de grille.
CUVES	Valide après horodatage	La première fois (UINT64 microsecondes à partir du 1er janvier 1970 - heure UNIX) à laquelle la tâche de grille est valide.
VBTS	Valide avant horodatage	Dernière heure (UINT64 microsecondes à partir du 1er janvier 1970 - heure UNIX) à laquelle la tâche de grille est valide.

Code	Champ	Description
TSRC	Source	Source de la tâche : <ul style="list-style-type: none"> <li>• TXTB : la tâche de grille a été soumise via le système StorageGRID sous forme de bloc de texte signé.</li> <li>• GRILLE : la tâche de grille a été soumise via le service de soumission de tâches Grid interne.</li> </ul>
ACTV	Type d'activation	Type d'activation : <ul style="list-style-type: none"> <li>• AUTO : la tâche de grille a été soumise pour l'activation automatique.</li> <li>• PEND : la tâche de grille a été envoyée dans la table en attente. C'est la seule possibilité pour la source TXTB.</li> </ul>
RSLT	Résultat	Résultat de la soumission : <ul style="list-style-type: none"> <li>• SUC : la tâche de grille a été envoyée avec succès.</li> <li>• ECHEC : la tâche a été déplacée directement vers la table historique.</li> </ul>

#### IDEL : suppression initiée ILM

Ce message est généré lorsque ILM démarre le processus de suppression d'un objet.

Le message IDEL est généré dans l'une ou l'autre des situations suivantes :

- **Pour les objets dans des compartiments S3 conformes** : ce message est généré lorsque ILM démarre le processus de suppression automatique d'un objet parce que sa période de conservation a expiré (en supposant que le paramètre de suppression automatique est activé et que la conservation légale est désactivée).
- **Pour les objets dans les compartiments S3 non conformes**. Ce message est généré lorsque ILM démarre le processus de suppression d'un objet, car aucune instruction de placement dans les règles ILM actives ne s'applique actuellement à cet objet.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	CBID de l'objet.
CMPA	Conformité : suppression automatique	Pour les objets des compartiments S3 uniquement. 0 (false) ou 1 (true), indiquant si un objet conforme doit être supprimé automatiquement à la fin de sa période de conservation, à moins que le compartiment ne soit soumis à une conservation légale.
CMPL	Conformité : obligation légale	Pour les objets des compartiments S3 uniquement. 0 (faux) ou 1 (vrai), indiquant si le godet est actuellement en attente légale.



Code	Champ	Description
CMPR	Conformité : période de conservation	Pour les objets des compartiments S3 uniquement. Durée de conservation de l'objet en minutes.
CTME	Conformité : temps d'entrée	Pour les objets des compartiments S3 uniquement. Temps d'ingestion de l'objet. Vous pouvez ajouter la période de conservation en minutes à cette valeur pour déterminer quand l'objet peut être supprimé du compartiment.
DMRM	Supprimer l'ID de version de marqueur	ID de version du marqueur de suppression créé lors de la suppression d'un objet d'un compartiment multiversion. Les opérations sur les compartiments n'incluent pas ce champ.
CSIZ	Taille du contenu	Taille de l'objet en octets.
EMPLACEMENT S	Emplacements	L'emplacement de stockage des données d'objet dans le système StorageGRID. La valeur des EMBLEMACEMENTS est "" si l'objet n'a pas d'emplacement (par exemple, il a été supprimé).  CLEC : pour les objets avec code d'effacement, l'ID de profil de code d'effacement et l'ID de groupe de codes d'effacement appliqués aux données de l'objet.  CLDI : pour les objets répliqués, l'ID de nœud LDR et l'ID de volume de l'emplacement de l'objet.  CLNL : ID de nœud D'ARC de l'emplacement de l'objet si les données de l'objet sont archivées.
CHEMIN	Compartiment/cl é S3	Nom du compartiment S3 et nom de la clé S3.
RSLT	Résultat	Résultat de l'opération ILM.  SUC : l'opération ILM a réussi.
RÈGLE	Libellé de règles	<ul style="list-style-type: none"> <li>• Si un objet d'un compartiment S3 conforme est supprimé automatiquement car sa période de conservation a expiré, ce champ est vide.</li> <li>• Si l'objet est supprimé car il n'y a plus d'instructions de placement qui s'appliquent actuellement à l'objet, ce champ affiche l'étiquette lisible par l'homme de la dernière règle ILM appliquée à l'objet.</li> </ul>
SGRP	Site (groupe)	S'il est présent, l'objet a été supprimé sur le site spécifié, ce qui n'est pas le site où l'objet a été ingéré.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.

Code	Champ	Description
VSID	ID de version	ID de version de la version spécifique d'un objet qui a été supprimé. Les opérations sur les compartiments et les objets dans les compartiments non versionnés n'incluent pas ce champ.

#### LKCU : nettoyage d'objet écrasé

Ce message est généré lorsque StorageGRID supprime un objet écrasé qui auparavant requiert un nettoyage pour libérer de l'espace de stockage. Un objet est écrasé lorsqu'un client S3 écrit un objet dans un chemin qui contient déjà un objet. Le processus de suppression se produit automatiquement et en arrière-plan.

Code	Champ	Description
CSIZ	Taille du contenu	Taille de l'objet en octets.
LTYP	Type de nettoyage	<i>Usage interne uniquement.</i>
LUID	UUID d'objet supprimé	Identifiant de l'objet qui a été supprimé.
CHEMIN	Compartiment/clé S3	Nom du compartiment S3 et nom de la clé S3.
SEGC	UUID du conteneur	UUID du conteneur pour l'objet segmenté. Cette valeur n'est disponible que si l'objet est segmenté.
UUID	Identifiant unique universel	Identifiant de l'objet qui existe toujours. Cette valeur est disponible uniquement si l'objet n'a pas été supprimé.

#### LKDM : nettoyage d'objets fuyée

Ce message est généré lorsqu'un morceau qui fuit a été nettoyé ou supprimé. Un bloc peut faire partie d'un objet répliqué ou d'un objet avec code d'effacement.

Code	Champ	Description
CLOC	Emplacement des blocs	Le chemin du fichier du morceau qui a fui et qui a été supprimé.
CTYP	Type de bloc	Type de bloc :  ec: Erasure-coded object chunk  repl: Replicated object chunk

Code	Champ	Description
LTyp	Type de fuite	Les cinq types de fuites pouvant être détectés :  object_leaked: Object doesn't exist in the grid  location_leaked: Object exists in the grid, but found location doesn't belong to object  mup_seg_leaked: Multipart upload was stopped or not completed, and the segment/part was left out  segment_leaked: Parent UUID/CBID (associated container object) is valid but doesn't contain this segment  no_parent: Container object is deleted, but object segment was left out and not deleted
CTIM	Temps de création des blocs	Heure à laquelle le morceau de fuite a été créé.
UUID	Identifiant unique universel	Identifiant de l'objet auquel appartient le bloc.
CBID	Identificateur du bloc de contenu	CBID de l'objet auquel appartient le segment divulgué.
CSIZ	Taille du contenu	Taille du bloc en octets.

#### LLST : emplacement perdu

Ce message est généré chaque fois qu'un emplacement pour une copie d'objet (répliquée ou avec code d'effacement) est introuvable.

Code	Champ	Description
BIL	CBID	CBID affecté.
ECPR	Profil de codage d'effacement	Pour les données d'objet avec code d'effacement. ID du profil de code d'effacement utilisé.
LTyp	Type d'emplacement	CLDI (Online) : pour les données d'objet répliquées  CLEC (en ligne) : pour les données d'objet avec code d'effacement  CLNL (Nearline) : pour les données d'objets répliqués archivés

Code	Champ	Description
NON	ID de nœud source	ID de nœud sur lequel les emplacements ont été perdus.
PCLD	Chemin d'accès à l'objet répliqué	Chemin complet vers l'emplacement du disque des données de l'objet perdu. Renvoyé uniquement lorsque LTYP a une valeur CLDI (c'est-à-dire pour les objets répliqués).  Prend le formulaire <code>/var/local/rangedb/2/p/13/13/00oJs6X%{h{U)SeUFxE@</code>
RSLT	Résultat	Toujours AUCUNE. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message. AUCUN n'est utilisé plutôt que LES CMC pour que ce message ne soit pas filtré.
TSRC	Déclenchement de la source	UTILISATEUR : utilisateur déclenché  SYST : déclenchement du système
UUID	ID universel unique	Identifiant de l'objet affecté dans le système StorageGRID.

#### MG AU : message d'audit de gestion

La catégorie gestion consigne les requêtes utilisateur dans l'API de gestion. Chaque requête HTTP qui n'est pas une requête GET ou HEAD à un URI d'API valide consigne une réponse contenant le nom d'utilisateur, l'adresse IP et le type de requête à l'API. Les URI d'API non valides (tels que /api/v3-Authorise) et les demandes non valides d'URI d'API valides ne sont pas consignés.

Code	Champ	Description
MDIP	Adresse IP de destination	Adresse IP du serveur (destination).
ADNM	Nom de domaine	Nom du domaine hôte.
MPAT	CHEMIN de la demande	Le chemin de la demande.
MPQP	Paramètres de requête	Paramètres de requête pour la demande.

Code	Champ	Description
MBD	Corps de la demande	<p>Le contenu de l'organisme de demande. Lorsque le corps de réponse est enregistré par défaut, le corps de la demande est enregistré dans certains cas lorsque le corps de réponse est vide. Comme les informations suivantes ne sont pas disponibles dans le corps de réponse, elles sont extraites du corps de la demande pour les méthodes SUIVANTES :</p> <ul style="list-style-type: none"> <li>• Nom d'utilisateur et ID de compte dans <b>POST Authorise</b></li> <li>• Nouvelle configuration de sous-réseaux dans <b>POST /grid/grid-Networks/update</b></li> <li>• Nouveaux serveurs NTP dans <b>POST /grid/ntp-servers/update</b></li> <li>• ID de serveur déclassés dans <b>POST /grid/serveurs/désaffecter</b></li> </ul> <p><b>Remarque</b> : les informations sensibles sont soit supprimées (par exemple, une clé d'accès S3), soit masquées par des astérisques (par exemple, un mot de passe).</p>
MMD	Méthode de demande	<p>La méthode de requête HTTP :</p> <ul style="list-style-type: none"> <li>• POST</li> <li>• EN</li> <li>• SUPPRIMER</li> <li>• CORRECTIF</li> </ul>
MRSC	Code de réponse	Le code de réponse.
MRSP	Corps de réponse	<p>Le contenu de la réponse (le corps de réponse) est consigné par défaut.</p> <p><b>Remarque</b> : les informations sensibles sont soit supprimées (par exemple, une clé d'accès S3), soit masquées par des astérisques (par exemple, un mot de passe).</p>
MSIP	Adresse IP source	Adresse IP du client (source).
UUUN	URN utilisateur	URN (nom de ressource uniforme) de l'utilisateur qui a envoyé la demande.
RSLT	Résultat	Renvoie réussi (CS) ou l'erreur signalée par le back-end.

**OLST** : le système a détecté un objet perdu

Ce message est généré lorsque le service DDS ne trouve aucune copie d'un objet dans le système StorageGRID.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	CBID de l'objet perdu.
NON	ID du nœud	S'il est disponible, dernier emplacement direct ou proche de la ligne connue de l'objet perdu. Il est possible d'avoir uniquement l'ID de nœud sans ID de volume si les informations sur le volume ne sont pas disponibles.
CHEMIN	Compartiment/clé S3	S'il est disponible, le nom du compartiment S3 et le nom de la clé S3.
RSLT	Résultat	Ce champ a la valeur AUCUNE. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message. AUCUN n'est utilisé plutôt que LES CMC pour que ce message ne soit pas filtré.
UUID	ID universel unique	Identificateur de l'objet perdu dans le système StorageGRID.
VOLI	ID du volume	S'il est disponible, l'ID de volume du nœud de stockage pour le dernier emplacement connu de l'objet perdu.

#### ORLM : règles d'objet respectées

Ce message est généré lorsque l'objet est stocké et copié comme spécifié par les règles ILM.



Le message ORLM n'est pas généré lorsqu'un objet est stocké avec succès par la règle de création de 2 copies par défaut si une autre règle de la stratégie utilise le filtre avancé taille d'objet.

Code	Champ	Description
BUID	Cueilleur de godet	Champ ID de compartiment. Utilisé pour les opérations internes. S'affiche uniquement si STAT est PRGD.
CBID	Identificateur du bloc de contenu	CBID de l'objet.
CSIZ	Taille du contenu	Taille de l'objet en octets.

Code	Champ	Description
EMPLACEMENT S	Emplacements	<p>L'emplacement de stockage des données d'objet dans le système StorageGRID. La valeur des EMBLEMENTS est "" si l'objet n'a pas d'emplacement (par exemple, il a été supprimé).</p> <p>CLEC : pour les objets avec code d'effacement, l'ID de profil de code d'effacement et l'ID de groupe de codes d'effacement appliqués aux données de l'objet.</p> <p>CLDI : pour les objets répliqués, l'ID de nœud LDR et l'ID de volume de l'emplacement de l'objet.</p> <p>CLNL : ID de nœud D'ARC de l'emplacement de l'objet si les données de l'objet sont archivées.</p>
CHEMIN	Compartiment/clé S3	Nom du compartiment S3 et nom de la clé S3.
RSLT	Résultat	<p>Résultat de l'opération ILM.</p> <p>SUC : l'opération ILM a réussi.</p>
RÈGLE	Libellé de règles	Étiquette lisible par l'homme donnée à la règle ILM appliquée à cet objet.
SEGC	UUID du conteneur	UUID du conteneur pour l'objet segmenté. Cette valeur n'est disponible que si l'objet est segmenté.
SGCB	CBID du conteneur	CBID du conteneur pour l'objet segmenté. Cette valeur n'est disponible que pour les objets segmentés et partitionnés.
URGENCE	État	<p>État de l'opération ILM.</p> <p>L'OPÉRATION ILM est terminée pour l'objet.</p> <p>DFER: L'objet a été marqué pour une future réévaluation ILM.</p> <p>PRGD : l'objet a été supprimé du système StorageGRID.</p> <p>NLOC : les données d'objet ne sont plus disponibles dans le système StorageGRID. Cet état peut indiquer que toutes les copies des données d'objet sont manquantes ou endommagées.</p>
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
VSID	ID de version	L'ID de version d'un nouvel objet créé dans un compartiment multiversion. Les opérations sur les compartiments et les objets dans les compartiments non versionnés n'incluent pas ce champ.

Le message d'audit ORLM peut être émis plusieurs fois pour un seul objet. Par exemple, il est émis chaque fois que l'un des événements suivants se produit :

- Les règles ILM de l'objet sont satisfaites à jamais.
- Les règles ILM de l'objet sont satisfaites pour cette époque.
- Les règles ILM ont supprimé l'objet.
- Le processus de vérification en arrière-plan détecte qu'une copie des données d'objet répliqué est corrompue. Le système StorageGRID effectue une évaluation ILM pour remplacer l'objet corrompu.

**Informations associées**

- ["Transactions d'ingestion d'objets"](#)
- ["Transactions de suppression d'objet"](#)

**OVWR : remplacement d'objet**

Ce message est généré lorsqu'une opération externe (client-demandé) provoque le remplacement d'un objet par un autre objet.

Code	Champ	Description
CBID	Identifiant de bloc de contenu (nouveau)	CBID du nouvel objet.
CSIZ	Taille d'objet précédente	Taille, en octets, de l'objet à remplacer.
OCBD	Identifiant de bloc de contenu (précédent)	CBID de l'objet précédent.
UUID	ID universel unique (nouveau)	Identifiant du nouvel objet dans le système StorageGRID.
OUID	ID universel unique (précédent)	Identifiant de l'objet précédent dans le système StorageGRID.
CHEMIN	Chemin d'objet S3	Chemin d'accès à l'objet S3 utilisé pour l'objet précédent et le nouvel objet
RSLT	Code de résultat	Résultat de la transaction de remplacement d'objet. Le résultat est toujours :  CMC : réussi
SGRP	Site (groupe)	S'il est présent, l'objet écrasé a été supprimé sur le site spécifié, ce qui n'est pas le site où l'objet écrasé a été ingéré.



## S3SL: Demande S3 Select

Ce message consigne une fin d'étude après le renvoi d'une demande S3 Select au client. Le message S3SL peut inclure des détails de message d'erreur et de code d'erreur. La demande n'a peut-être pas abouti.

Code	Champ	Description
BYSC	Octets analysés	Nombre d'octets analysés (reçus) à partir des nœuds de stockage.  BYSC et BYPR sont susceptibles d'être différents si l'objet est compressé. Si l'objet est compressé, BYSC aura le nombre d'octets compressés et BYPR les octets après décompression.
MODÈLE BYPR	Octets traités	Nombre d'octets traités. Indique le nombre d'octets analysés ou traités par un travail S3 Select.
MODÈLE BYRT	Octets renvoyés	Nombre d'octets renvoyés par une tâche S3 Select au client.
RÉFÉRENTIEL	Enregistrements traités	Nombre d'enregistrements ou de lignes qu'un travail S3 Select a reçus des nœuds de stockage.
REIU	Documents renvoyés	Nombre d'enregistrements ou de lignes qu'un travail S3 Select a renvoyé au client.
JOFI	Travail terminé	Indique si le traitement du travail S3 Select est terminé ou non. Si cette valeur est faux, le travail n'a pas pu se terminer et les champs d'erreur contiennent probablement des données. Le client a peut-être reçu des résultats partiels ou aucun résultat.
REID	ID de la demande	Identifiant de la demande S3 Select.
EXTM	Heure d'exécution	Temps, en secondes, nécessaire à la réalisation de S3 Select Job.
GROUPE DE GESTION	Message d'erreur	Message d'erreur généré par le travail S3 Select.
QTÉ	Type d'erreur	Type d'erreur généré par le travail S3 Select.
ERST	Erreur Stacktrace	Erreur Stacktrace générée par le travail S3 Select.
S3BK	Compartiment S3	Nom du compartiment S3.

Code	Champ	Description
S3AK	ID de clé d'accès S3 (expéditeur de la demande)	ID de clé d'accès S3 pour l'utilisateur qui a envoyé la demande.
S3AI	ID de compte de locataire S3 (expéditeur de la demande)	ID de compte de locataire de l'utilisateur qui a envoyé la demande.
S3KY	Clé S3	Le nom de la clé S3 n'inclut pas le nom du compartiment.

#### SADD : désactivation de l'audit de sécurité

Ce message indique que le service d'origine (ID de nœud) a désactivé la journalisation des messages d'audit ; les messages d'audit ne sont plus collectés ou livrés.

Code	Champ	Description
AETM	Activer la méthode	Méthode utilisée pour désactiver l'audit.
AEUN	Nom d'utilisateur	Nom d'utilisateur qui a exécuté la commande pour désactiver la journalisation d'audit.
RSLT	Résultat	Ce champ a la valeur AUCUNE. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message. AUCUN n'est utilisé plutôt que LES CMC pour que ce message ne soit pas filtré.

Ce message implique que la journalisation était déjà activée, mais qu'elle a été désactivée. Ces éléments sont généralement utilisés uniquement lors de l'ingestion en bloc afin d'améliorer les performances du système. Suite à l'activité groupée, l'audit est restauré (SADE) et la capacité de désactivation de l'audit est ensuite bloquée de manière permanente.

#### SADE : activation de l'audit de sécurité

Ce message indique que le service d'origine (ID de nœud) a restauré la journalisation des messages d'audit ; les messages d'audit sont de nouveau collectés et livrés.

Code	Champ	Description
AETM	Activer la méthode	Méthode utilisée pour activer l'audit.
AEUN	Nom d'utilisateur	Nom d'utilisateur qui a exécuté la commande pour activer la journalisation d'audit.

Code	Champ	Description
RSLT	Résultat	Ce champ a la valeur AUCUNE. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message. AUCUN n'est utilisé plutôt que LES CMC pour que ce message ne soit pas filtré.

Ce message implique que la consignation a été précédemment désactivée (SADD), mais qu'elle a maintenant été restaurée. Ces éléments sont généralement utilisés uniquement lors de l'ingestion en bloc afin d'améliorer les performances du système. Suite à l'activité groupée, l'audit est restauré et la fonctionnalité de désactivation de l'audit est bloquée définitivement.

#### SCMT : validation du magasin d'objets

Le contenu de la grille n'est pas disponible ou reconnu comme stocké tant qu'il n'a pas été engagé (c'est-à-dire qu'il a été stocké de manière persistante). Le contenu stocké de manière persistante a été entièrement écrit sur le disque et a transmis des contrôles d'intégrité liés. Ce message est émis lorsqu'un bloc de contenu est attribué au stockage.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu engagé dans le stockage permanent.
RSLT	Code de résultat	Statut au moment où l'objet était stocké sur le disque :  SUCS : objet enregistré avec succès.

Ce message signifie qu'un bloc de contenu donné a été complètement stocké et vérifié, et qu'il peut maintenant être demandé. Il peut être utilisé pour suivre le flux de données dans le système.

#### SDEL : SUPPRESSION S3

Lorsqu'un client S3 émet une transaction DE SUPPRESSION, une demande de suppression de l'objet ou du compartiment spécifié ou de suppression d'une sous-ressource de compartiment/objet est formulée. Ce message est émis par le serveur si la transaction a réussi.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les compartiments n'incluent pas ce champ.
CNCH	En-tête de contrôle de cohérence	Valeur de l'en-tête de la requête HTTP de contrôle de cohérence, s'il est présent dans la demande.
CNID	Identificateur de connexion	Identifiant système unique pour la connexion TCP/IP.

Code	Champ	Description
CSIZ	Taille du contenu	Taille de l'objet supprimé en octets. Les opérations sur les compartiments n'incluent pas ce champ.
DMRM	Supprimer l'ID de version de marqueur	ID de version du marqueur de suppression créé lors de la suppression d'un objet d'un compartiment multiversion. Les opérations sur les compartiments n'incluent pas ce champ.
GFID	ID de connexion de fédération de grille	ID de connexion de la connexion de fédération de grille associée à une demande de suppression de réplication de grille croisée. Inclus uniquement dans les journaux d'audit sur la grille de destination.
GFSA	ID de compte source de fédération de grille	ID de compte du locataire sur la grille source pour une demande de suppression de réplication multigrille. Inclus uniquement dans les journaux d'audit sur la grille de destination.
HTRH	En-tête de requête HTTP	<p>Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration.</p> <div style="border: 1px solid gray; padding: 10px; margin: 10px 0;"> <pre>`X-Forwarded-For` Est automatiquement inclus s'il est présent dans la demande et si la `X-Forwarded-For` valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP).</pre> </div> <p><code>x-amz-bypass-governance-retention</code> est automatiquement inclus s'il est présent dans la demande.</p>
MTME	Heure de la dernière modification	Horodatage Unix, en microsecondes, indiquant quand l'objet a été modifié pour la dernière fois.
RSLT	Code de résultat	Résultat de la transaction DE SUPPRESSION. Le résultat est toujours : CMC : réussi
S3AI	ID de compte de locataire S3 (expéditeur de la demande)	ID de compte de locataire de l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3AK	ID de clé d'accès S3 (expéditeur de la demande)	ID de clé d'accès S3 écrasé pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.

Code	Champ	Description
S3BK	Compartiment S3	Nom du compartiment S3.
S3KY	Clé S3	Le nom de la clé S3 n'inclut pas le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.
S3SR	Sous-ressource S3	Le godet ou la sous-ressource d'objet utilisé, le cas échéant.
CCUA	Nom du compte de locataire S3 (expéditeur de la demande)	Nom du compte de tenant pour l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SAIP	Adresse IP (expéditeur de la demande)	Adresse IP de l'application client qui a fait la demande.
SBAC	Nom de compte de locataire S3 (propriétaire du compartiment)	Nom du compte du locataire pour le propriétaire du compartiment. Permet d'identifier les accès inter-comptes ou anonymes.
SBAI	ID de compte de locataire S3 (propriétaire du compartiment)	ID du compte du locataire du propriétaire du compartiment cible. Permet d'identifier les accès inter-comptes ou anonymes.
SGRP	Site (groupe)	S'il est présent, l'objet a été supprimé sur le site spécifié, ce qui n'est pas le site où l'objet a été ingéré.
SUSR	URN de l'utilisateur S3 (expéditeur de la demande)	L'ID du compte de locataire et le nom d'utilisateur de l'utilisateur qui fait la demande. L'utilisateur peut être un utilisateur local ou LDAP. Par exemple : <code>urn:sgws:identity::03393893651506583485:root</code>  Vide pour les demandes anonymes.
TEMPS	Heure	Temps de traitement total de la demande en microsecondes.
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.

Code	Champ	Description
UDM	Identificateur unique universel pour un marqueur de suppression	Identifiant d'un marqueur de suppression. Les messages du journal d'audit indiquent UUDM ou UUID : UUDM indique un marqueur de suppression créé à la suite d'une demande de suppression d'objet et UUID indique un objet.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
VSID	ID de version	ID de version de la version spécifique d'un objet qui a été supprimé. Les opérations sur les compartiments et les objets dans les compartiments non versionnés n'incluent pas ce champ.

### SGET : OBTENEZ S3

Lorsqu'un client S3 émet une transaction GET, une demande est formulée pour extraire un objet ou répertorier les objets dans un compartiment, ou pour supprimer une sous-ressource de compartiment/objet. Ce message est émis par le serveur si la transaction a réussi.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les compartiments n'incluent pas ce champ.
CNCH	En-tête de contrôle de cohérence	Valeur de l'en-tête de la requête HTTP de contrôle de cohérence, s'il est présent dans la demande.
CNID	Identificateur de connexion	Identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	Taille de l'objet récupéré en octets. Les opérations sur les compartiments n'incluent pas ce champ.
HTRH	En-tête de requête HTTP	Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration. <div style="border: 1px solid gray; padding: 10px; margin-top: 10px;"> <pre>`X-Forwarded-For` Est automatiquement inclus s'il est présent dans la demande et si la `X-Forwarded-For` valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP).</pre> </div>

Code	Champ	Description
NULLITÉ	ListObjectsV2	Une réponse <i>v2 format</i> a été demandée. Pour plus de détails, voir " <a href="#">AWS ListObjectsV2</a> ". Uniquement pour les opérations GET bucket.
NHD	Nombre d'enfants	Inclut des clés et des préfixes courants. Uniquement pour les opérations GET bucket.
AU RANG	Plage lue	Pour les opérations de lecture de plage uniquement. Indique la plage d'octets lus par cette demande. La valeur après la barre oblique (/) indique la taille de l'objet entier.
RSLT	Code de résultat	Résultat de la transaction GET. Le résultat est toujours :  CMC : réussi
S3AI	ID de compte de locataire S3 (expéditeur de la demande)	ID de compte de locataire de l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3AK	ID de clé d'accès S3 (expéditeur de la demande)	ID de clé d'accès S3 écrasé pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Compartiment S3	Nom du compartiment S3.
S3KY	Clé S3	Le nom de la clé S3 n'inclut pas le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.
S3SR	Sous-ressource S3	Le godet ou la sous-ressource d'objet utilisé, le cas échéant.
CCUA	Nom du compte de locataire S3 (expéditeur de la demande)	Nom du compte de tenant pour l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SAIP	Adresse IP (expéditeur de la demande)	Adresse IP de l'application client qui a fait la demande.
SBAC	Nom de compte de locataire S3 (propriétaire du compartiment)	Nom du compte du locataire pour le propriétaire du compartiment. Permet d'identifier les accès inter-comptes ou anonymes.

Code	Champ	Description
SBAI	ID de compte de locataire S3 (propriétaire du compartiment)	ID du compte du locataire du propriétaire du compartiment cible. Permet d'identifier les accès inter-comptes ou anonymes.
SUSR	URN de l'utilisateur S3 (expéditeur de la demande)	L'ID du compte de locataire et le nom d'utilisateur de l'utilisateur qui fait la demande. L'utilisateur peut être un utilisateur local ou LDAP. Par exemple : <code>urn:sgws:identity::03393893651506583485:root</code>  Vide pour les demandes anonymes.
TEMPS	Heure	Temps de traitement total de la demande en microsecondes.
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
TRNC	Tronqué ou non tronqué	Définissez sur FALSE si tous les résultats ont été renvoyés. Réglez sur vrai si d'autres résultats sont disponibles pour revenir. Uniquement pour les opérations GET bucket.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
VSID	ID de version	ID de version de la version spécifique d'un objet demandé. Les opérations sur les compartiments et les objets dans les compartiments non versionnés n'incluent pas ce champ.

### SHEA : TÊTE S3

Lorsqu'un client S3 émet une transaction DE TÊTE, une requête est effectuée afin de vérifier l'existence d'un objet ou d'un compartiment et de récupérer les métadonnées relatives à un objet. Ce message est émis par le serveur si la transaction a réussi.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les compartiments n'incluent pas ce champ.
CNID	Identificateur de connexion	Identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	Taille de l'objet vérifié en octets. Les opérations sur les compartiments n'incluent pas ce champ.



Code	Champ	Description
HTRH	En-tête de requête HTTP	Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration.  <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> `X-Forwarded-For` Est automatiquement inclus s'il est présent dans la demande et si la `X-Forwarded-For` valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP). </div>
RSLT	Code de résultat	Résultat de la transaction GET. Le résultat est toujours :  CMC : réussi
S3AI	ID de compte de locataire S3 (expéditeur de la demande)	ID de compte de locataire de l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3AK	ID de clé d'accès S3 (expéditeur de la demande)	ID de clé d'accès S3 écrasé pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Compartiment S3	Nom du compartiment S3.
S3KY	Clé S3	Le nom de la clé S3 n'inclut pas le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.
CCUA	Nom du compte de locataire S3 (expéditeur de la demande)	Nom du compte de tenant pour l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SAIP	Adresse IP (expéditeur de la demande)	Adresse IP de l'application client qui a fait la demande.
SBAC	Nom de compte de locataire S3 (propriétaire du compartiment)	Nom du compte du locataire pour le propriétaire du compartiment. Permet d'identifier les accès inter-comptes ou anonymes.

Code	Champ	Description
SBAI	ID de compte de locataire S3 (propriétaire du compartiment)	ID du compte du locataire du propriétaire du compartiment cible. Permet d'identifier les accès inter-comptes ou anonymes.
SUSR	URN de l'utilisateur S3 (expéditeur de la demande)	L'ID du compte de locataire et le nom d'utilisateur de l'utilisateur qui fait la demande. L'utilisateur peut être un utilisateur local ou LDAP. Par exemple : <code>urn:sgws:identity::03393893651506583485:root</code>  Vide pour les demandes anonymes.
TEMPS	Heure	Temps de traitement total de la demande en microsecondes.
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
VSID	ID de version	ID de version de la version spécifique d'un objet demandé. Les opérations sur les compartiments et les objets dans les compartiments non versionnés n'incluent pas ce champ.

#### SPO : BORNE S3

Lorsqu'un client S3 émet une requête POST-objet, ce message est émis par le serveur si la transaction a réussi.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0.
CNCH	En-tête de contrôle de cohérence	Valeur de l'en-tête de la requête HTTP de contrôle de cohérence, s'il est présent dans la demande.
CNID	Identificateur de connexion	Identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	Taille de l'objet récupéré en octets.

Code	Champ	Description
HTRH	En-tête de requête HTTP	<p>Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration.</p> <div style="border: 1px solid gray; padding: 10px; margin: 10px 0;"> <p><code>`X-Forwarded-For`</code> Est automatiquement inclus s'il est présent dans la demande et si la <code>`X-Forwarded-For`</code> valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP).</p> </div> <p>(Non prévu pour SPOS).</p>
RSLT	Code de résultat	<p>Résultat de la demande RestoreObject. Le résultat est toujours :</p> <p>CMC : réussi</p>
S3AI	ID de compte de locataire S3 (expéditeur de la demande)	ID de compte de locataire de l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3AK	ID de clé d'accès S3 (expéditeur de la demande)	ID de clé d'accès S3 écrasé pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Compartiment S3	Nom du compartiment S3.
S3KY	Clé S3	Le nom de la clé S3 n'inclut pas le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.
S3SR	Sous-ressource S3	<p>Le godet ou la sous-ressource d'objet utilisé, le cas échéant.</p> <p>Réglez sur « SELECT » pour une opération S3 Select.</p>
CCUA	Nom du compte de locataire S3 (expéditeur de la demande)	Nom du compte de tenant pour l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SAIP	Adresse IP (expéditeur de la demande)	Adresse IP de l'application client qui a fait la demande.

Code	Champ	Description
SBAC	Nom de compte de locataire S3 (propriétaire du compartiment)	Nom du compte du locataire pour le propriétaire du compartiment. Permet d'identifier les accès inter-comptes ou anonymes.
SBAI	ID de compte de locataire S3 (propriétaire du compartiment)	ID du compte du locataire du propriétaire du compartiment cible. Permet d'identifier les accès inter-comptes ou anonymes.
SFCF	Configuration des sous-ressources	Informations sur la restauration.
SUSR	URN de l'utilisateur S3 (expéditeur de la demande)	L'ID du compte de locataire et le nom d'utilisateur de l'utilisateur qui fait la demande. L'utilisateur peut être un utilisateur local ou LDAP. Par exemple : <code>urn:sgws:identity::03393893651506583485:root</code>  Vide pour les demandes anonymes.
TEMPS	Heure	Temps de traitement total de la demande en microsecondes.
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
VSID	ID de version	ID de version de la version spécifique d'un objet demandé. Les opérations sur les compartiments et les objets dans les compartiments non versionnés n'incluent pas ce champ.

#### SPUT : PUT S3

Lorsqu'un client S3 émet une transaction PUT, une demande est formulée pour créer un nouvel objet ou un nouveau compartiment, ou pour supprimer une sous-ressource bucket/objet. Ce message est émis par le serveur si la transaction a réussi.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les compartiments n'incluent pas ce champ.

Code	Champ	Description
CMPS	Paramètres de conformité	Les paramètres de conformité utilisés lors de la création du compartiment, s'ils sont présents dans la demande (tronqués aux 1024 premiers caractères).
CNCH	En-tête de contrôle de cohérence	Valeur de l'en-tête de la requête HTTP de contrôle de cohérence, s'il est présent dans la demande.
CNID	Identificateur de connexion	Identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	Taille de l'objet récupéré en octets. Les opérations sur les compartiments n'incluent pas ce champ.
GFID	ID de connexion de fédération de grille	ID de connexion de la connexion de fédération de grille associée à une demande PUT de réplication de grille croisée. Inclus uniquement dans les journaux d'audit sur la grille de destination.
GFSA	ID de compte source de fédération de grille	ID de compte du locataire sur la grille source pour une demande PUT de réplication multigrille. Inclus uniquement dans les journaux d'audit sur la grille de destination.
HTRH	En-tête de requête HTTP	<p>Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration.</p> <div style="border: 1px solid gray; padding: 10px; margin: 10px 0;"> <pre>`X-Forwarded-For` Est automatiquement inclus s'il est présent dans la demande et si la `X-Forwarded-For` valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP).</pre> </div> <p><code>x-amz-bypass-governance-retention</code> est automatiquement inclus s'il est présent dans la demande.</p>
LKEN	Verrouillage d'objet activé	Valeur de l'en-tête <code>x-amz-bucket-object-lock-enabled</code> de la demande, s'il est présent dans la demande.
LKLH	Verrouillage de l'objet en attente légale	Valeur de l'en-tête de requête <code>x-amz-object-lock-legal-hold</code> , s'il est présent dans la demande PutObject.

Code	Champ	Description
LKMD	Mode de conservation du verrouillage d'objet	Valeur de l'en-tête de requête <code>x-amz-object-lock-mode</code> , s'il est présent dans la demande <code>PutObject</code> .
LKRU	Conservation de l'objet jusqu'à la date	Valeur de l'en-tête de requête <code>x-amz-object-lock-retain-until-date</code> , s'il est présent dans la demande <code>PutObject</code> . Les valeurs sont limitées à 100 ans après la date d'ingestion de l'objet.
MTME	Heure de la dernière modification	Horodatage Unix, en microsecondes, indiquant quand l'objet a été modifié pour la dernière fois.
RSLT	Code de résultat	Résultat de la transaction <code>PUT</code> . Le résultat est toujours :  CMC : réussi
S3AI	ID de compte de locataire S3 (expéditeur de la demande)	ID de compte de locataire de l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3AK	ID de clé d'accès S3 (expéditeur de la demande)	ID de clé d'accès S3 écrasé pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Compartiment S3	Nom du compartiment S3.
S3KY	Clé S3	Le nom de la clé S3 n'inclut pas le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.
S3SR	Sous-ressource S3	Le godet ou la sous-ressource d'objet utilisé, le cas échéant.
CCUA	Nom du compte de locataire S3 (expéditeur de la demande)	Nom du compte de tenant pour l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SAIP	Adresse IP (expéditeur de la demande)	Adresse IP de l'application client qui a fait la demande.

Code	Champ	Description
SBAC	Nom de compte de locataire S3 (propriétaire du compartiment)	Nom du compte du locataire pour le propriétaire du compartiment. Permet d'identifier les accès inter-comptes ou anonymes.
SBAI	ID de compte de locataire S3 (propriétaire du compartiment)	ID du compte du locataire du propriétaire du compartiment cible. Permet d'identifier les accès inter-comptes ou anonymes.
SFCF	Configuration des sous-ressources	La nouvelle configuration de sous-ressource (tronquée aux 1024 premiers caractères).
SUSR	URN de l'utilisateur S3 (expéditeur de la demande)	L'ID du compte de locataire et le nom d'utilisateur de l'utilisateur qui fait la demande. L'utilisateur peut être un utilisateur local ou LDAP. Par exemple : <code>urn:sgws:identity::03393893651506583485:root</code>  Vide pour les demandes anonymes.
TEMPS	Heure	Temps de traitement total de la demande en microsecondes.
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
ID ULID	ID de téléchargement	Inclus uniquement dans les messages SPUT pour les opérations CompleteMultipartUpload. Indique que toutes les pièces ont été téléchargées et assemblées.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
VSID	ID de version	L'ID de version d'un nouvel objet créé dans un compartiment multiversion. Les opérations sur les compartiments et les objets dans les compartiments non versionnés n'incluent pas ce champ.
VSST	Etat de gestion des versions	Nouvel état de gestion des versions d'un compartiment. Deux États sont utilisés : « activé » ou « suspendu ». Les opérations sur les objets n'incluent pas ce champ.

#### SREM : Suppression du magasin d'objets

Ce message est émis lorsque le contenu est supprimé du stockage persistant et n'est plus accessible via des API régulières.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu supprimé du stockage permanent.
RSLT	Code de résultat	Indique le résultat des opérations de suppression de contenu. La seule valeur définie est :  SUCS : contenu supprimé du stockage persistant

Ce message d'audit signifie qu'un bloc de contenu donné a été supprimé d'un nœud et ne peut plus être demandé directement. Le message peut être utilisé pour suivre le flux de contenu supprimé dans le système.

#### SUPD : métadonnées S3 mises à jour

Ce message est généré par l'API S3 lorsqu'un client S3 met à jour les métadonnées pour un objet ingéré. Le message est émis par le serveur si la mise à jour des métadonnées a réussi.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les compartiments n'incluent pas ce champ.
CNCH	En-tête de contrôle de cohérence	Valeur de l'en-tête de requête HTTP de contrôle de cohérence, s'il est présent dans la demande, lors de la mise à jour des paramètres de conformité d'un compartiment.
CNID	Identificateur de connexion	Identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	Taille de l'objet récupéré en octets. Les opérations sur les compartiments n'incluent pas ce champ.
HTRH	En-tête de requête HTTP	Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration.  <div style="border: 1px solid #ccc; padding: 10px; background-color: #f9f9f9;"> <pre>`X-Forwarded-For` Est automatiquement inclus s'il est présent dans la demande et si la `X-Forwarded-For` valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP).</pre> </div>
RSLT	Code de résultat	Résultat de la transaction GET. Le résultat est toujours :  CMC : réussi



Code	Champ	Description
S3AI	ID de compte de locataire S3 (expéditeur de la demande)	ID de compte de locataire de l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3AK	ID de clé d'accès S3 (expéditeur de la demande)	ID de clé d'accès S3 écrasé pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Compartiment S3	Nom du compartiment S3.
S3KY	Clé S3	Le nom de la clé S3 n'inclut pas le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.
CCUA	Nom du compte de locataire S3 (expéditeur de la demande)	Nom du compte de tenant pour l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SAIP	Adresse IP (expéditeur de la demande)	Adresse IP de l'application client qui a fait la demande.
SBAC	Nom de compte de locataire S3 (propriétaire du compartiment)	Nom du compte du locataire pour le propriétaire du compartiment. Permet d'identifier les accès inter-comptes ou anonymes.
SBAI	ID de compte de locataire S3 (propriétaire du compartiment)	ID du compte du locataire du propriétaire du compartiment cible. Permet d'identifier les accès inter-comptes ou anonymes.
SUSR	URN de l'utilisateur S3 (expéditeur de la demande)	L'ID du compte de locataire et le nom d'utilisateur de l'utilisateur qui fait la demande. L'utilisateur peut être un utilisateur local ou LDAP. Par exemple : <code>urn:sgws:identity::03393893651506583485:root</code>  Vide pour les demandes anonymes.
TEMPS	Heure	Temps de traitement total de la demande en microsecondes.
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.

Code	Champ	Description
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
VSID	ID de version	ID de version de la version spécifique d'un objet dont les métadonnées ont été mises à jour. Les opérations sur les compartiments et les objets dans les compartiments non versionnés n'incluent pas ce champ.

#### SVRF : échec de la vérification du magasin d'objets

Ce message est émis chaque fois qu'un bloc de contenu échoue au processus de vérification. Chaque fois que les données d'objet répliqué sont lues ou écrites sur le disque, plusieurs vérifications et vérifications d'intégrité sont effectuées pour s'assurer que les données envoyées à l'utilisateur requérant sont identiques aux données initialement ingérées sur le système. Si l'une de ces vérifications échoue, le système met automatiquement en quarantaine les données d'objet répliqué corrompues pour les empêcher d'être récupérées à nouveau.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu qui a échoué à la vérification.
RSLT	Code de résultat	Type d'échec de vérification :  CRCF : échec du contrôle de redondance cyclique (CRC).  HMAC : échec de la vérification du code d'authentification du message basé sur le hachage (HMAC).  EHSR : hachage de contenu crypté inattendu.  PHSR : hachage de contenu original inattendu.  SEQC : séquence de données incorrecte sur le disque.  PERR : structure non valide du fichier de disque.  DERR : erreur disque.  FNAM : nom de fichier incorrect.



Ce message doit être surveillé de près. Les défaillances de vérification de contenu peuvent indiquer des pannes matérielles imminentes.

Pour déterminer quelle opération a déclenché le message, reportez-vous à la valeur du champ ID du module. Par exemple, une valeur SVFY indique que le message a été généré par le module Storage Verifier, c'est-à-dire la vérification en arrière-plan et STOR indique que le message a été déclenché par la récupération du contenu.

## SVRU : Vérification du magasin d'objets inconnue

Le composant de stockage du service LDR analyse en continu toutes les copies des données objet répliquées dans le magasin d'objets. Ce message est émis lorsqu'une copie inconnue ou inattendue des données d'objet répliqué est détectée dans le magasin d'objets et déplacée vers le répertoire de quarantaine.

Code	Champ	Description
FPTH	Chemin du fichier	Chemin du fichier de la copie d'objet inattendue.
RSLT	Résultat	Ce champ a la valeur 'NONE'. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message. 'AUCUN' est utilisé plutôt que 'UCS' pour que ce message ne soit pas filtré.



Le message d'audit SVRU: Object Store Verify Unknown doit être suivi de près. Cela signifie que des copies inattendues de données objet ont été détectées dans le magasin d'objets. Cette situation doit être examinée immédiatement pour déterminer comment ces copies ont été créées, car elle peut indiquer des défaillances matérielles imminentes.

## SYSD : arrêt du nœud

Lorsqu'un service est arrêté avec élégance, ce message est généré pour indiquer que l'arrêt a été demandé. Généralement, ce message est envoyé uniquement après un redémarrage ultérieur, car la file d'attente des messages d'audit n'est pas effacée avant l'arrêt. Recherchez le message SYST, envoyé au début de la séquence d'arrêt, si le service n'a pas redémarré.

Code	Champ	Description
RSLT	Nettoyer l'arrêt	La nature de l'arrêt :  SUCS : le système s'est arrêté correctement.

Le message n'indique pas si le serveur hôte est arrêté, seul le service de génération de rapports. Le RSLT d'un SYSD ne peut pas indiquer un arrêt « non planifié », car le message est généré uniquement par des arrêts « corrects ».

## SYST : arrêt du nœud

Lorsqu'un service est correctement arrêté, ce message est généré pour indiquer que l'arrêt a été demandé et que le service a lancé sa séquence d'arrêt. SYST peut être utilisé pour déterminer si l'arrêt a été demandé, avant le redémarrage du service (contrairement à SYSD, qui est généralement envoyé après le redémarrage du service).

Code	Champ	Description
RSLT	Nettoyer l'arrêt	La nature de l'arrêt :  SUCS : le système s'est arrêté correctement.

Le message n'indique pas si le serveur hôte est arrêté, seul le service de génération de rapports. Le code RSLT d'un message SYST ne peut pas indiquer un arrêt « non planifié », car le message est généré uniquement par des arrêts « corrects ».

#### **SYSU : démarrage du nœud**

Lors du redémarrage d'un service, ce message est généré pour indiquer si l'arrêt précédent était propre (commandé) ou désordonné (inattendu).

Code	Champ	Description
RSLT	Nettoyer l'arrêt	La nature de l'arrêt :  SUCS : le système a été arrêté proprement.  DSDN : le système n'a pas été arrêté complètement.  VRGN : le système a été démarré pour la première fois après l'installation du serveur (ou la réinstallation).

Le message n'indique pas si le serveur hôte a été démarré, seul le service de génération de rapports. Ce message peut être utilisé pour :

- Détecter la discontinuité dans la piste d'audit.
- Déterminez si un service échoue pendant le fonctionnement (étant donné que la nature distribuée du système StorageGRID peut masquer ces défaillances). Server Manager redémarre automatiquement un service en panne.

#### **WDEL : SUPPRESSION rapide**

Lorsqu'un client Swift émet une transaction DE SUPPRESSION, une demande est faite pour supprimer l'objet ou le conteneur spécifié. Ce message est émis par le serveur si la transaction a réussi.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les conteneurs n'incluent pas ce champ.
CSIZ	Taille du contenu	Taille de l'objet supprimé en octets. Les opérations sur les conteneurs n'incluent pas ce champ.

Code	Champ	Description
HTRH	En-tête de requête HTTP	Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration.  <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> `X-Forwarded-For` Est automatiquement inclus s'il est présent dans la demande et si la `X-Forwarded-For` valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP). </div>
MTME	Heure de la dernière modification	Horodatage Unix, en microsecondes, indiquant quand l'objet a été modifié pour la dernière fois.
RSLT	Code de résultat	Résultat de la transaction DE SUPPRESSION. Le résultat est toujours :  CMC : réussi
SAIP	Adresse IP du client requérant	Adresse IP de l'application client qui a fait la demande.
SGRP	Site (groupe)	S'il est présent, l'objet a été supprimé sur le site spécifié, ce qui n'est pas le site où l'objet a été ingéré.
TEMPS	Heure	Temps de traitement total de la demande en microsecondes.
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
WACC	ID de compte Swift	ID de compte unique tel que spécifié par le système StorageGRID.
CONEM	Conteneur Swift	Nom du conteneur Swift.
WOBJ	Objet Swift	Identifiant de l'objet Swift. Les opérations sur les conteneurs n'incluent pas ce champ.
WUSR	Utilisateur du compte Swift	Nom d'utilisateur du compte Swift qui identifie de manière unique le client effectuant la transaction.

## WGET: SWIFT GET

Lorsqu'un client Swift émet une transaction GET, une demande est faite pour récupérer un objet, répertorier les objets dans un conteneur ou répertorier les conteneurs dans un compte. Ce message est émis par le serveur si la transaction a réussi.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les comptes et les conteneurs n'incluent pas ce champ.
CSIZ	Taille du contenu	Taille de l'objet récupéré en octets. Les opérations sur les comptes et les conteneurs n'incluent pas ce champ.
HTRH	En-tête de requête HTTP	Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration. <div style="border: 1px solid gray; padding: 10px; margin-top: 10px;"><code>`X-Forwarded-For` Est automatiquement inclus s'il est présent dans la demande et si la `X-Forwarded-For` valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP).</code></div>
RSLT	Code de résultat	Résultat de la transaction GET. Le résultat est toujours  CMC : réussi
SAIP	Adresse IP du client requérant	Adresse IP de l'application client qui a fait la demande.
TEMPS	Heure	Temps de traitement total de la demande en microsecondes.
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
WACC	ID de compte Swift	ID de compte unique tel que spécifié par le système StorageGRID.
CONEM	Conteneur Swift	Nom du conteneur Swift. Les opérations sur les comptes n'incluent pas ce champ.

Code	Champ	Description
WOBJ	Objet Swift	Identifiant de l'objet Swift. Les opérations sur les comptes et les conteneurs n'incluent pas ce champ.
WUSR	Utilisateur du compte Swift	Nom d'utilisateur du compte Swift qui identifie de manière unique le client effectuant la transaction.

#### WHEA: TÊTE SWIFT

Lorsqu'un client Swift émet une transaction DE TÊTE, une demande est faite pour vérifier l'existence d'un compte, d'un conteneur ou d'un objet, et pour récupérer toutes les métadonnées pertinentes. Ce message est émis par le serveur si la transaction a réussi.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les comptes et les conteneurs n'incluent pas ce champ.
CSIZ	Taille du contenu	Taille de l'objet récupéré en octets. Les opérations sur les comptes et les conteneurs n'incluent pas ce champ.
HTRH	En-tête de requête HTTP	Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration.  <div style="border: 1px solid gray; padding: 10px; margin: 10px 0;"> <pre>`X-Forwarded-For` Est automatiquement inclus s'il est présent dans la demande et si la `X- Forwarded-For` valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP).</pre> </div>
RSLT	Code de résultat	Résultat de la transaction DE TÊTE. Le résultat est toujours :  CMC : réussi
SAIP	Adresse IP du client requérant	Adresse IP de l'application client qui a fait la demande.
TEMPS	Heure	Temps de traitement total de la demande en microsecondes.
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.

Code	Champ	Description
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
WACC	ID de compte Swift	ID de compte unique tel que spécifié par le système StorageGRID.
CONEM	Conteneur Swift	Nom du conteneur Swift. Les opérations sur les comptes n'incluent pas ce champ.
WOBJ	Objet Swift	Identifiant de l'objet Swift. Les opérations sur les comptes et les conteneurs n'incluent pas ce champ.
WUSR	Utilisateur du compte Swift	Nom d'utilisateur du compte Swift qui identifie de manière unique le client effectuant la transaction.

#### WPUT : PUT SWIFT

Lorsqu'un client Swift émet une transaction PUT, une demande est faite pour créer un objet ou un conteneur. Ce message est émis par le serveur si la transaction a réussi.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les conteneurs n'incluent pas ce champ.
CSIZ	Taille du contenu	Taille de l'objet récupéré en octets. Les opérations sur les conteneurs n'incluent pas ce champ.
HTRH	En-tête de requête HTTP	Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration. <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <pre>`X-Forwarded-For` Est automatiquement inclus s'il est présent dans la demande et si la `X-Forwarded-For` valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP).</pre> </div>
MTME	Heure de la dernière modification	Horodatage Unix, en microsecondes, indiquant quand l'objet a été modifié pour la dernière fois.



<b>Code</b>	<b>Champ</b>	<b>Description</b>
RSLT	Code de résultat	Résultat de la transaction PUT. Le résultat est toujours : CMC : réussi
SAIP	Adresse IP du client requérant	Adresse IP de l'application client qui a fait la demande.
TEMPS	Heure	Temps de traitement total de la demande en microsecondes.
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
WACC	ID de compte Swift	ID de compte unique tel que spécifié par le système StorageGRID.
CONEM	Conteneur Swift	Nom du conteneur Swift.
WOBJ	Objet Swift	Identifiant de l'objet Swift. Les opérations sur les conteneurs n'incluent pas ce champ.
WUSR	Utilisateur du compte Swift	Nom d'utilisateur du compte Swift qui identifie de manière unique le client effectuant la transaction.

## 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.