Surveiller et dépanner

StorageGRID software

NetApp
December 03, 2025

Sommaire

Surveiller et dépanner 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 Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Tu as"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**.

À propos de cette tâche

Ces instructions décrivent comment :

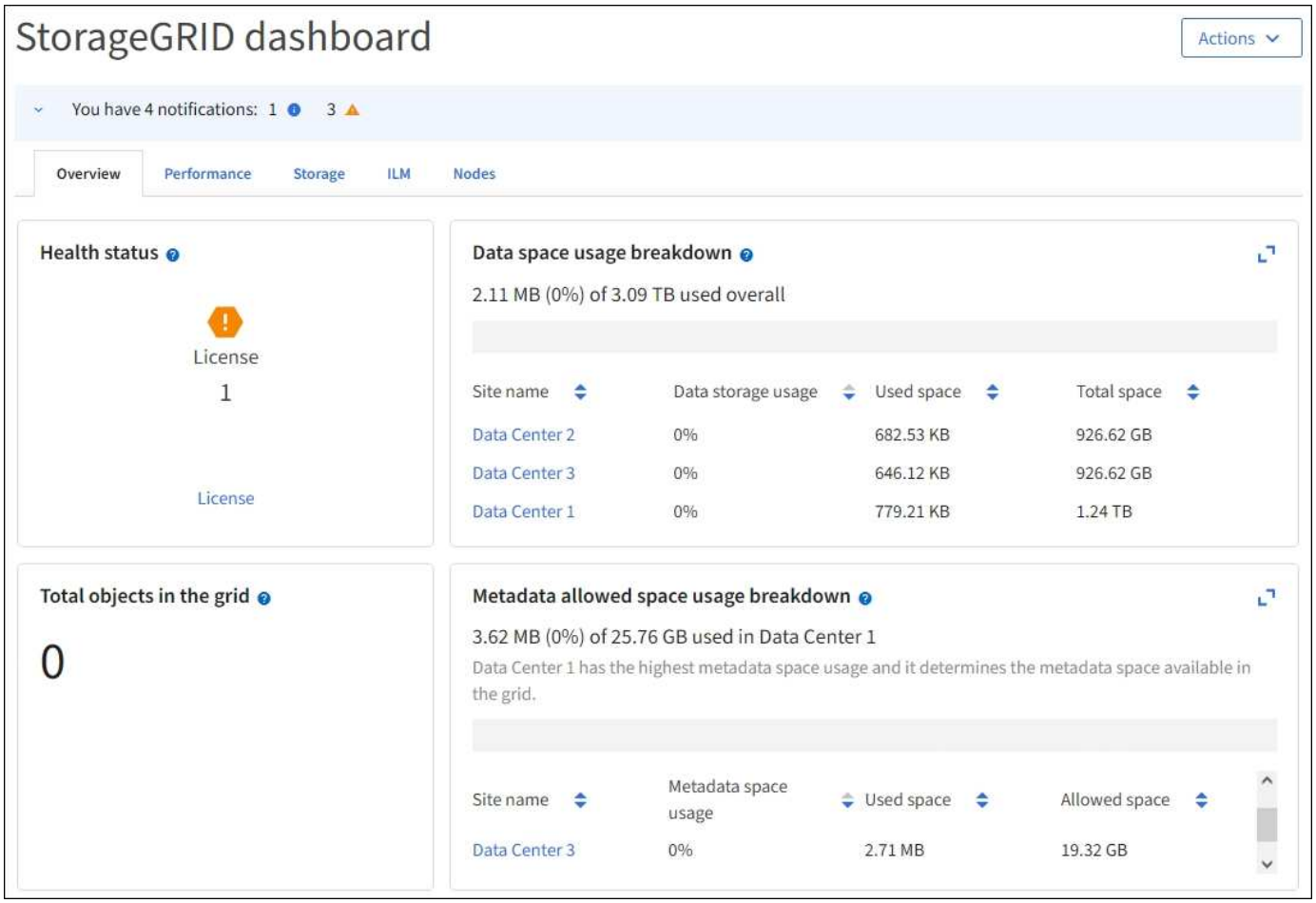
- "Afficher et gérer le tableau de bord"
- "Afficher la page Nœuds"
- "Surveillez régulièrement ces aspects du système :"
  - "Santé du système"
  - "Capacité de stockage"
  - "Gestion du cycle de vie de l'information"
  - "Ressources réseau et système"
  - "Activité des locataires"
  - "Opérations d'équilibrage de charge"
  - "Connexions de la fédération de réseau"
- "Gérer les alertes"
- "Afficher les fichiers journaux"
- "Configurer les messages d'audit et les destinations des journaux"
- "Utiliser un serveur syslog externe"pour collecter des informations d'audit
- "Utiliser SNMP pour la surveillance"
- "Obtenir des données StorageGRID supplémentaires", y compris les mesures et les diagnostics

Afficher et gérer 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 surveiller 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 être différent 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 quel. De plus, vous pouvez créer des tableaux de bord personnalisés qui contiennent uniquement les onglets et les cartes pertinents pour la surveillance de votre implémentation de StorageGRID.

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

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

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

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

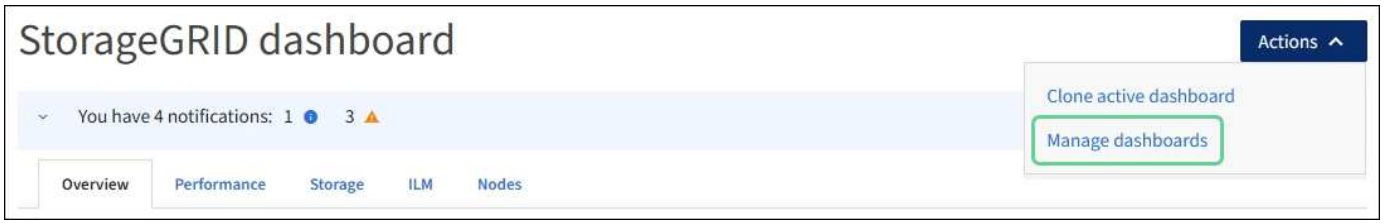
Gérer les tableaux de bord

Si vous avez un accès root (voir"Autorisations du groupe d'administrateurs"), 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 les informations StorageGRID affichées et la manière dont ces informations sont organisées.
- Clonez 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 le tableau de bord fourni par le système ou un tableau de bord personnalisé.
- Définissez un tableau de bord par défaut, qui est ce que tous les utilisateurs voient, à moins qu'ils n'activent leur propre tableau de bord.
- Modifier 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.
- Supprimer un tableau de bord.

> Si vous disposez d'une autre autorisation en plus de l'accès root, vous ne pouvez définir qu'un tableau de bord actif.

Pour gérer les tableaux de bord, sélectionnez **Actions** > **Gérer les tableaux de bord**.



Configurer les tableaux de bord

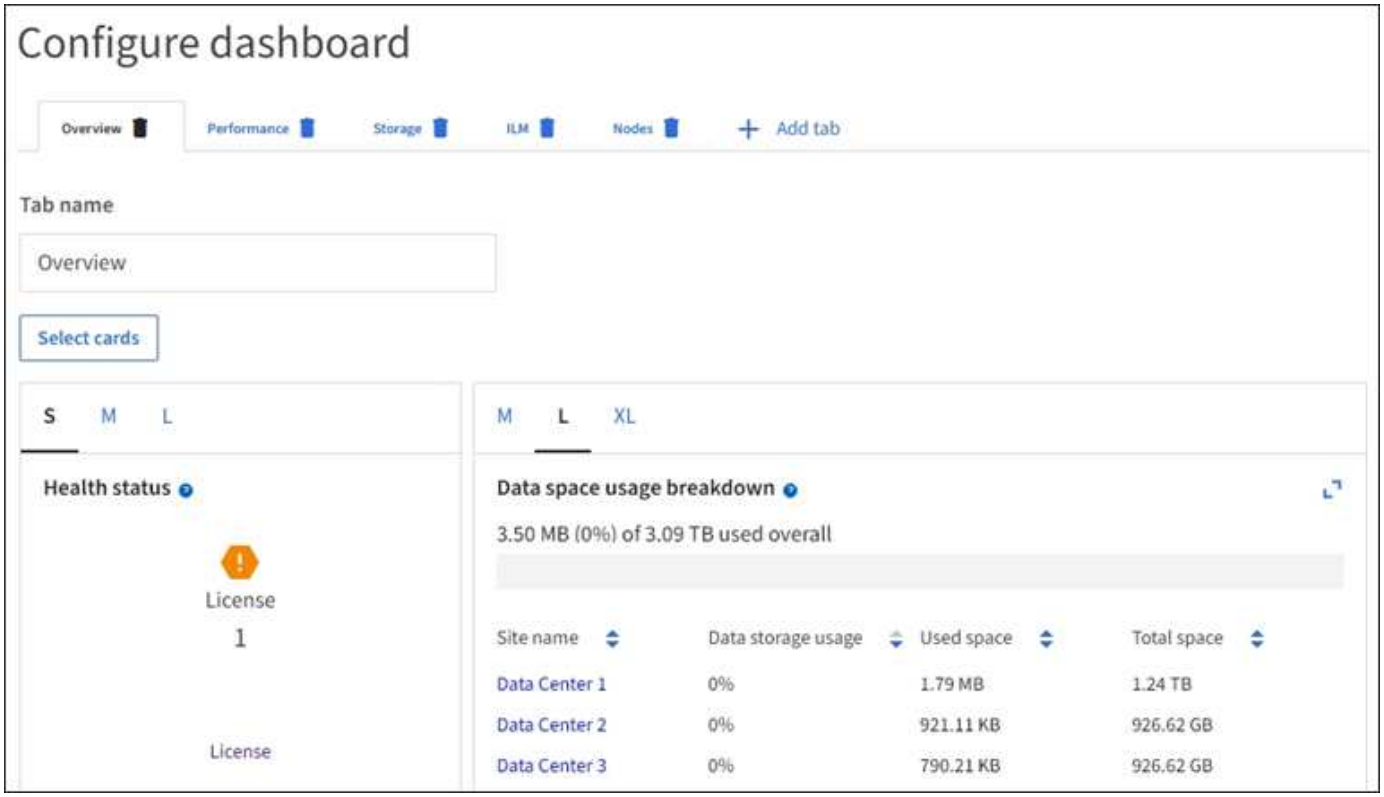
Pour créer un nouveau tableau de bord en clonant le tableau de bord actif, sélectionnez **Actions** > **Cloner le tableau de bord actif**.

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
- Renommer les onglets et donner aux nouveaux onglets des noms uniques
- Ajouter, supprimer ou réorganiser (faire glisser) des cartes pour chaque onglet
- Sélectionnez la taille des cartes individuelles en sélectionnant **S**, **M**, **L** ou **XL** en haut de la carte



Afficher la page Nœuds

Afficher la page Nœuds

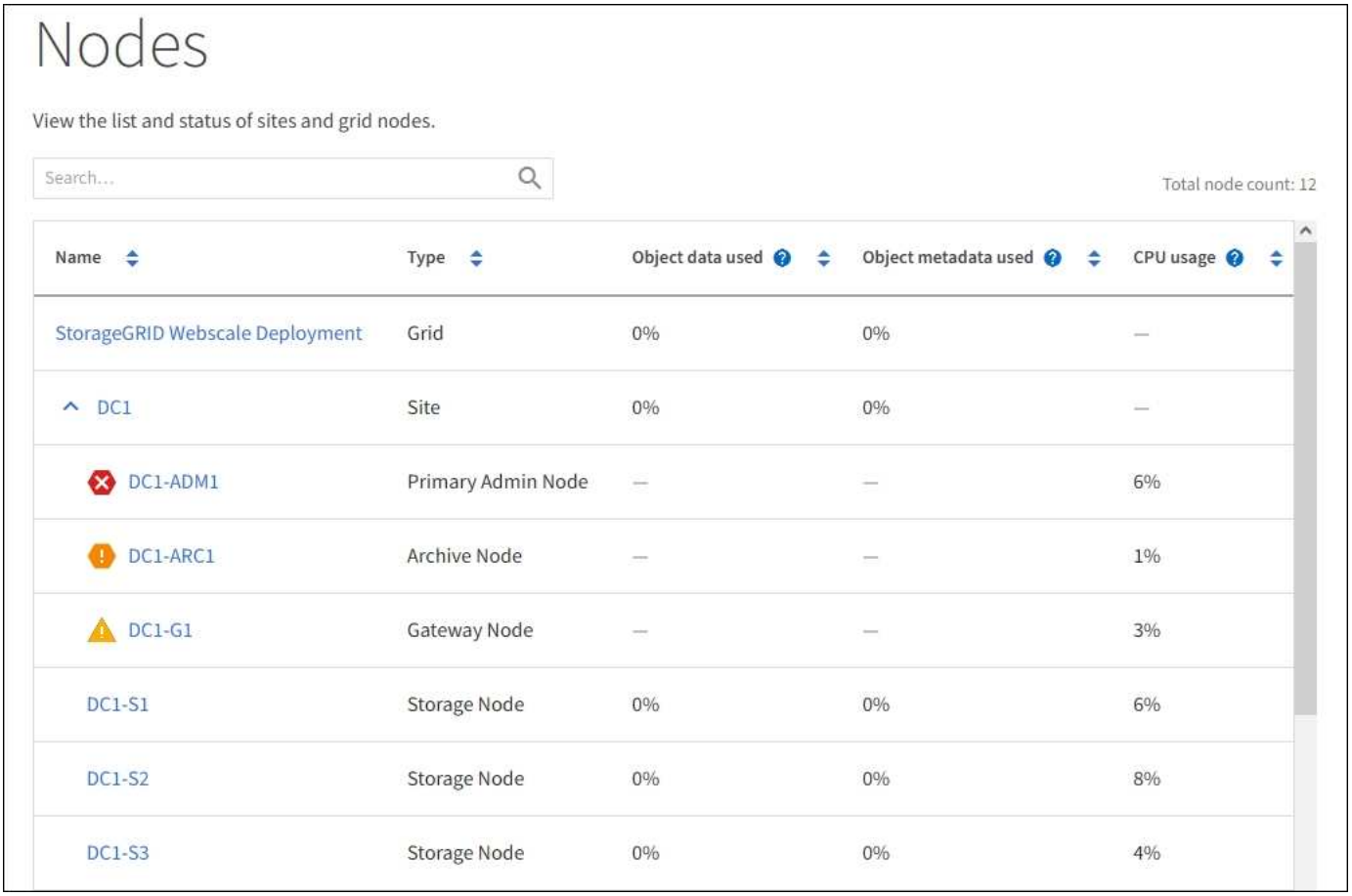
Lorsque vous avez besoin d'informations plus détaillées sur votre système StorageGRID que celles fournies par le tableau de bord, vous pouvez utiliser la page Nœuds pour afficher les métriques de l'ensemble de la grille, de chaque site de la grille et de chaque nœud d'un site.

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 apparaît à côté du nom du nœud. Si le nœud est connecté et n'a aucune alerte active, aucune icône n'est affichée.

Lorsqu'un nœud n'est pas connecté au réseau, par exemple lors d'une mise à niveau ou d'un état déconnecté, certaines mesures peuvent être indisponibles ou exclues des totaux du site et du réseau. Une fois qu'un nœud se reconnecte au réseau, attendez quelques 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 présentées sont des exemples. Vos résultats peuvent varier en fonction de votre version de StorageGRID .



Icônes d'état de connexion

Si un nœud est déconnecté du réseau, l'une des icônes suivantes apparaît à côté du nom du nœud.

Icône	Description	Action requise
	Non connecté - Inconnu Pour une raison inconnue, un nœud est déconnecté ou les services sur le nœud sont interrompus de manière inattendue. Par exemple, un service sur le nœud peut être arrêté ou le nœud peut avoir perdu sa connexion réseau en raison d'une panne de courant ou d'une panne inattendue. L'alerte **Impossible de communiquer avec le nœud** peut également être déclenchée. D'autres alertes peuvent également être actives.	Nécessite une attention immédiate. "Sélectionnez chaque alerte" et suivez les actions recommandées. Par exemple, vous devrez peut-être redémarrer un service qui s'est arrêté ou redémarrer l'hôte du nœud. **Remarque** : un nœud peut apparaître comme inconnu lors des opérations d'arrêt géré. Vous pouvez ignorer l'état Inconnu dans ces cas.
	Non connecté - Administrativement en panne Pour une raison attendue, le nœud n'est pas connecté au réseau. Par exemple, le nœud ou les services sur le nœud ont été arrêtés correctement, le nœud redémarre ou le logiciel est en cours de mise à niveau. Une ou plusieurs alertes peuvent également être actives. En fonction du problème sous-jacent, ces nœuds reviennent souvent en ligne sans intervention.	Déterminez si des alertes affectent ce nœud. Si une ou plusieurs alertes sont actives,"Sélectionnez chaque alerte" et suivez les actions recommandées.

Si un nœud est déconnecté du réseau, il peut y avoir une alerte sous-jacente, mais seule l'icône « Non connecté » apparaît. Pour voir les alertes actives pour un nœud, sélectionnez le nœud.

Icônes d'alerte

S'il existe une alerte active pour un nœud, l'une des icônes suivantes apparaît à côté du nom du nœud :

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

Majeur : Une condition anormale existe qui affecte les opérations en cours ou approche le seuil d'une alerte critique. Vous devez enquêter sur les alertes majeures et résoudre tous les problèmes sous-jacents pour garantir que la condition anormale n'arrête pas le fonctionnement normal d'un nœud ou d'un service StorageGRID .

Mineur : Le système fonctionne normalement, mais une condition anormale existe qui pourrait affecter la capacité du système à fonctionner si elle persiste. Vous devez surveiller et résoudre les alertes mineures qui ne disparaissent pas d'elles-mêmes pour vous assurer qu'elles n'entraînent pas un problème plus grave.

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

Pour filtrer les informations affichées dans le tableau Nœuds, saisissez une chaîne de recherche dans le champ **Rechercher**. Vous pouvez effectuer une recherche par nom de système, nom d'affichage ou type (par exemple, saisissez **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 voir un résumé global des statistiques de l'ensemble de votre système StorageGRID .
- Sélectionnez un site de centre de données spécifique pour voir un résumé global des statistiques de tous les nœuds de ce site.
- Sélectionnez un nœud spécifique pour afficher des informations détaillées sur ce nœud.

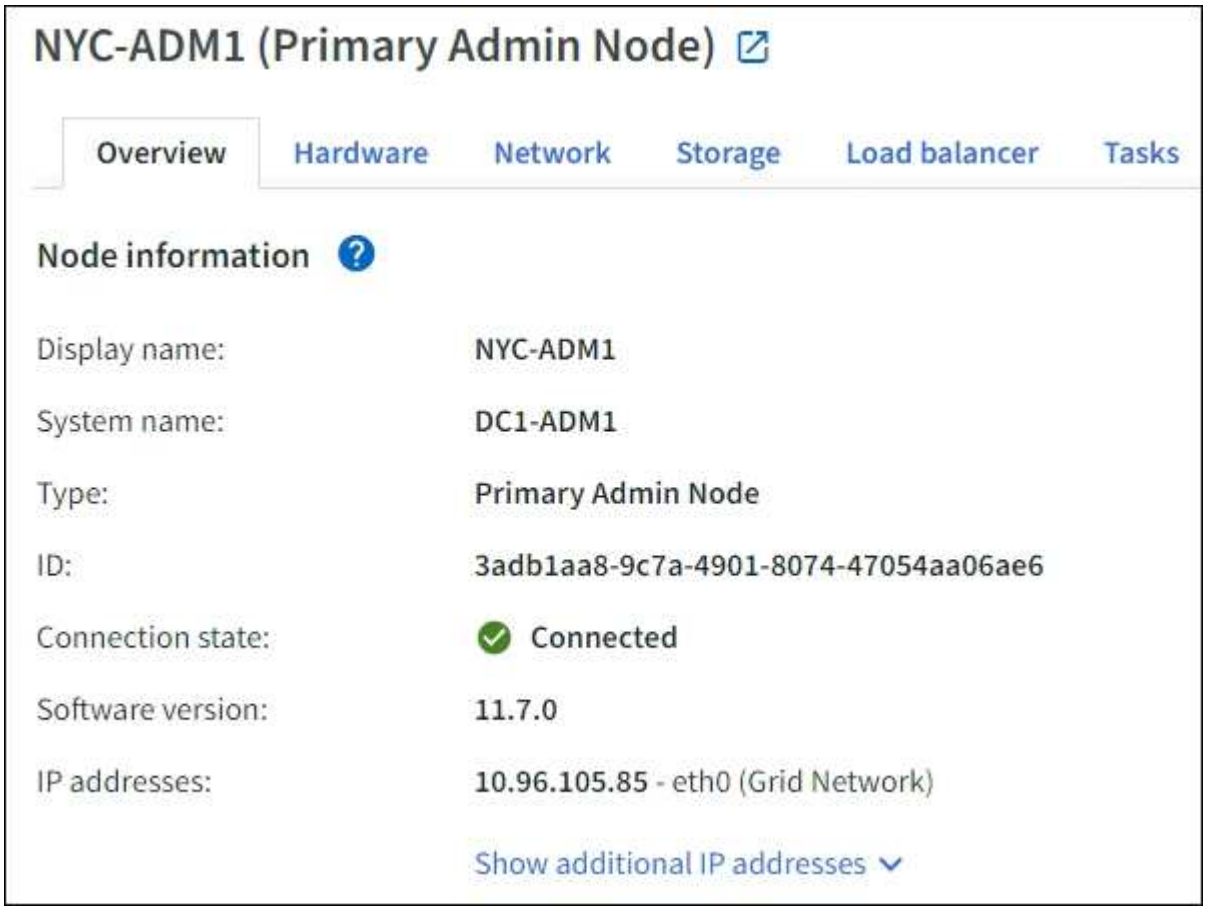
Afficher l'onglet Aperçu

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

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

Informations sur le nœud

La section Informations sur le nœud de l'onglet Présentation répertorie les informations de base sur le nœud.



Les informations générales 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 le"Renommer 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 d'administration, nœud d'administration principal, nœud de stockage ou nœud de passerelle.
- **ID** : l'identifiant unique du nœud, également appelé UUID.
- **État 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 au réseau ou un ou plusieurs services sont inopinément hors service. Par exemple, la connexion réseau entre les nœuds a été perdue, l'alimentation est coupée 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 nécessite une attention immédiate.

    > Un nœud peut apparaître comme inconnu lors des opérations d'arrêt gérées. Vous pouvez ignorer l'état Inconnu dans ces cas.

  - *Administrativement en panne* :Le nœud n'est pas connecté au réseau pour une raison attendue. Par exemple, le nœud ou les services sur le nœud ont été arrêtés correctement, le nœud redémarre ou le logiciel est en cours de mise à niveau. Une ou plusieurs alertes peuvent également être actives.
  - *Connecté* :Le nœud est connecté au réseau.
- **Stockage utilisé** : Pour les nœuds de stockage uniquement.
  - **Données d'objet** : le pourcentage de l'espace total utilisable pour les données d'objet qui a été utilisé sur le nœud de stockage.
  - **Métadonnées d'objet** : le 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 les nœuds de passerelle uniquement. Indique si une interface réseau sur le nœud est incluse dans un groupe de haute disponibilité et si cette interface est l'interface principale.
- **Adresses IP** : Les adresses IP du nœud. Cliquez sur **Afficher les adresses IP supplémentaires** pour afficher les adresses IPv4 et IPv6 du nœud et les mappages d'interface.

Alertes

La section Alertes de l'onglet Aperçu répertorie toutes les"alertes affectant actuellement ce nœud qui n'ont pas été désactivées" . Sélectionnez le nom de l'alerte pour afficher des détails supplémentaires et les actions recommandées.

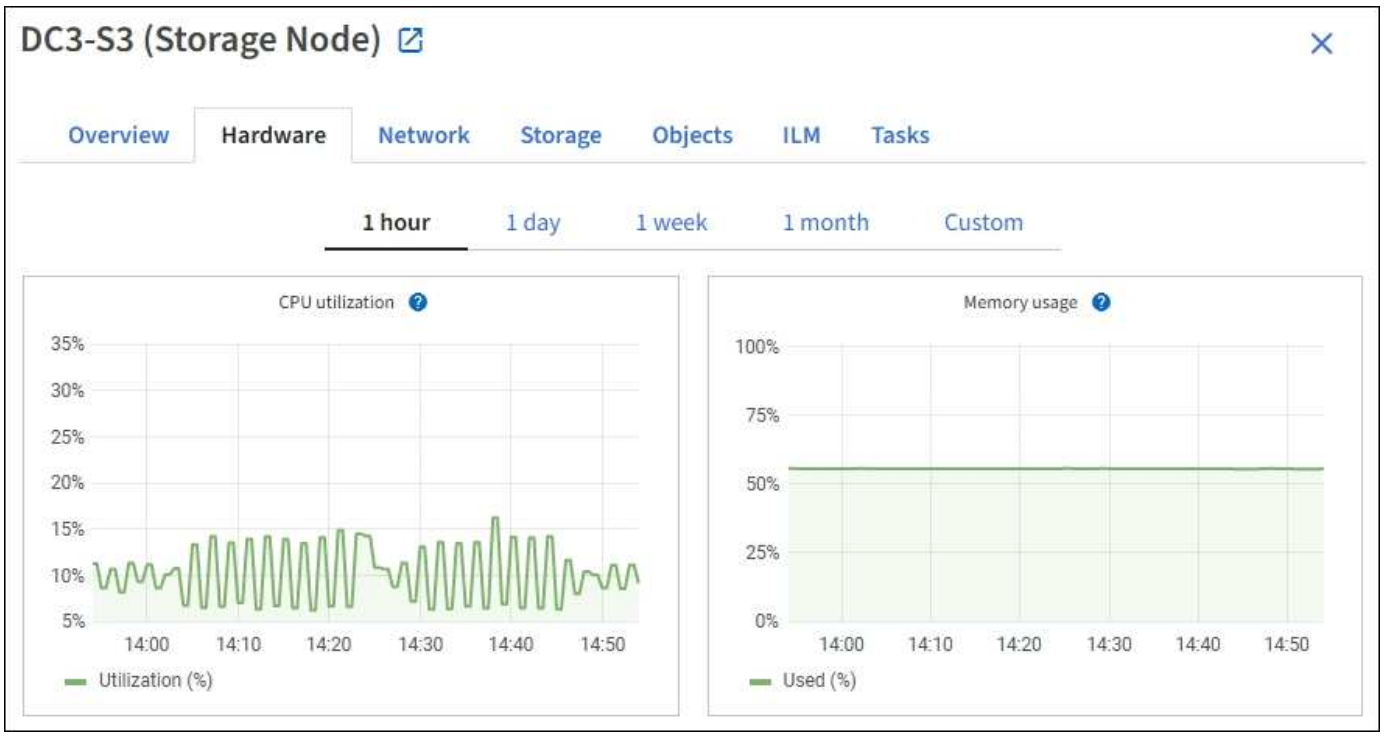
Des alertes sont également incluses pour"états de connexion des nœuds" .

Afficher l'onglet Matériel

L'onglet Matériel affiche l'utilisation du processeur et de la mémoire pour chaque nœud, ainsi que des informations matérielles supplémentaires sur les appareils.

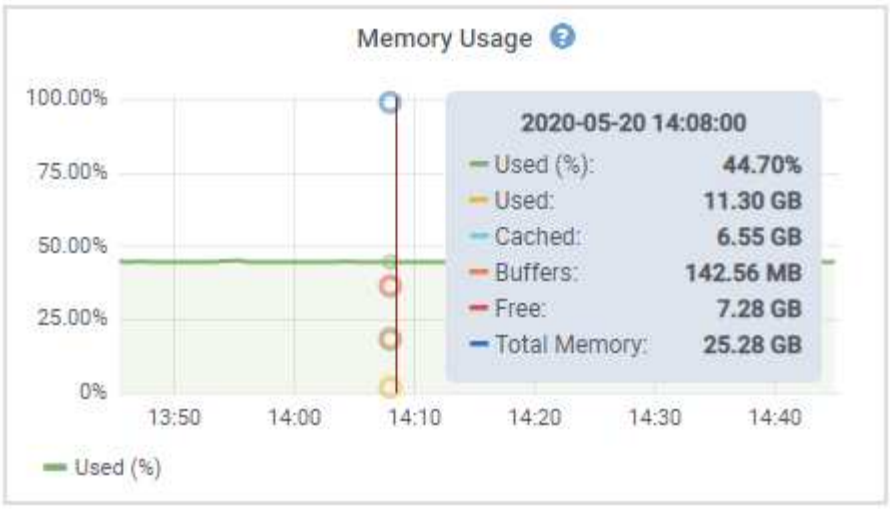
> Le gestionnaire de grille est mis à jour à chaque version et peut ne pas correspondre aux exemples de captures d'écran sur cette page.

L'onglet Matériel est affiché pour tous les nœuds.



Pour afficher un intervalle de temps différent, sélectionnez l'un des contrôles au-dessus du graphique ou du diagramme. Vous pouvez afficher les informations disponibles pour des 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 dates et d'heures.

Pour voir les détails de l'utilisation du processeur 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 plus d'informations sur le matériel de l'appliance.

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

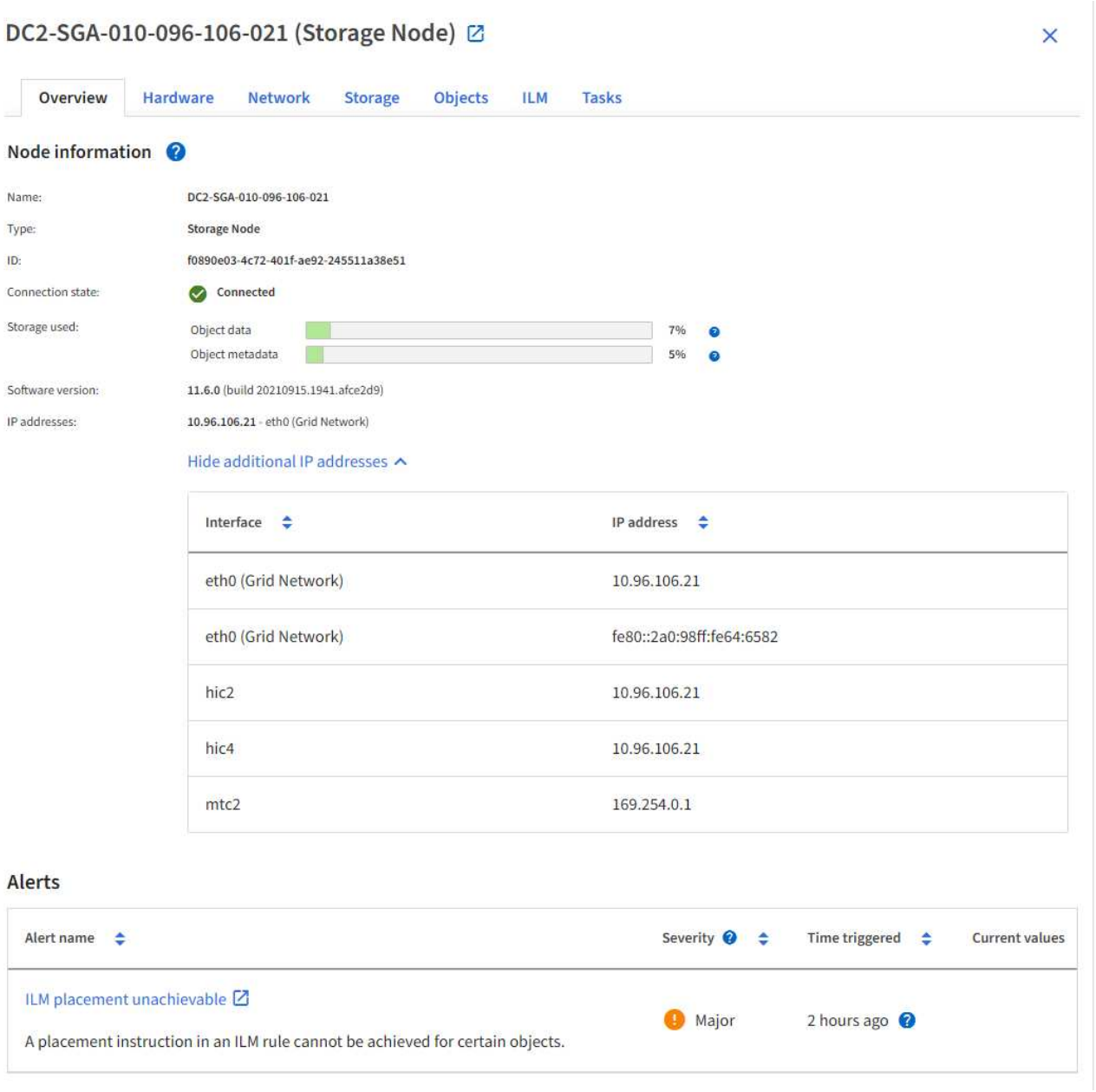
La page Nœuds répertorie les informations sur l'état du service et toutes les ressources de calcul, de disque et de réseau pour chaque nœud de stockage de l'appliance. Vous pouvez également voir la mémoire, le matériel de stockage, la version du micrologiciel du contrôleur, les ressources réseau, les interfaces réseau, les adresses réseau et recevoir et transmettre des données.

Étapes

1. Depuis la page Nœuds, sélectionnez un nœud de stockage d'appliance.
2. Sélectionnez **Aperçu**.

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

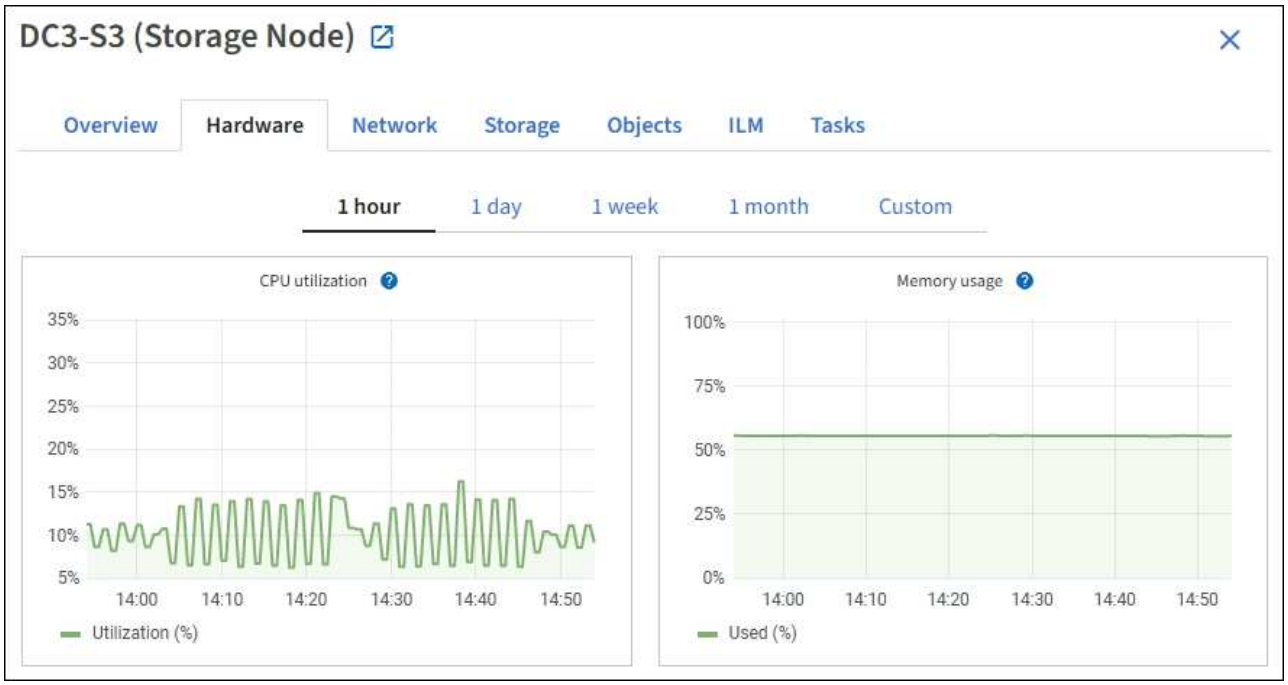
   - **eth** : Le réseau Grid, le réseau administrateur ou le réseau client.
   - **hic**: L'un des ports physiques 10, 25 ou 100 GbE de l'appareil. Ces ports peuvent être liés ensemble et connectés au réseau de grille StorageGRID (eth0) et au réseau client (eth2).
   - **mtc** : l'un des ports physiques 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.



La section Alertes de l'onglet Présentation affiche toutes les alertes actives pour le nœud.

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

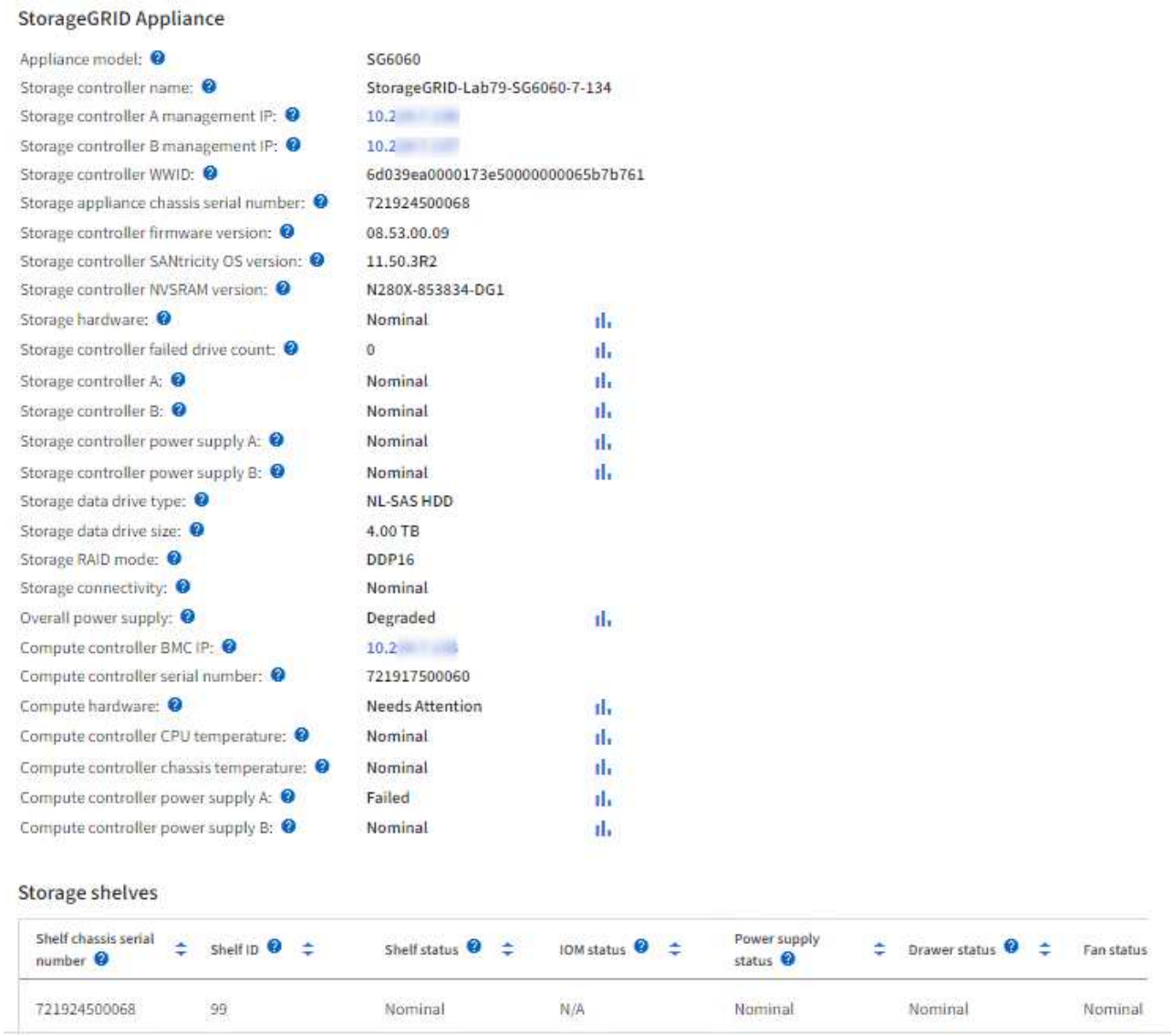
   a. Affichez les graphiques d'utilisation du processeur et de la mémoire pour déterminer les pourcentages d'utilisation du processeur et de la mémoire au fil du temps. Pour afficher un intervalle de temps différent, sélectionnez l'un des contrôles au-dessus du graphique ou du diagramme. Vous pouvez afficher les informations disponibles pour des 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 dates et d'heures.



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'appareil, les noms des contrôleurs, les numéros de série et les adresses IP, ainsi que l'état de chaque composant.

> Certains champs, tels que l'adresse IP du contrôleur de calcul BMC et le matériel de calcul, n'apparaissent que pour les appliances dotées de cette fonctionnalité.

Les composants des étagères de stockage et des étagères d'extension si elles font partie de l'installation apparaissent dans un tableau séparé sous le tableau des appareils.



Champ dans la table Appliance	Description
Modèle d'appareil	Le numéro de modèle de cet appareil StorageGRID affiché dans SANtricity OS.
Nom du contrôleur de stockage	Le nom de cet appareil StorageGRID affiché dans SANtricity OS.
Contrôleur de stockage Une adresse IP de gestion	Adresse IP pour le port de gestion 1 sur le contrôleur de stockage A. Vous utilisez cette adresse IP pour accéder à SANtricity OS afin de résoudre les problèmes de stockage.
IP de gestion du contrôleur de stockage B	Adresse IP pour le port de gestion 1 sur le contrôleur de stockage B. Vous utilisez cette adresse IP pour accéder à SANtricity OS afin de résoudre les problèmes de stockage. Certains modèles d'appareils ne disposent pas de contrôleur de stockage B.

Champ dans la table Appliance	Description
WWID du contrôleur de stockage	L'identifiant mondial du contrôleur de stockage affiché dans SANtricity OS.
Numéro de série du châssis de l'appareil de stockage	Le numéro de série du châssis de l'appareil.
Version du micrologiciel du contrôleur de stockage	La version du micrologiciel sur le contrôleur de stockage de cet appareil.
Version du système d'exploitation SANtricity du contrôleur de stockage	La version du système d'exploitation SANtricity du contrôleur de stockage A.
Contrôleur de stockage version NVSRAM	Version NVSRAM du contrôleur de stockage telle que rapportée par SANtricity System Manager. Pour les SG6060 et SG6160, s'il existe une incompatibilité de version NVSRAM 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	L'état général du matériel du contrôleur de stockage. Si SANtricity System Manager signale un état « Nécessite une attention particulière » pour le matériel de stockage, le système StorageGRID signale également cette valeur. Si le statut est « nécessite une attention particulière », vérifiez d'abord le contrôleur de stockage à l'aide de SANtricity OS. Ensuite, assurez-vous qu'aucune autre alerte n'existe qui s'applique au contrôleur de calcul.
Nombre de disques défaillants du contrôleur de stockage	Le nombre de lecteurs qui ne sont pas optimaux.
Contrôleur de stockage A	L'état du contrôleur de stockage A.
Contrôleur de stockage B	L'état du contrôleur de stockage B. Certains modèles d'appareils ne disposent pas de contrôleur de stockage B.
Alimentation du contrôleur de stockage A	L'état de l'alimentation A pour le contrôleur de stockage.
Alimentation du contrôleur de stockage B	L'état de l'alimentation B du contrôleur de stockage.
Type de lecteur de données de stockage	Le type de lecteurs de l'appareil, tels que HDD (disque dur) ou SSD (disque SSD).

Champ dans la table Appliance	Description
Taille du lecteur de données de stockage	La taille effective d'un lecteur de données. Pour le SG6160, la taille du lecteur de cache s'affiche également. **Remarque** : Pour les nœuds avec des étagères d'extension, utilisez leTaille du lecteur de données pour chaque étagère plutôt. La taille effective du lecteur peut varier selon l'étagère.
Mode RAID de stockage	Le mode RAID configuré pour l'appareil.
Connectivité de stockage	L'état de connectivité du stockage.
Alimentation électrique globale	L'état de toutes les alimentations électriques de l'appareil.
Contrôleur de calcul BMC IP	L'adresse IP du port du contrôleur de gestion de la carte mère (BMC) dans le contrôleur de calcul. Vous utilisez cette IP pour vous connecter à l'interface BMC afin de surveiller et de diagnostiquer le matériel de l'appliance. Ce champ n'est pas affiché pour les modèles d'appareils qui ne contiennent pas de BMC.
Numéro de série du contrôleur de calcul	Le numéro de série du contrôleur de calcul.
Matériel informatique	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 distincts.
Température du processeur du contrôleur de calcul	L'état de température du processeur du contrôleur de calcul.
Température du châssis du contrôleur de calcul	L'état de température du contrôleur de calcul.

+

Colonne dans le tableau des étagères de rangement	Description
Numéro de série du châssis d'étagère	Le numéro de série du châssis de l'étagère de stockage.

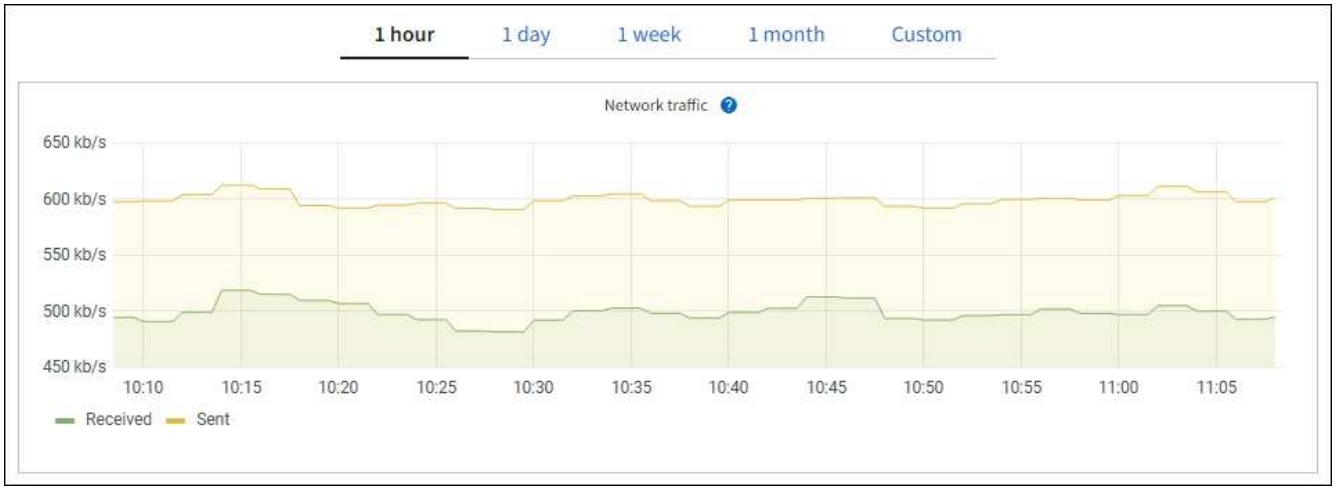
Colonne dans le tableau des étagères de rangement	Description
ID d'étagère	L'identifiant numérique de l'étagère de stockage. • 99 : Étagère de contrôleur de stockage • 0 : Première étagère d'extension • 1 : Deuxième étagère d'extension **Remarque :** les étagères d'extension s'appliquent uniquement aux modèles SG6060 et SG6160.
État des étagères	L'état général de l'étagère de stockage.
Statut de l'OIM	L'état des modules d'entrée/sortie (IOM) dans toutes les étagères d'extension. N/A s'il ne s'agit pas d'une étagère d'extension.
État de l'alimentation électrique	L'état général des alimentations électriques de l'étagère de stockage.
État du tiroir	L'état des tiroirs de l'étagère de rangement. N/A si l'étagère ne contient pas de tiroirs.
Statut du ventilateur	L'état général des ventilateurs de refroidissement dans l'étagère de stockage.
Emplacements de lecteur	Le nombre total d'emplacements de lecteur dans l'étagère de stockage.
Lecteurs de données	Le nombre de lecteurs dans l'étagère de stockage qui sont utilisés pour le stockage des données.
Taille du lecteur de données	La taille effective d'un lecteur de données dans l'étagère de stockage.
Lecteurs de cache	Le nombre de lecteurs dans l'étagère de stockage qui sont utilisés comme cache.
Taille du lecteur de cache	La taille du plus petit lecteur de cache dans l'étagère de stockage. Normalement, les lecteurs de cache ont tous la même taille.
État de la configuration	L'état de configuration de l'étagère de stockage.

a. Confirmez que tous les statuts sont « Nominaux ».

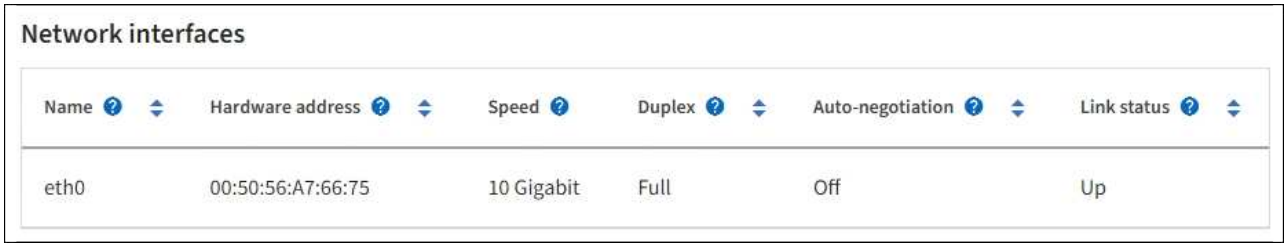
   Si un statut n'est pas « Nominal », vérifiez toutes les alertes actuelles. Vous pouvez également utiliser SANtricity System Manager pour en savoir plus sur certaines de ces valeurs matérielles. Consultez les instructions d'installation et d'entretien de votre appareil.

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

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



a. Consultez la section Interfaces réseau.



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

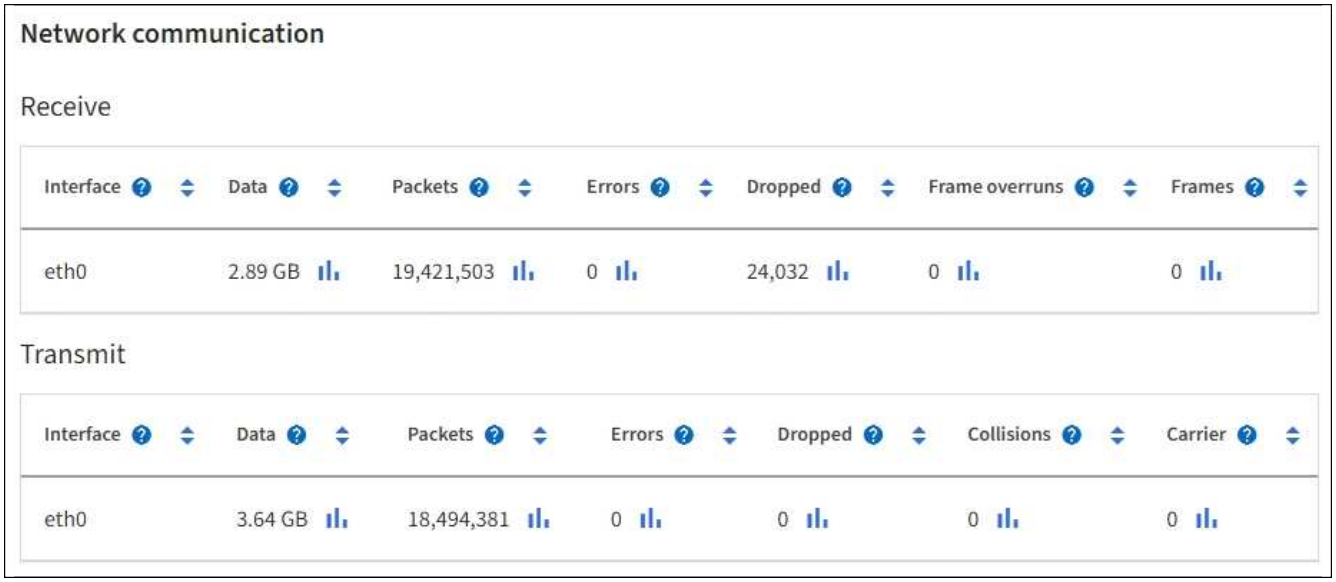
Les valeurs indiquées dans le tableau supposent que les quatre liens sont utilisés.

Mode de liaison	Mode liaison	Vitesse de liaison HIC individuelle (hic1, hic2, hic3, hic4)	Vitesse attendue du réseau grille/client (eth0, eth2)
Agrégat	LACP	25	100
Fixé	LACP	25	50
Fixé	Actif/Sauvegarde	25	25
Agrégat	LACP	10	40
Fixé	LACP	10	20
Fixé	Actif/Sauvegarde	10	10

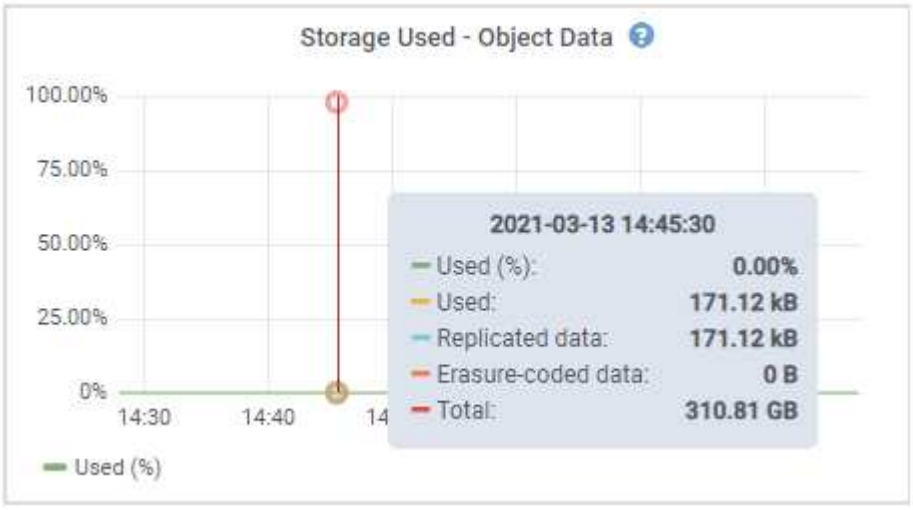
Voir "Configurer les liens réseau" pour plus d'informations sur la configuration des ports 10/25-GbE.

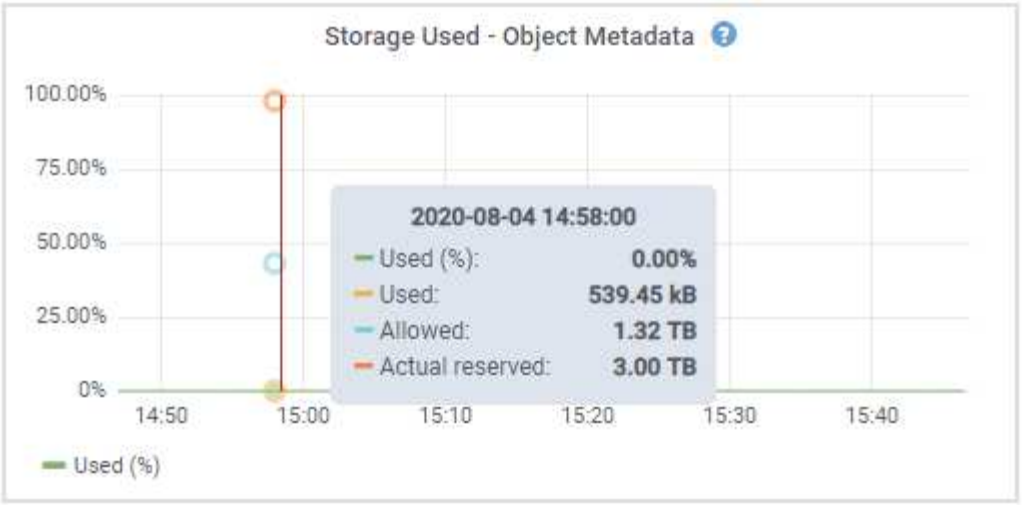
b. Consultez la section Communication réseau.

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.



5. Sélectionnez **Stockage** pour afficher les graphiques qui montrent les pourcentages de stockage utilisés au fil du temps pour les données d'objet et les métadonnées d'objet, ainsi que des informations sur les périphériques de disque, les volumes et les magasins d'objets.

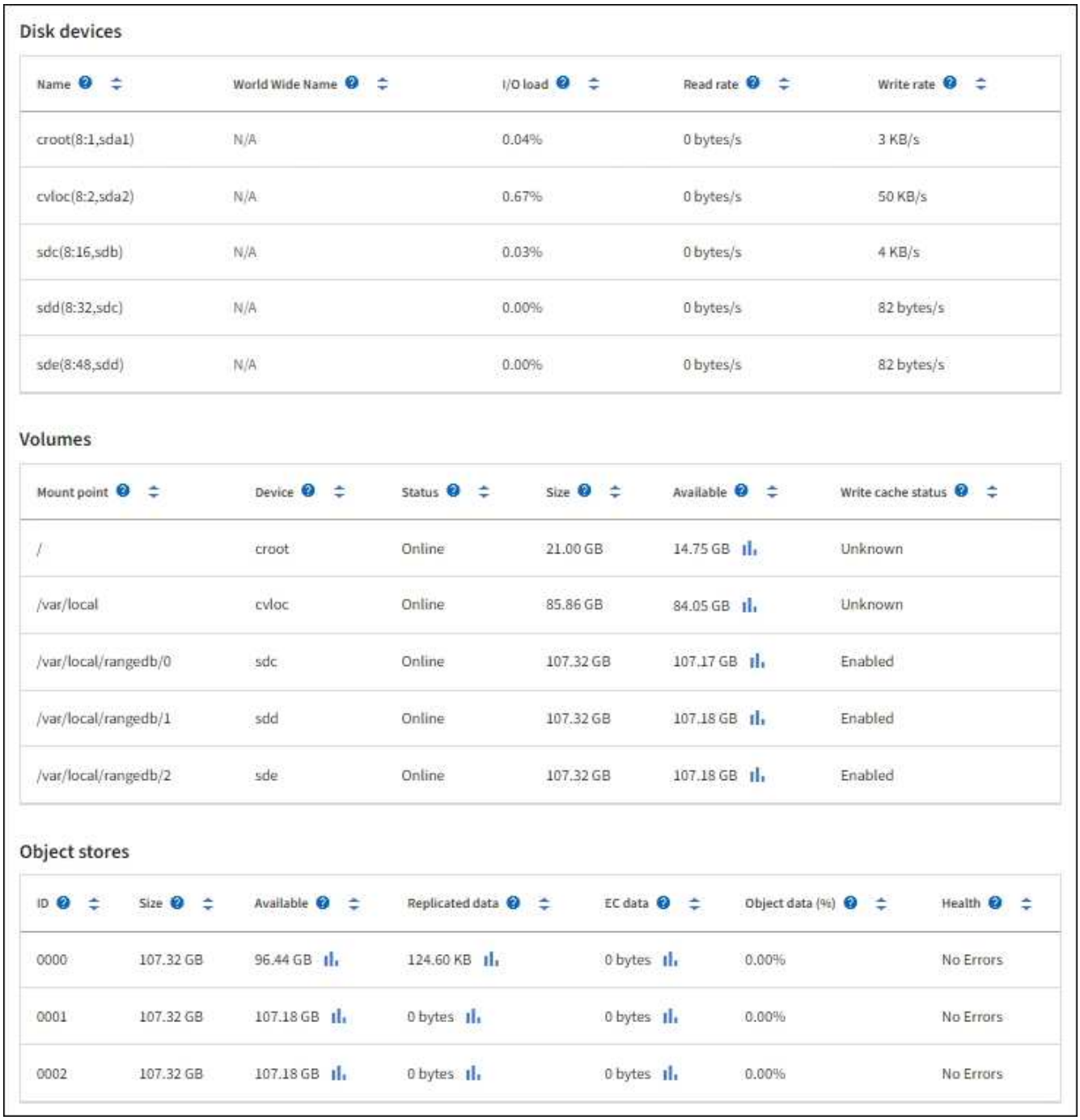




a. Faites défiler vers le bas pour afficher les quantités de stockage disponibles pour chaque volume et magasin d'objets.

   Le nom mondial de chaque disque correspond à l'identifiant mondial du volume (WWID) qui apparaît lorsque vous affichez les propriétés du volume standard 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 sur disque liées aux points de montage de volume, la première partie du nom affichée dans la colonne **Nom** du tableau Périphériques de disque (c'est-à-dire *sdc*, *sdd*, *sde*, etc.) correspond à la valeur affichée dans la colonne **Périphérique** du tableau 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

Afficher les informations sur les nœuds d'administration et les nœuds de passerelle de l'appareil

La page Nœuds répertorie les informations sur l'état du service et toutes les ressources de calcul, de périphérique de disque et de réseau pour chaque dispositif de services utilisé comme nœud d'administration ou nœud de passerelle. Vous pouvez également voir la mémoire, le matériel de stockage, les ressources réseau, les interfaces réseau, les adresses réseau et recevoir et transmettre des données.

Étapes

1. À partir de la page Nœuds, sélectionnez un nœud d'administration d'appareil ou un nœud de passerelle d'appareil.
2. Sélectionnez **Aperçu**.

   La section Informations sur le nœud de l'onglet Présentation affiche des informations récapitulatives sur le

nœud, telles que le nom, le type, l'ID et l'état de connexion du nœud. La liste des adresses IP comprend le nom de l'interface pour chaque adresse, comme suit :

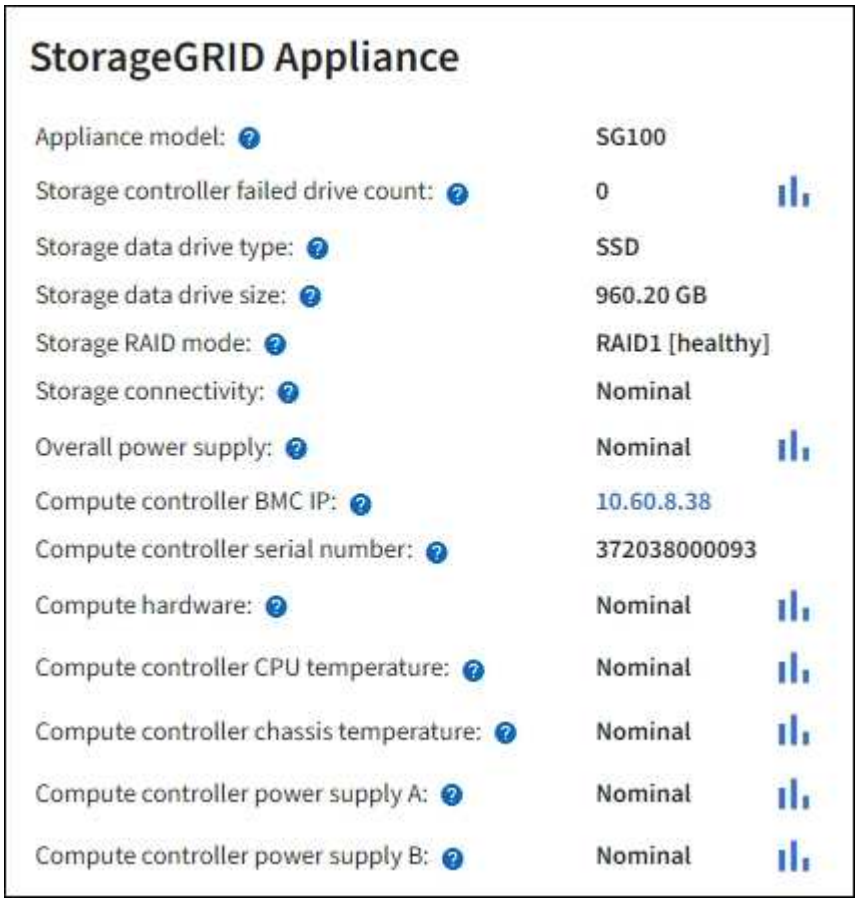
- **adllb** et **adlli** : affichés si la liaison active/de secours est utilisée pour l'interface réseau d'administration
- **eth** : Le réseau Grid, le réseau administrateur ou le réseau client.
- **hic**: L'un des ports physiques 10, 25 ou 100 GbE de l'appareil. Ces ports peuvent être liés ensemble et connectés au réseau de grille StorageGRID (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 (eth1). Vous pouvez laisser d'autres interfaces mtc disponibles pour une connectivité locale temporaire pour un technicien du centre de données.

La section Alertes de l'onglet Présentation affiche toutes les alertes actives pour le nœud.

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

   a. Affichez les graphiques d'utilisation du processeur et de la mémoire pour déterminer les pourcentages d'utilisation du processeur et de la mémoire au fil du temps. Pour afficher un intervalle de temps différent, sélectionnez l'un des contrôles au-dessus du graphique ou du diagramme. Vous pouvez afficher les informations disponibles pour des 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 dates et d'heures.

   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.



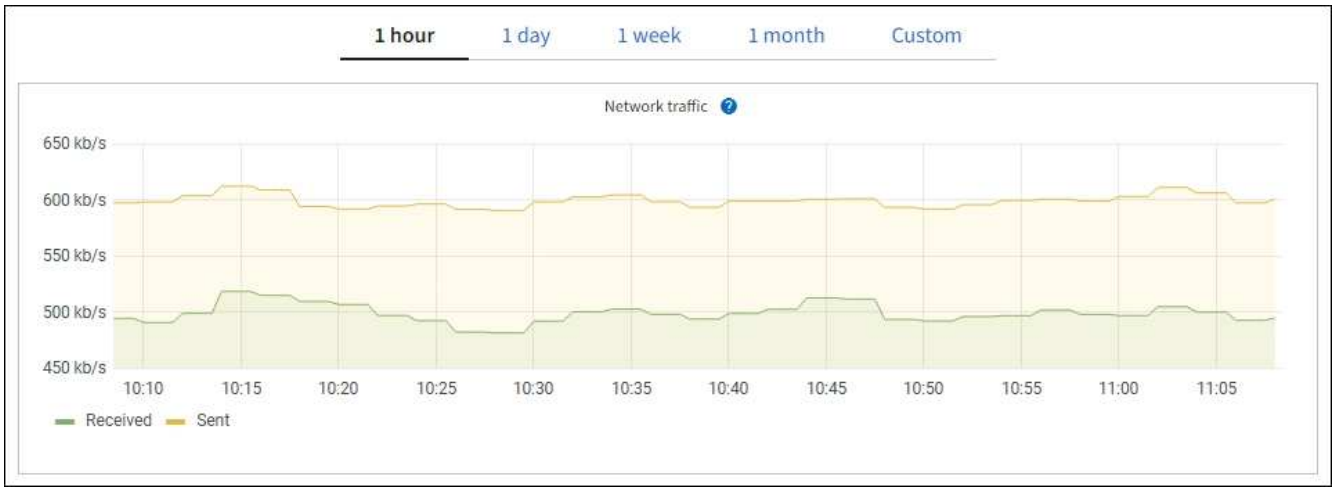
Champ dans la table Appliance	Description
Modèle d'appareil	Le numéro de modèle de cet appareil StorageGRID .
Nombre de disques défaillants du contrôleur de stockage	Le nombre de lecteurs qui ne sont pas optimaux.
Type de lecteur de données de stockage	Le type de lecteurs de l'appareil, tels que HDD (disque dur) ou SSD (disque SSD).
Taille du lecteur de données de stockage	La taille effective d'un lecteur de données.
Mode RAID de stockage	Le mode RAID de l'appareil.
Alimentation électrique globale	L'état de toutes les alimentations de l'appareil.
Contrôleur de calcul BMC IP	L'adresse IP du port du contrôleur de gestion de la carte mère (BMC) dans le contrôleur de calcul. Vous pouvez utiliser cette IP pour vous connecter à l'interface BMC afin de surveiller et de diagnostiquer le matériel de l'appliance. Ce champ n'est pas affiché pour les modèles d'appareils qui ne contiennent pas de BMC.
Numéro de série du contrôleur de calcul	Le numéro de série du contrôleur de calcul.
Matériel informatique	L'état du matériel du contrôleur de calcul.
Température du processeur du contrôleur de calcul	L'état de température du processeur du contrôleur de calcul.
Température du châssis du contrôleur de calcul	L'état de température du contrôleur de calcul.

a. Confirmez que tous les statuts sont « Nominaux ».

   Si un statut n'est pas « Nominal », vérifiez toutes les alertes actuelles.

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

   Le graphique du trafic réseau fournit un résumé 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

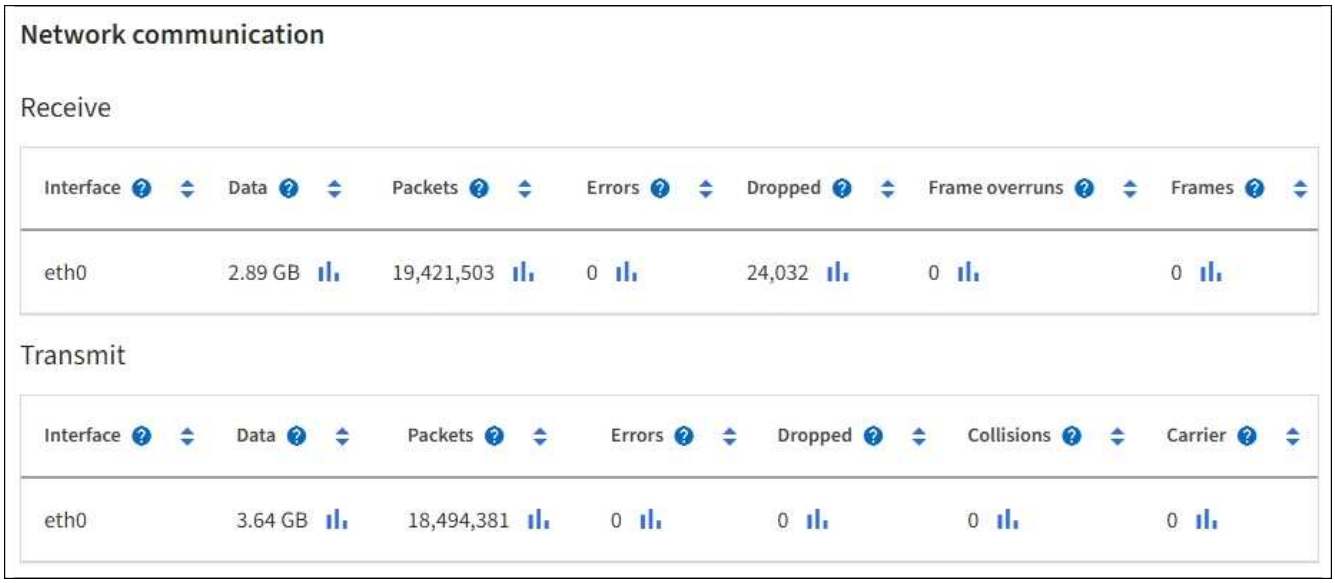
Utilisez le tableau suivant avec les valeurs de la colonne **Vitesse** du tableau Interfaces réseau pour déterminer si les quatre ports réseau 40/100-GbE de l'appliance ont été configurés pour utiliser le mode actif/de secours ou le mode LACP.

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

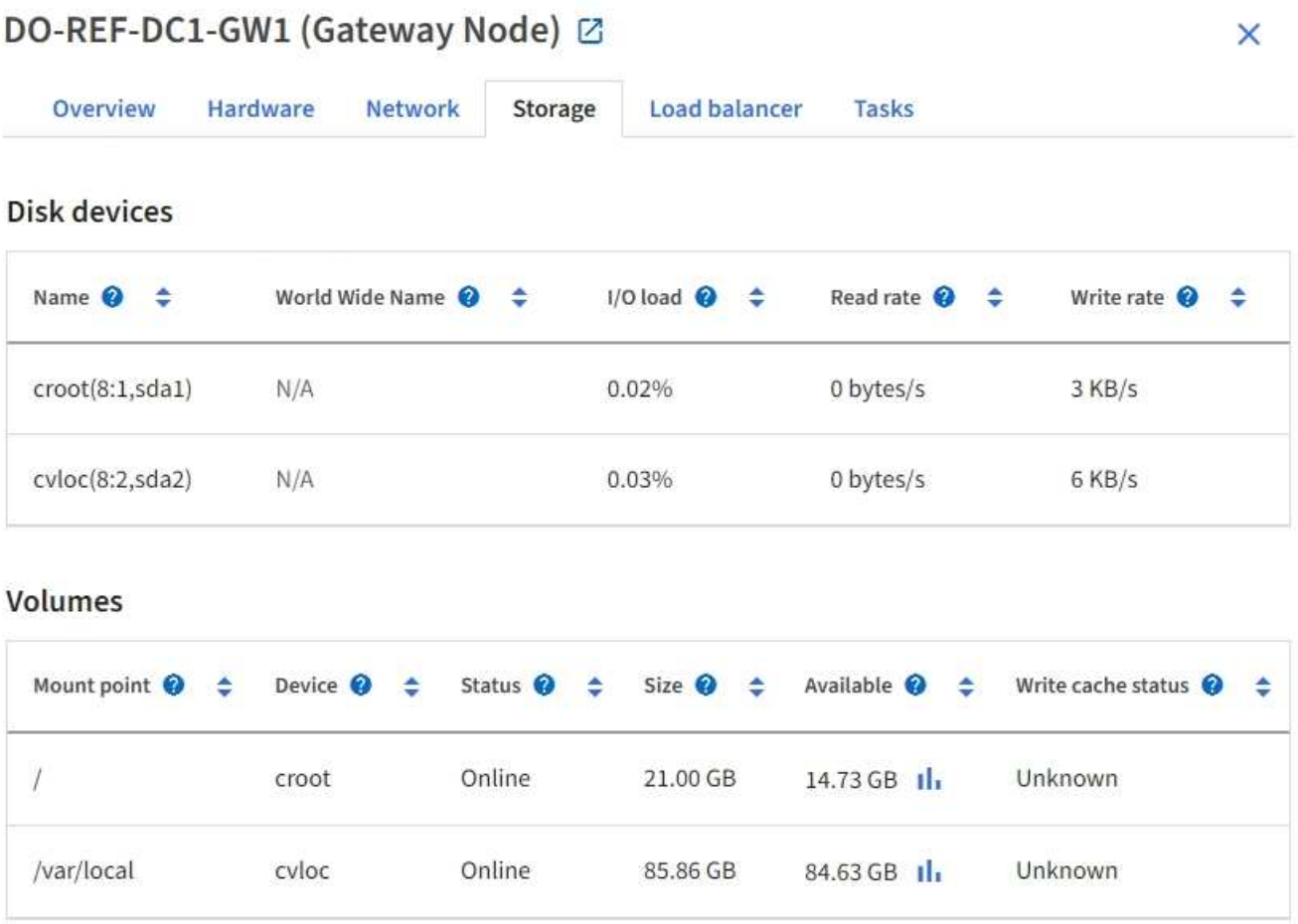
Mode de liaison	Mode liaison	Vitesse de liaison HIC individuelle (hic1, hic2, hic3, hic4)	Vitesse attendue du réseau grille/client (eth0, eth2)
Agrégat	LACP	100	400
Fixé	LACP	100	200
Fixé	Actif/Sauvegarde	100	100
Agrégat	LACP	40	160
Fixé	LACP	40	80
Fixé	Actif/Sauvegarde	40	40

b. Consultez 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.



5. Sélectionnez **Stockage** pour afficher des informations sur les périphériques de disque et les volumes sur le dispositif de services.



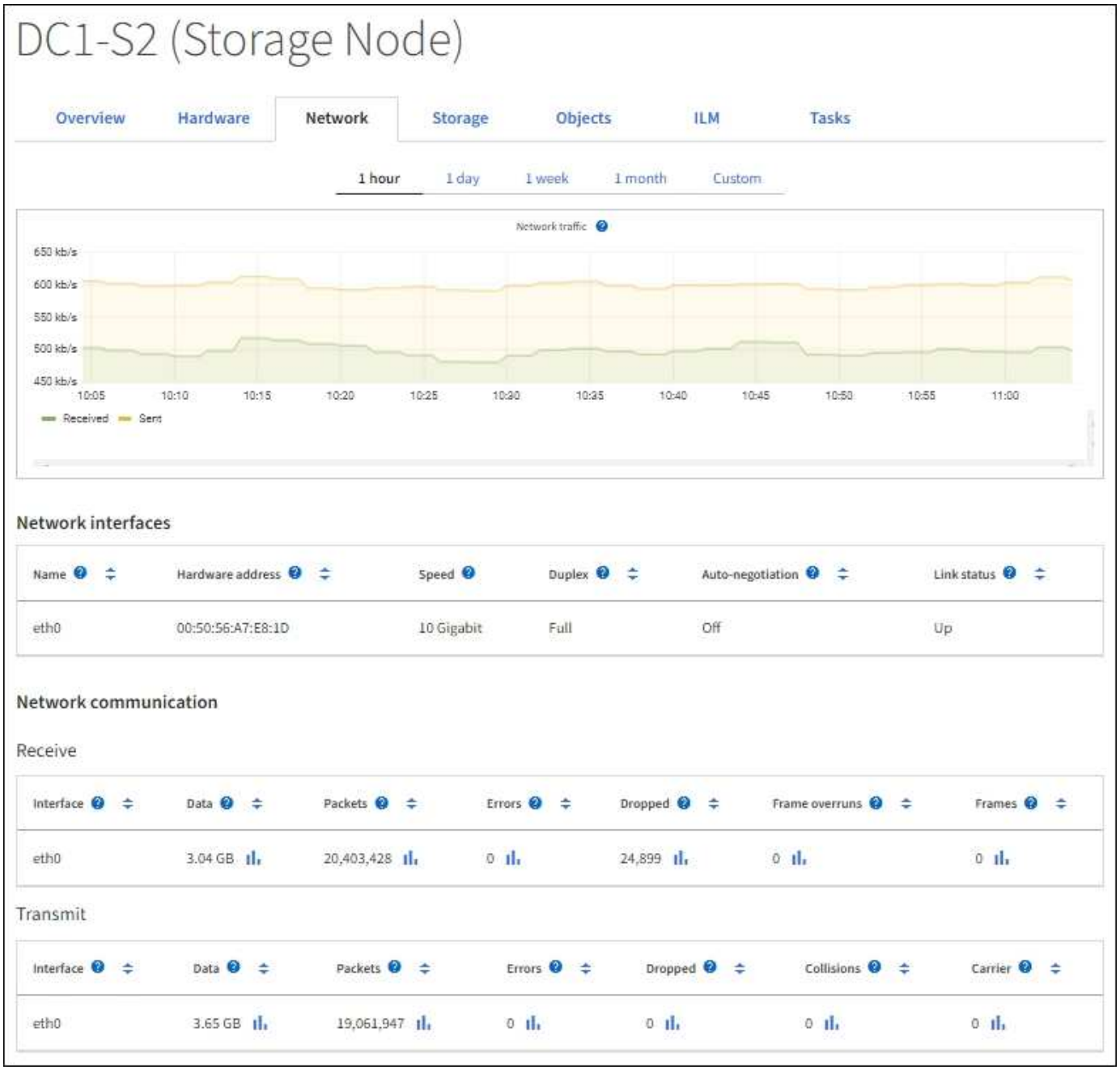
Afficher l'onglet Réseau

L'onglet Réseau affiche un graphique montrant 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 l'ensemble de la grille.

Pour afficher un intervalle de temps différent, sélectionnez l'un des contrôles au-dessus du graphique ou du diagramme. Vous pouvez afficher les informations disponibles pour des 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 dates et d'heures.

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 les compteurs d'erreurs signalés par le pilote.



Informations connexes

"Surveiller les connexions et les performances du réseau"

Afficher l'onglet Stockage

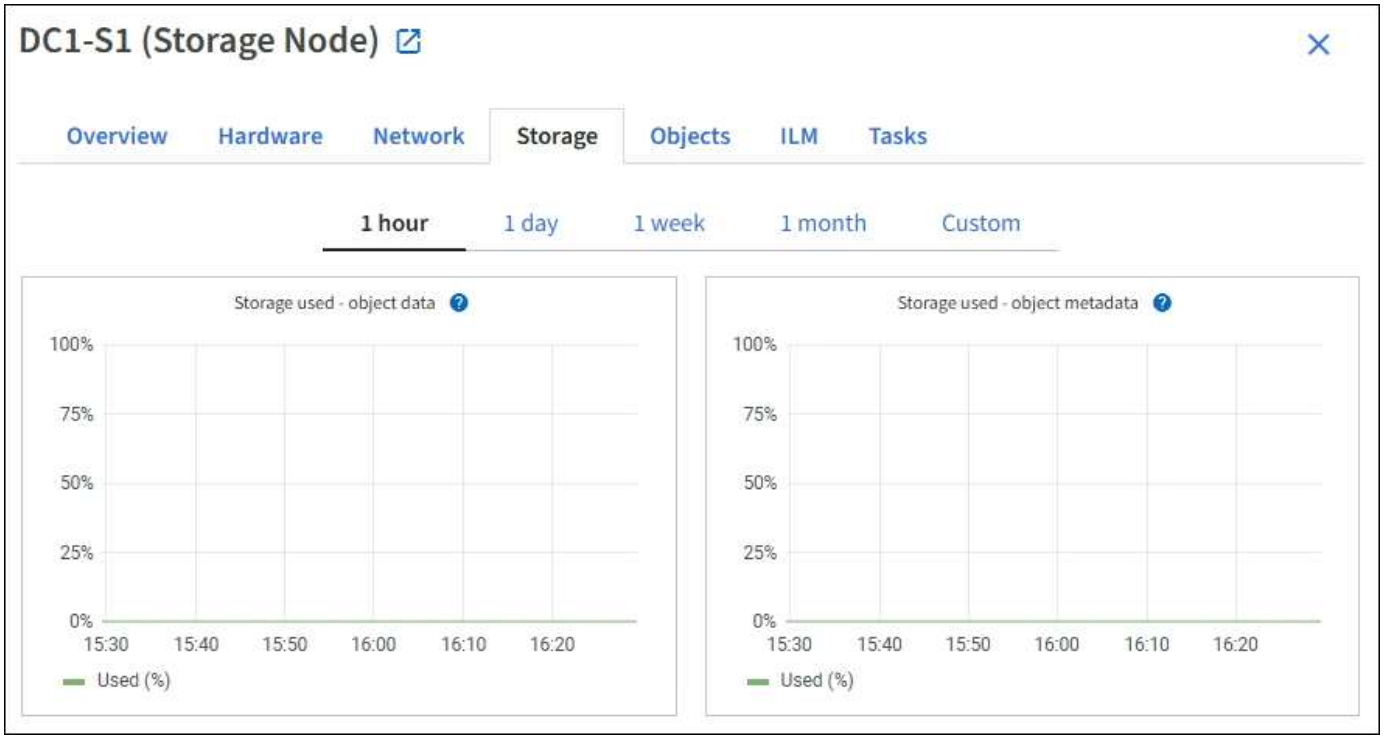
L'onglet Stockage résume la disponibilité du stockage et d'autres mesures de stockage.

L'onglet Stockage s'affiche pour tous les nœuds, chaque site et l'ensemble de la grille.

Graphiques utilisés pour le stockage

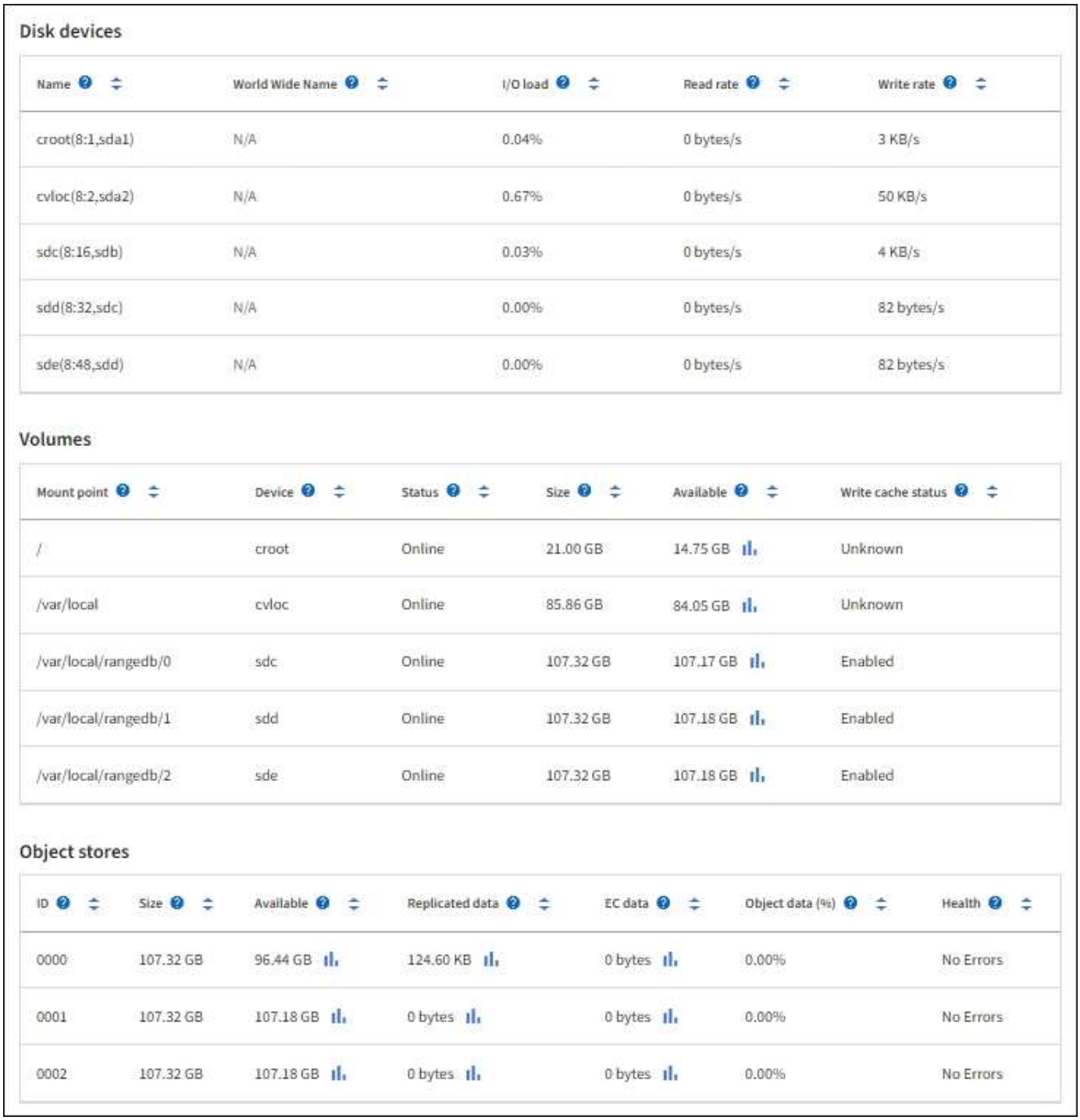
Pour les nœuds de stockage, chaque site et l'ensemble de la grille, l'onglet Stockage inclut des graphiques indiquant la quantité de stockage utilisée par les données d'objet et les métadonnées d'objet au fil du temps.

Lorsqu'un nœud n'est pas connecté au réseau, par exemple lors d'une mise à niveau ou d'un état déconnecté, certaines mesures peuvent être indisponibles ou exclues des totaux du site et du réseau. Une fois qu'un nœud se reconnecte au réseau, attendez quelques minutes que les valeurs se stabilisent.



Tableaux des périphériques de disque, des volumes et des magasins d'objets

Pour tous les nœuds, l'onglet Stockage contient des détails sur les périphériques de disque et les volumes sur le 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

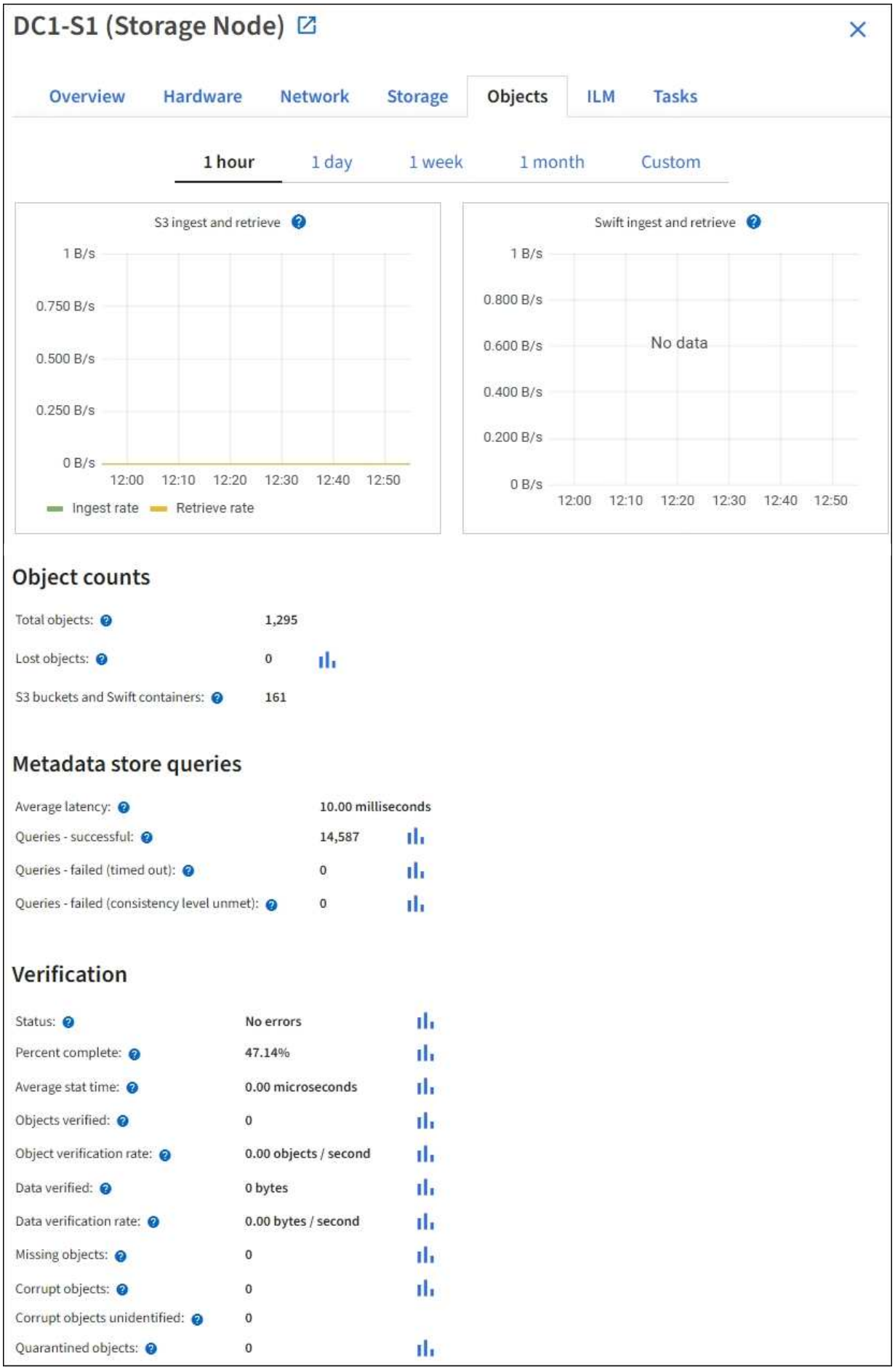
Informations connexes

"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.


DC1-S1 (Storage Node)
Overview
Hardware
Network
Storage
Objects
ILM
Tasks
1 hour
1 day
1 week
1 month
Custom
S3 ingest and retrieve
1 B/s
0.750 B/s
0.500 B/s
0.250 B/s
0 B/s
12:00
12:10
12:20
12:30
12:40
12:50
Ingest rate
Retrieve rate
Swift ingest and retrieve
1 B/s
0.800 B/s
0.600 B/s
0.400 B/s
0.200 B/s
0 B/s
No data
12:00
12:10
12:20
12:30
12:40
12:50
Object counts
Total objects: 1,295
Lost objects: 0
S3 buckets and Swift containers: 161
Metadata store queries
Average latency: 10.00 milliseconds
Queries - successful: 14,587
Queries - failed (timed out): 0
Queries - failed (consistency level unmet): 0
Verification
Status: No errors
Percent complete: 47.14%
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

Afficher l'onglet ILM

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

L'onglet ILM s'affiche pour chaque nœud de stockage, chaque site et la grille entière. Pour chaque site et la grille, l'onglet ILM affiche un graphique de la file d'attente ILM au fil du temps. Pour la grille, cet onglet fournit également le temps estimé pour effectuer une analyse ILM complète de tous les objets.

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

Informations connexes

- "Surveiller la gestion du cycle de vie des informations"
- "Administrer StorageGRID"

Utiliser 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 les exigences et les instructions complètes pour chaque option de cet onglet, consultez les éléments suivants :

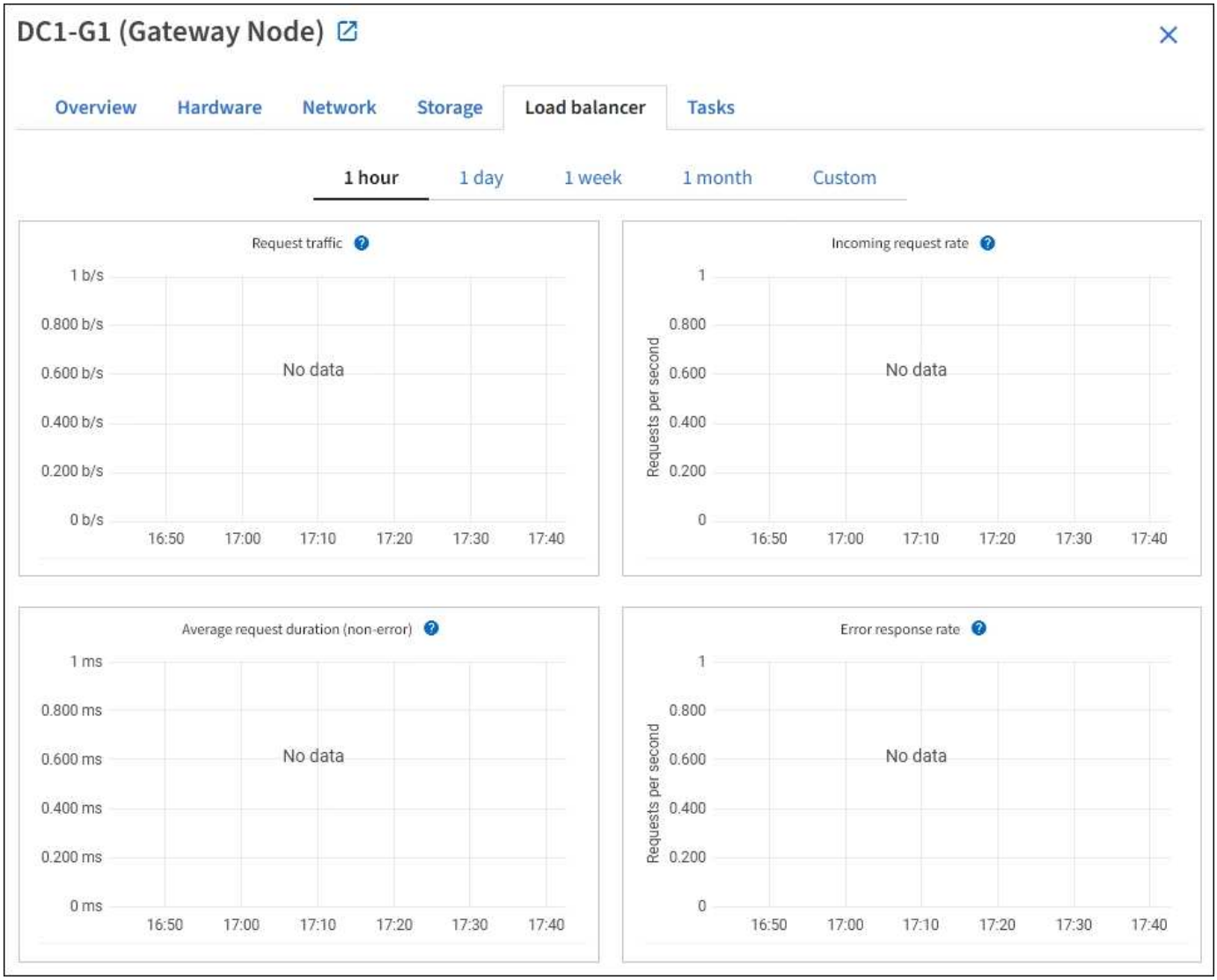
- "Renommer la grille, les sites et les nœuds"
- "Redémarrer le nœud de grille"
- "Mettre l'appareil en mode maintenance"

Afficher l'onglet Équilibreur de charge

L'onglet Équilibreur de charge inclut des graphiques de performances et de diagnostic liés au fonctionnement du service Équilibreur de charge.

L'onglet Équilibreur de charge s'affiche pour les nœuds d'administration et les nœuds de passerelle, chaque site et l'ensemble de la grille. Pour chaque site, l'onglet Équilibreur de charge fournit un résumé global des statistiques de tous les nœuds de ce site. Pour l'ensemble de la grille, l'onglet Équilibreur de charge fournit un résumé global des statistiques pour tous les sites.

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



Demande de trafic

Ce graphique fournit une moyenne mobile sur 3 minutes du débit des données transmises entre les points de terminaison 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 requête. Par conséquent, cette valeur peut différer du débit en temps réel à des taux de requête faibles ou pour des requêtes de très longue durée. Vous pouvez consulter l'onglet Réseau pour obtenir une vue plus réaliste du comportement actuel du réseau.

Taux de demandes entrantes

Ce graphique fournit une moyenne mobile sur 3 minutes du nombre de nouvelles requêtes par seconde, réparties par type de requête (GET, PUT, HEAD et DELETE). Cette valeur est mise à jour lorsque les en-têtes d'une nouvelle requête ont été validés.

Durée moyenne de la requête (sans erreur)

Ce graphique fournit une moyenne mobile sur 3 minutes des durées de requête, réparties par type de requête (GET, PUT, HEAD et DELETE). La durée de chaque demande commence lorsqu'un en-tête de demande est analysé par le service Load Balancer et se termine lorsque le corps de la réponse complet est renvoyé au

client.

Taux de réponse aux erreurs

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

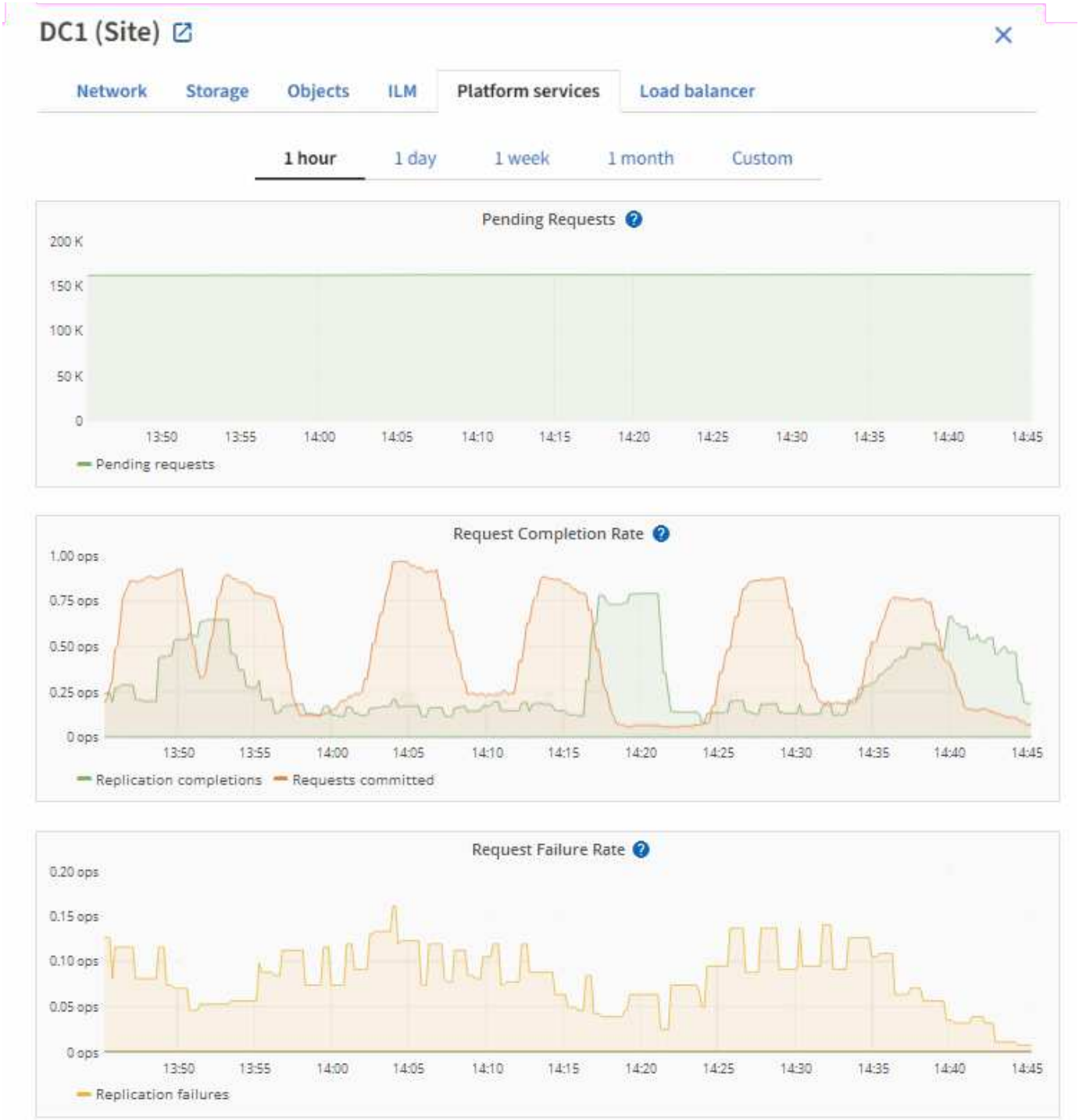
Informations connexes

- "Surveiller les opérations d'équilibrage de charge"
- "Administrer StorageGRID"

Afficher l'onglet Services de la plateforme

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

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



Pour plus d'informations sur les services de la plateforme S3, y compris les détails de dépannage, consultez le"instructions pour administrer StorageGRID" .

Afficher l'onglet Gérer les lecteurs

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

À l'aide de l'onglet Gérer les lecteurs, vous pouvez effectuer les opérations suivantes :

- Afficher la disposition des lecteurs de stockage de données dans l'appareil
- Afficher un tableau qui répertorie chaque emplacement de lecteur, type, état, version du micrologiciel et numéro de série
- Exécuter des fonctions de dépannage et de maintenance sur chaque lecteur

Pour accéder à l'onglet Gérer les lecteurs, vous devez disposer du"Administrateur de l'appareil de stockage ou autorisation d'accès root" .

Pour plus d'informations sur l'utilisation de l'onglet Gérer les lecteurs, consultez "Utiliser l'onglet Gérer les lecteurs" .

Afficher l'onglet Gestionnaire de système SANtricity (série E uniquement)

L'onglet SANtricity System Manager vous permet d'accéder à SANtricity System Manager sans avoir à configurer ou à connecter le port de gestion du dispositif de stockage. Vous pouvez utiliser cet onglet pour consulter les informations de diagnostic matériel et environnementales ainsi que les problèmes liés aux lecteurs.

> L'accès à SANtricity System Manager à partir du Grid Manager est généralement destiné uniquement à surveiller le matériel de l'appareil et à configurer E-Series AutoSupport. De nombreuses fonctionnalités et opérations au sein de SANtricity System Manager, telles que la mise à niveau du micrologiciel, ne s'appliquent pas à la surveillance de votre appliance StorageGRID . Pour éviter les problèmes, suivez toujours les instructions de maintenance matérielle de votre appareil. Pour mettre à niveau le micrologiciel SANtricity , consultez le "Procédures de configuration de maintenance" pour votre appareil de stockage.

> L'onglet Gestionnaire de système SANtricity s'affiche uniquement pour les nœuds d'appliance de stockage utilisant du matériel de la série E.

En utilisant SANtricity System Manager, vous pouvez effectuer les opérations suivantes :

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

> Pour utiliser SANtricity System Manager pour configurer un proxy pour E-Series AutoSupport, voir"Envoyer des packages AutoSupport de la série E via StorageGRID" .

Pour accéder à SANtricity System Manager via Grid Manager, vous devez disposer du"Administrateur de l'appareil de stockage ou autorisation d'accès root" .

> Vous devez disposer du micrologiciel 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.

Vous pouvez utiliser le lien SANtricity System Manager pour ouvrir SANtricity System Manager dans une nouvelle fenêtre de navigateur pour une visualisation plus facile.

Pour voir les détails des performances au niveau de la baie de stockage et de l'utilisation de la capacité, placez votre curseur sur chaque graphique.

Pour plus de détails sur l'affichage des informations accessibles depuis l'onglet SANtricity System Manager, voir "Documentation NetApp E-Series et SANtricity" .

Informations à suivre 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 ne sont pas disponibles, 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 Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Tu as"autorisations d'accès spécifiques" .

À 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.

Que surveiller	Fréquence
"État de santé du système"	Tous les jours
Taux auquel"Capacité de l'objet et des métadonnées du nœud de stockage" est consommé	Hebdomadaire
"Opérations de gestion du cycle de vie de l'information"	Hebdomadaire
"Ressources réseau et système"	Hebdomadaire
"Activité des locataires"	Hebdomadaire
"Opérations client S3"	Hebdomadaire
"Opérations d'équilibrage de charge"	Après la configuration initiale et après toute modification de configuration
"Connexions de la fédération de réseau"	Hebdomadaire

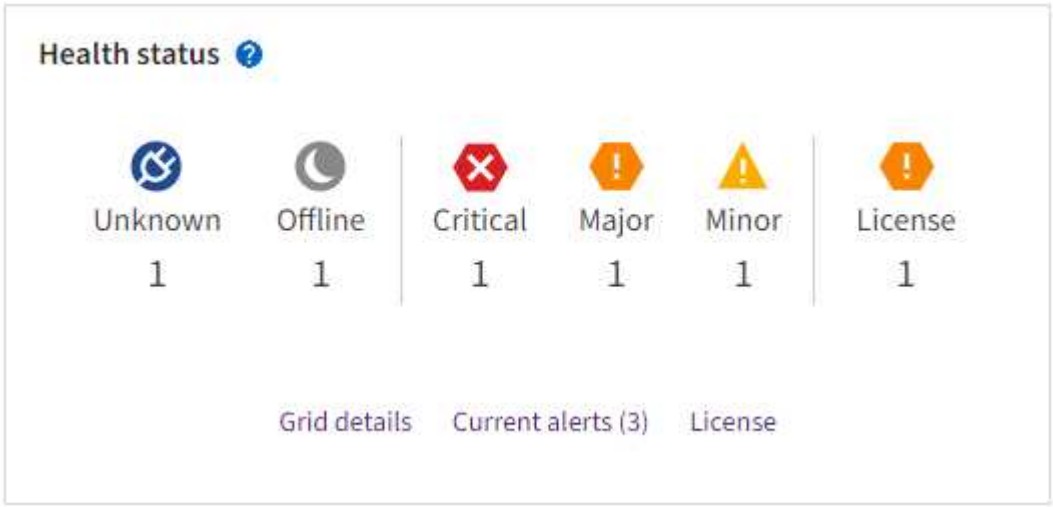
Surveiller la santé du système

Surveillez quotidiennement l'état de santé général de votre système StorageGRID .

À propos de cette tâche

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

Pour être averti des alertes dès qu'elles sont déclenchées, vous pouvez "configurer des notifications par e-mail pour les alertes" ou"configurer les interruptions SNMP" .



Lorsque des problèmes surviennent, des liens apparaissent qui vous permettent d'afficher des détails supplémentaires :

Lien	Apparaît lorsque…
Détails de la grille	Tous les nœuds sont déconnectés (état de connexion inconnu ou administrativement hors service).
Alertes actuelles (critiques, majeures, mineures)	Les alertes sontactuellement actif .
Alertes récemment résolues	Alertes déclenchées la semaine dernièresont maintenant résolus .
Licence	Il y a un problème avec la licence du logiciel pour ce système StorageGRID . Vous pouvez "mettre à jour les informations de licence selon les besoins" .

Surveiller les états de connexion des nœuds

Si un ou plusieurs nœuds sont déconnectés de la grille, les opérations critiques de StorageGRID peuvent être affectées. Surveillez les états de connexion des nœuds et résolvez rapidement tout problème.

Icône	Description	Action requise
	**Non connecté - Inconnu** Pour une raison inconnue, un nœud est déconnecté ou les services sur le nœud sont interrompus de manière inattendue. Par exemple, un service sur le nœud peut être arrêté ou le nœud peut avoir perdu sa connexion réseau en raison d'une panne de courant ou d'une panne inattendue. L'alerte **Impossible de communiquer avec le nœud** peut également être déclenchée. D'autres alertes peuvent également être actives.	Nécessite une attention immédiate. Sélectionnez chaque alerte et suivez les actions recommandées. Par exemple, vous devrez peut-être redémarrer un service qui s'est arrêté ou redémarrer l'hôte du nœud. **Remarque** : un nœud peut apparaître comme inconnu lors des opérations d'arrêt géré. Vous pouvez ignorer l'état Inconnu dans ces cas.
	**Non connecté - Administrativement en panne** Pour une raison attendue, le nœud n'est pas connecté au réseau. Par exemple, le nœud ou les services sur le nœud ont été arrêtés correctement, le nœud redémarre ou le logiciel est en cours de mise à niveau. Une ou plusieurs alertes peuvent également être actives. En fonction du problème sous-jacent, ces nœuds reviennent souvent en ligne sans intervention.	Déterminez si des alertes affectent ce nœud. Si une ou plusieurs alertes sont actives,sélectionnez chaque alerte et suivez les actions recommandées.
	**Connecté** Le nœud est connecté au réseau.	Aucune action requise.

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 est également affichée 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 désactivée.

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

En option, vous avez regardé la vidéo : "Vidéo : Aperçu des alertes"

Le tableau suivant décrit les informations affichées dans le gestionnaire de grille pour les alertes actuelles et résolues.

En-tête de colonne	Description
Nom ou titre	Le nom de l'alerte et sa description.
Gravité	La 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 niveau de gravité. **Critique** : une condition anormale existe qui a arrêté les opérations normales d'un nœud ou d'un service StorageGRID . Vous devez résoudre le problème sous-jacent immédiatement. Une interruption de service et une perte de données peuvent survenir si le problème n'est pas résolu. **Majeur** : Une condition anormale existe qui affecte les opérations en cours ou approche le seuil d'une alerte critique. Vous devez enquêter sur les alertes majeures et résoudre tous les problèmes sous-jacents pour garantir que la condition anormale n'arrête pas le fonctionnement normal d'un nœud ou d'un service StorageGRID . **Mineur** : Le système fonctionne normalement, mais une condition anormale existe qui pourrait affecter la capacité du système à fonctionner si elle persiste. Vous devez surveiller et résoudre les alertes mineures qui ne disparaissent pas d'elles-mêmes pour vous assurer qu'elles n'entraînent pas un problème plus grave.
Le temps déclenché	**Alertes actuelles** : La date et l'heure auxquelles l'alerte a été déclenchée dans votre 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 (*newest*) et de l'instance la plus ancienne de l'alerte (*oldest*). **Alertes résolues** : Il y a combien de temps l'alerte a été déclenchée.
Site/Nœud	Le nom du site et du nœud où l'alerte se produit ou s'est produite.

En-tête de colonne	Description
Statut	Que l'alerte soit active, silencieuse ou résolue. Si plusieurs alertes sont regroupées et que **Toutes les alertes** est sélectionné dans la liste déroulante, la ligne de titre indique combien d'instances de cette alerte sont actives et combien d'instances ont été désactivées.
Temps résolu (alertes résolues uniquement)	Il y a combien de temps l'alerte a été résolue.
Valeurs actuelles ou *valeurs de données*	La valeur de la métrique qui a provoqué le 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 **Faible stockage de données d'objet** incluent le pourcentage d'espace disque utilisé, la quantité totale d'espace disque et la quantité d'espace disque utilisée. **Remarque :** si plusieurs alertes actuelles sont regroupées, les valeurs actuelles ne sont pas affichées dans la ligne de titre.
Valeurs déclenchées (alertes résolues uniquement)	La valeur de la métrique qui a provoqué le 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 **Faible stockage de données d'objet** incluent 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 une liste des alertes dans ces catégories. Vous pouvez également afficher les détails d'une alerte en sélectionnant **Nœuds** > ***node*** > **Aperçu**, puis en sélectionnant l'alerte dans le tableau Alertes.

   Par défaut, les alertes actuelles sont affichées comme suit :

   - Les alertes déclenchées le plus récemment sont affichées en premier.
   - Plusieurs alertes du même type sont affichées sous forme de groupe.
   - Les alertes qui ont été désactivées ne sont pas affichées.
   - Pour une alerte spécifique sur un nœud spécifique, si les seuils sont atteints pour plusieurs niveaux de gravité, seule l'alerte la plus grave est affichée. Autrement dit, si les seuils d'alerte sont atteints pour les niveaux de gravité mineur, majeur et critique, seule l'alerte critique est affichée.

     La page Alertes actuelles est actualisée toutes les deux minutes.

2. Pour développer des groupes d'alertes, sélectionnez le curseur vers le bas . Pour réduire les alertes individuelles dans un groupe, sélectionnez le curseur vers le haut , 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 actuelles ou les groupes d'alertes, 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 au sein de chaque groupe sont triés. Par exemple, vous souhaiterez peut-être trier les alertes d'un groupe par

Heure de déclenchement pour trouver l'instance la plus récente d'une alerte spécifique.

- Lorsque **Alertes de groupe** est effacé, la liste entière des alertes est triée. Par exemple, vous souhaiterez peut-être trier toutes les alertes par **Nœud/Site** pour voir toutes les alertes affectant un nœud spécifique.

5. Pour filtrer les alertes actuelles par statut (**Toutes les alertes**, **Actif** ou **Silencieux**), utilisez le menu déroulant en haut du tableau.

   Voir "Notifications d'alerte silencieuses" .

6. Pour trier les alertes résolues :
   - Sélectionnez une période dans le menu déroulant **Lors du déclenchement**.
   - Sélectionnez une ou plusieurs gravités 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 liées à une règle d'alerte spécifique.
   - Sélectionnez un ou plusieurs nœuds dans le menu déroulant **Nœud** 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 « Désactiver cette alerte » pour désactiver la règle d'alerte qui a provoqué le déclenchement de cette alerte.

   Vous devez avoir le"Gérer les alertes ou l'autorisation d'accès root" pour faire taire une règle d'alerte.

   > Soyez prudent lorsque vous décidez de désactiver une règle d'alerte. Si une règle d'alerte est désactivée, vous risquez de ne pas détecter un problème sous-jacent jusqu'à ce qu'il empêche une opération critique de se terminer.

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 apparaît, 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 provoqué le déclenchement de cette alerte.

    Vous devez avoir le"Gérer les alertes ou l'autorisation d'accès root" pour modifier une règle d'alerte.

    > Soyez prudent lorsque vous décidez de modifier une règle d'alerte. Si vous modifiez les valeurs de déclenchement, vous risquez de ne pas détecter un problème sous-jacent jusqu'à ce qu'il empêche une opération critique de se terminer.

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

Surveiller la capacité de stockage

Surveillez l'espace utilisable total disponible pour garantir que le système StorageGRID ne manque pas d'espace de stockage pour les objets ou pour les métadonnées des objets.

StorageGRID stocke les données d'objet et les métadonnées d'objet séparément et réserve une quantité spécifique d'espace pour une base de données Cassandra distribuée contenant des métadonnées d'objet. Surveillez la quantité totale d'espace consommée pour les objets et pour les métadonnées des objets, ainsi que les tendances de la quantité d'espace consommée pour chacun. Cela vous permettra de planifier à l'avance l'ajout de nœuds et d'éviter toute interruption de service.

Tu peux"afficher les informations sur la capacité de stockage" pour l'ensemble de la grille, pour chaque site et pour chaque nœud de stockage de votre système StorageGRID .

Surveiller la capacité de stockage de l'ensemble du réseau

Surveillez la capacité de stockage globale de votre grille pour garantir qu'il reste suffisamment d'espace libre pour les données d'objet et les métadonnées d'objet. Comprendre comment la capacité de stockage évolue au fil du temps peut vous aider à planifier l'ajout de nœuds de stockage ou de volumes de stockage avant que la capacité de stockage utilisable du réseau ne soit consommée.

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

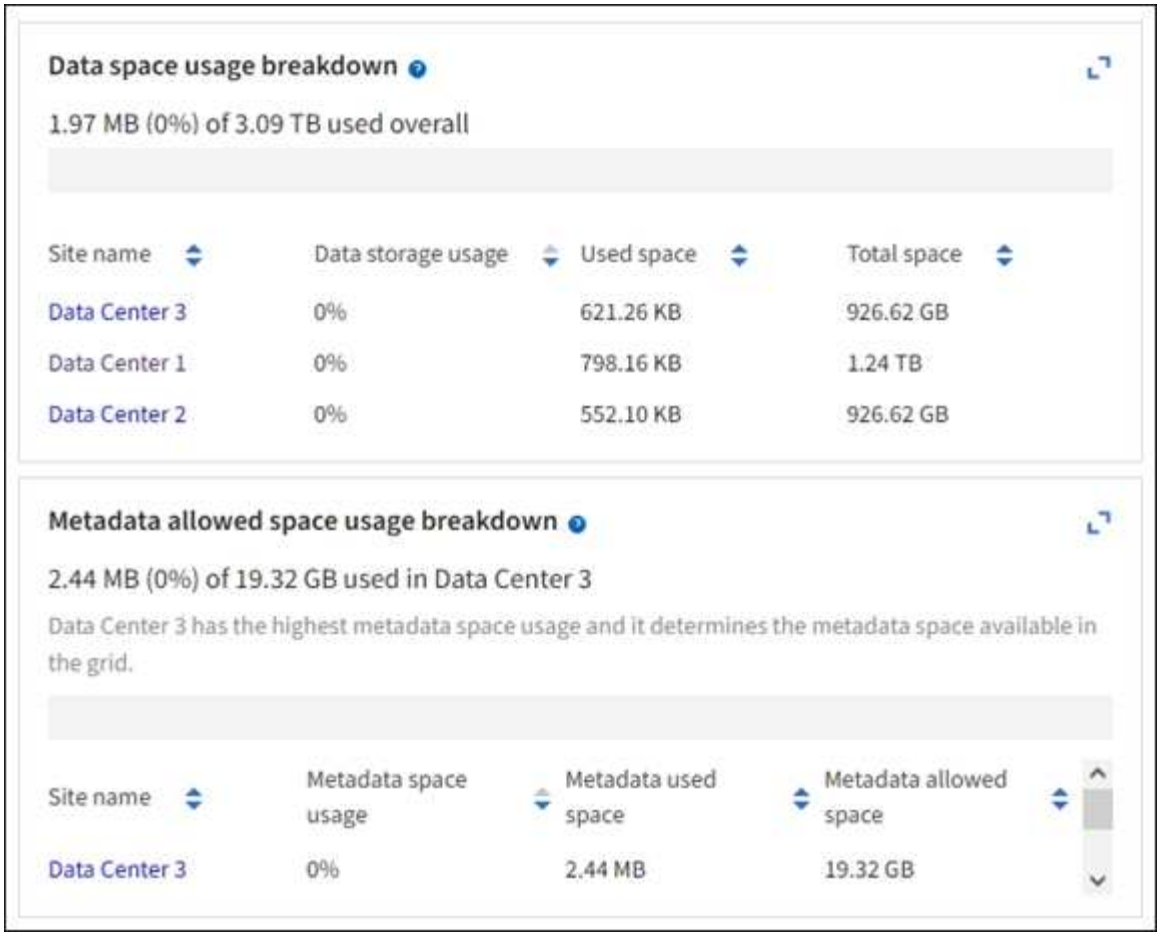
Étapes

1. Évaluez la quantité de stockage disponible pour l'ensemble du réseau et pour chaque centre de données.

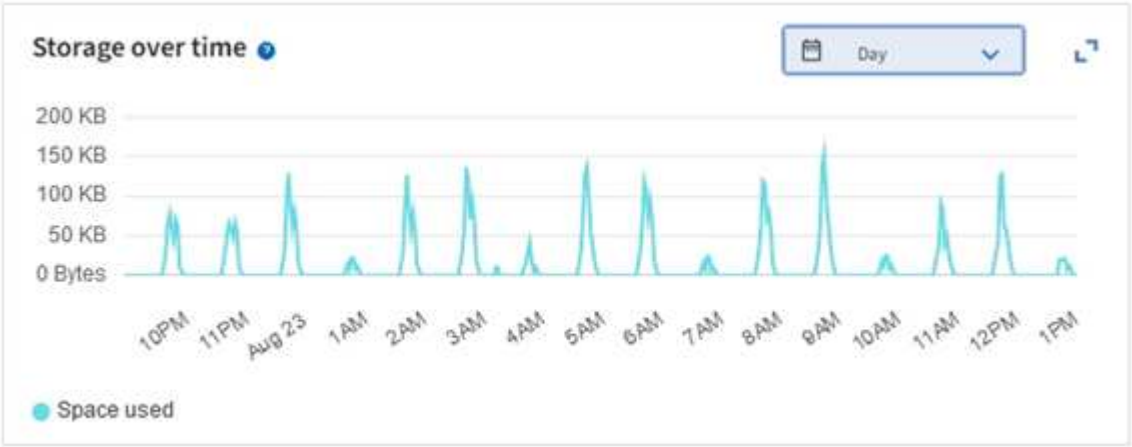
   a. Sélectionnez **Tableau de bord > Aperçu**.

   b. Notez les valeurs sur les cartes de répartition de l'utilisation de l'espace de données et de répartition de l'utilisation de l'espace autorisé des métadonnées. Chaque carte répertorie un pourcentage d'utilisation du stockage, la capacité de l'espace utilisé et l'espace total disponible ou autorisé par le site.

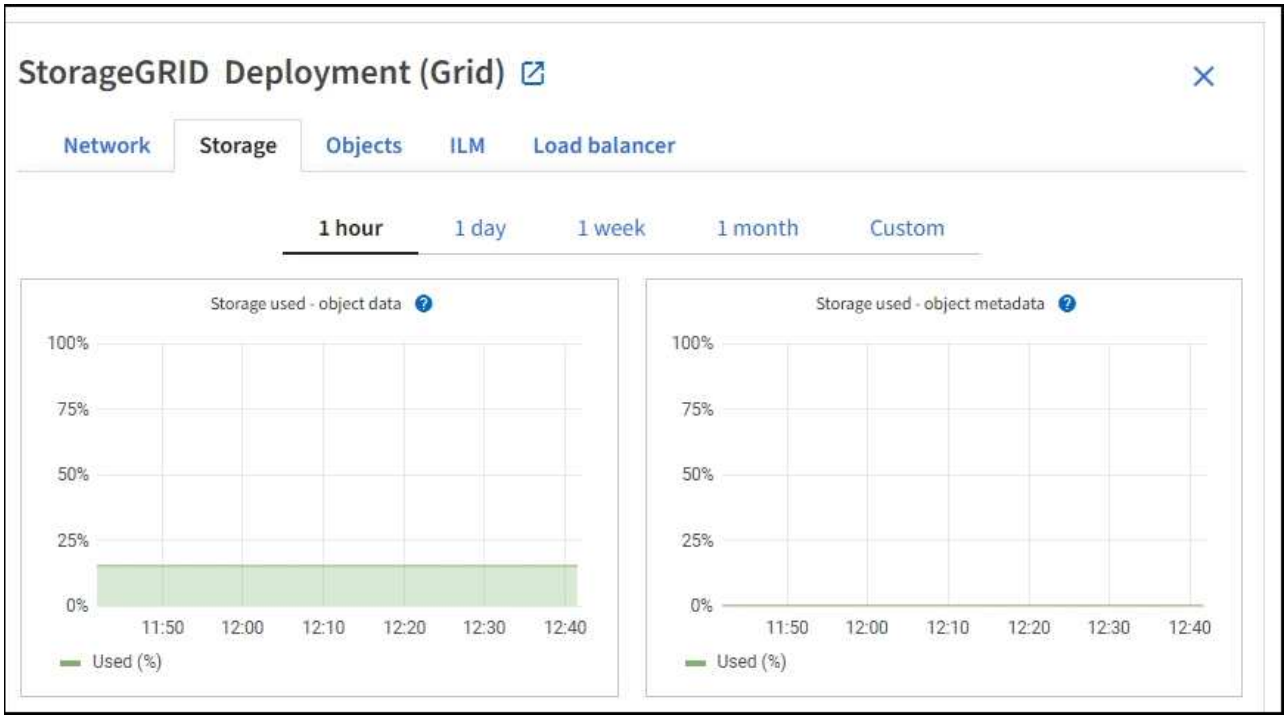
      Le résumé n'inclut pas les supports d'archives.



a. Notez le tableau sur la carte Stockage au fil du temps. Utilisez la liste déroulante de la période pour vous aider à déterminer la vitesse à laquelle le stockage est consommé.



2. Utilisez la page Nœuds pour obtenir des détails supplémentaires sur la quantité de stockage utilisée et la quantité de stockage restant disponible sur la grille pour les données d'objet et les métadonnées d'objet.
   a. Sélectionnez **NODES**.
   b. Sélectionnez ***grid*** > **Stockage**.



c. Placez votre curseur sur les graphiques **Stockage utilisé - données d'objet** et **Stockage utilisé - métadonnées d'objet** pour voir la quantité de stockage d'objet et de stockage de métadonnées d'objet disponible pour l'ensemble de la grille, et 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, tels que les nœuds hors ligne.

3. Prévoyez d'effectuer une extension pour ajouter des nœuds de stockage ou des volumes de stockage avant que la capacité de stockage utilisable du réseau ne soit consommée.

   Lorsque vous planifiez le calendrier d'une extension, tenez compte du temps qu'il faudra pour acquérir et installer un stockage supplémentaire.

   > ⓘ Si votre stratégie ILM utilise le codage d'effacement, vous préférerez peut-être étendre lorsque les nœuds de stockage existants sont remplis à environ 70 % pour réduire le nombre de nœuds à ajouter.

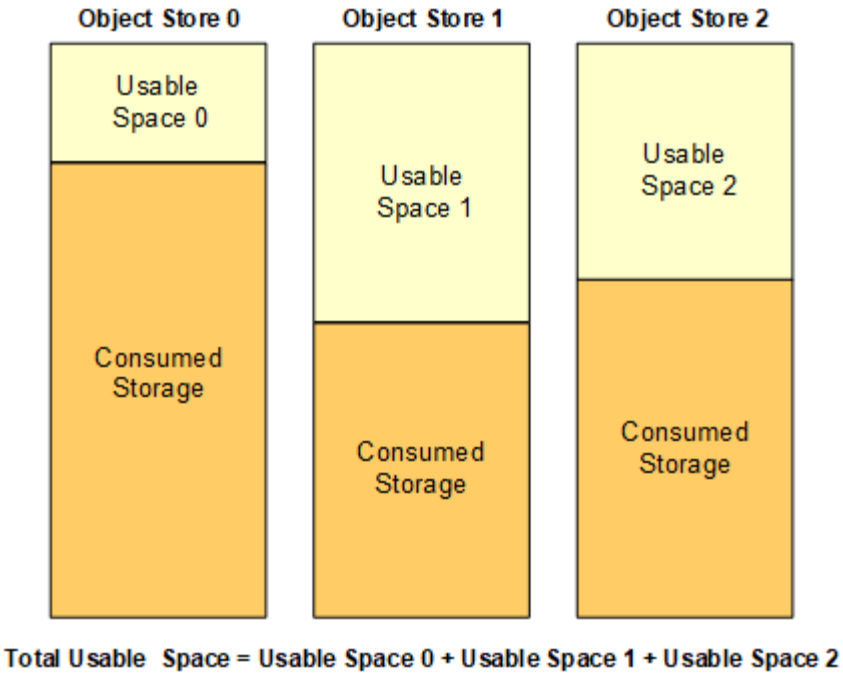
   Pour plus d'informations sur la planification d'une extension de stockage, consultez le"instructions pour étendre StorageGRID" .

Surveiller la capacité de stockage pour chaque nœud de stockage

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

À propos de cette tâche

L'espace utilisable est la quantité d'espace de stockage disponible pour stocker des objets. L'espace utilisable total pour un nœud de stockage est calculé en additionnant l'espace disponible sur tous les magasins d'objets au sein du nœud.



Étapes

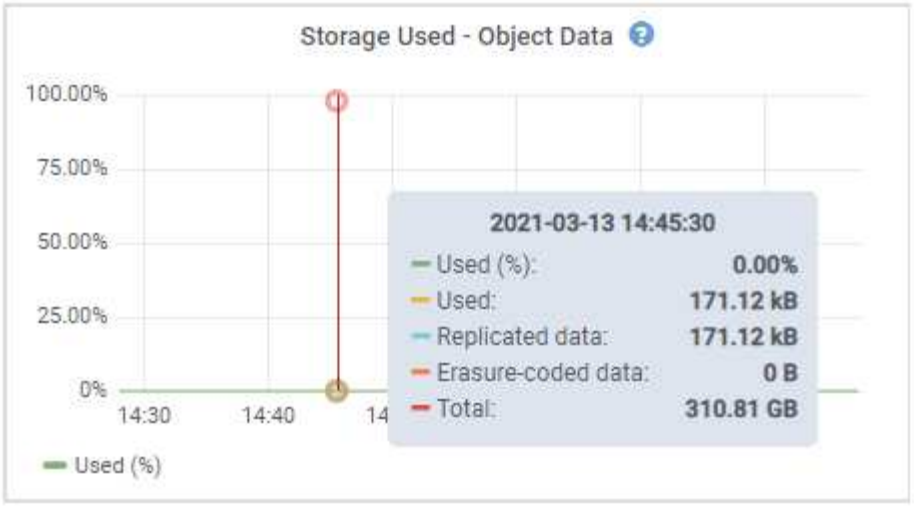
1. Sélectionnez **NODES** > ***Storage Node*** > **Storage**.

   Les graphiques et les tableaux du nœud apparaissent.

2. Positionnez votre curseur sur le graphique Stockage utilisé - données de l'objet.

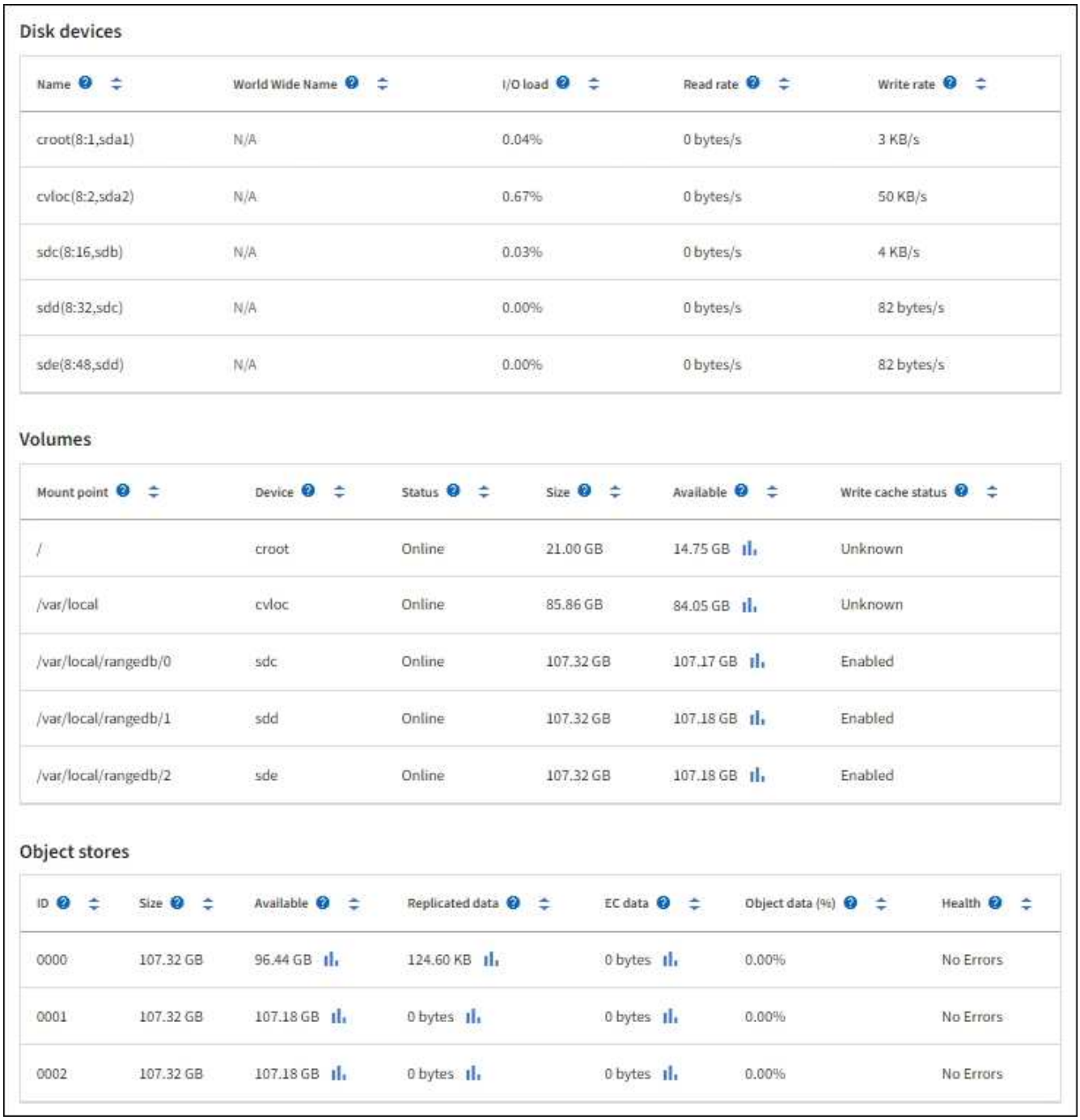
   Les valeurs suivantes sont affichées :

   - **Utilisé (%)** : Le pourcentage de l'espace total utilisable qui a été utilisé pour les données de l'objet.
   - **Utilisé** : la quantité d'espace total utilisable qui a été utilisée pour les données de l'objet.
   - **Données répliquées** : une estimation de la quantité de données d'objet répliquées sur ce nœud, ce site ou cette grille.
   - **Données codées par effacement** : une estimation de la quantité de données d'objet codées par effacement sur ce nœud, ce site ou cette grille.
   - **Total**: La quantité totale d'espace utilisable sur ce nœud, ce site ou cette grille. La valeur utilisée est la `storagegrid_storage_utilization_data_bytes` métrique.



3. Consultez 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 de 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

4. Surveillez les valeurs au fil du temps pour estimer la vitesse à laquelle l'espace de stockage utilisable est consommé.
5. Pour maintenir le fonctionnement normal du système, ajoutez des nœuds de stockage, ajoutez des volumes de stockage ou archivez les données d'objet avant que l'espace utilisable ne soit consommé.

   Lorsque vous planifiez le calendrier d'une extension, tenez compte du temps qu'il faudra pour acquérir et installer un stockage supplémentaire.

   > Si votre stratégie ILM utilise le codage d'effacement, vous préférerez peut-être étendre 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, consultez le"instructions pour

étendre StorageGRID" .

Le"Faible stockage de données d'objets" l'alerte est déclenchée lorsqu'il ne reste pas suffisamment d'espace pour stocker les données d'objet sur un nœud de stockage.

Surveiller la capacité des métadonnées des objets pour chaque nœud de stockage

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

À propos de cette tâche

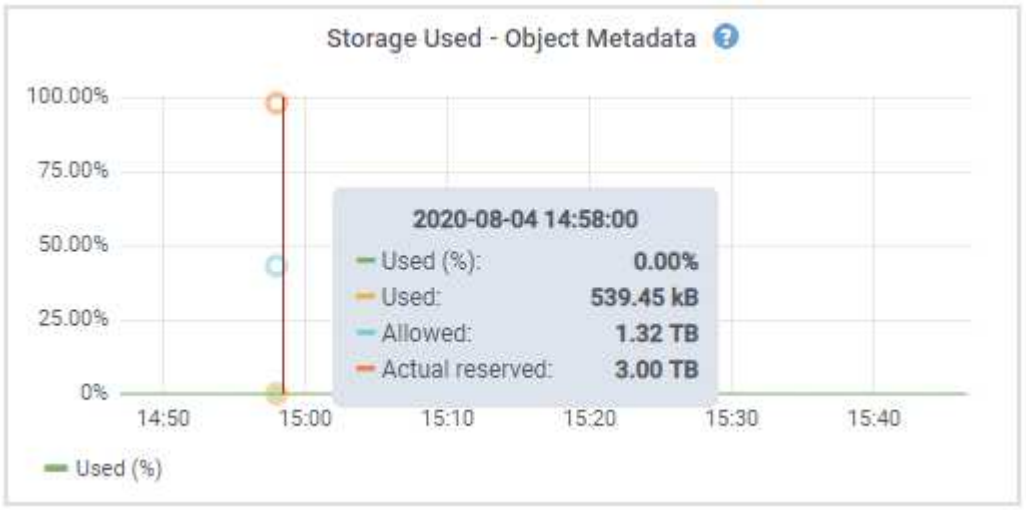
StorageGRID conserve trois copies des métadonnées d'objet sur chaque site pour assurer la redondance et protéger les métadonnées d'objet contre la perte. Les trois copies sont réparties uniformément sur tous les nœuds de stockage de chaque site à l'aide de l'espace réservé aux métadonnées sur le volume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

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

Certains des facteurs qui peuvent augmenter l'utilisation des métadonnées incluent la taille et la quantité de métadonnées et de balises utilisateur, le nombre total de parties dans un téléchargement en plusieurs parties et la fréquence des modifications des emplacements de stockage ILM.

Étapes

1. Sélectionnez **NODES** > ***Storage Node*** > **Storage**.
2. Placez votre curseur sur le graphique Stockage utilisé - métadonnées de l'objet pour voir les valeurs pour une période spécifique.



Utilisé (%)

Le pourcentage de l'espace de métadonnées autorisé qui a été utilisé sur ce nœud de stockage.

Métriques 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.

Métrique Prometheus : `storagegrid_storage_utilization_metadata_bytes`

Autorisé

L'espace autorisé pour les métadonnées d'objet sur ce nœud de stockage. Pour savoir comment cette valeur est déterminée pour chaque nœud de stockage, consultez le"description complète de l'espace de métadonnées autorisé" .

Métrique Prometheus : `storagegrid_storage_utilization_metadata_allowed_bytes`

Réel réservé

L'espace réel réservé aux métadonnées sur ce nœud de stockage. Comprend l'espace autorisé et l'espace requis pour les opérations de métadonnées essentielles. Pour savoir comment cette valeur est calculée pour chaque nœud de stockage, consultez le"description complète de l'espace réservé réel pour les métadonnées" .

La métrique Prometheus sera ajoutée 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, tels que les nœuds hors ligne.

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

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

Lorsque vous ajoutez les nouveaux nœuds, le système rééquilibre automatiquement les métadonnées des objets sur tous les nœuds de stockage du site. Voir le"instructions pour étendre un système StorageGRID" .

Surveiller 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."étendre une grille" .

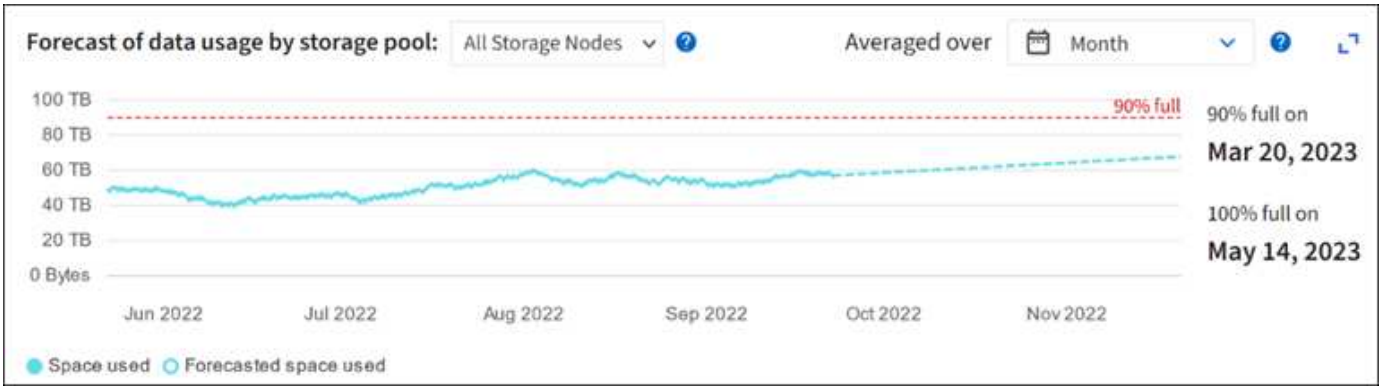
Si vous remarquez que le taux de consommation change au fil du temps, sélectionnez une plage plus courte dans le menu déroulant **Moyenne sur** pour refléter uniquement les modèles d'ingestion les plus récents. Si vous remarquez des tendances saisonnières, sélectionnez une plage plus longue.

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

Étapes

1. Sur le tableau de bord, sélectionnez **Stockage**.
2. Consultez les cartes du tableau de bord, les prévisions d'utilisation des données par pool de stockage et les prévisions d'utilisation des métadonnées par site.
3. Utilisez ces valeurs pour estimer quand vous devrez ajouter de nouveaux nœuds de stockage pour le

stockage des données et des métadonnées.



Surveiller la gestion du cycle de vie des informations

Le système de gestion du cycle de vie de l'information (ILM) fournit une gestion des données pour tous les objets stockés sur la grille. Vous devez surveiller les opérations ILM pour comprendre si le réseau peut gérer la charge actuelle ou si davantage de ressources sont nécessaires.

À propos de cette tâche

Le système StorageGRID gère les objets en appliquant les politiques ILM actives. Les politiques ILM et 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 ILM, ce qui oblige le système à mettre en file d'attente les objets dont les instructions de placement ILM ne peuvent pas être exécutées en temps quasi réel. Vous devez surveiller si StorageGRID suit les actions du client.

Utiliser l'onglet du tableau de bord Grid Manager

Étapes

Utilisez l'onglet ILM sur le tableau de bord du Grid Manager pour surveiller les opérations ILM :

1. Sign in au gestionnaire de grille.
2. Depuis le tableau de bord, sélectionnez l'onglet ILM et notez les valeurs sur la carte File d'attente ILM (Objets) et la carte de taux d'évaluation ILM.

   Des pics temporaires dans la carte de file d'attente ILM (Objets) sur le tableau de bord sont à prévoir. Mais si la file d'attente continue d'augmenter et ne diminue jamais, la grille a besoin de plus de ressources pour fonctionner efficacement : soit plus de nœuds de stockage, soit, si la politique ILM place les objets dans des emplacements distants, plus de bande passante réseau.

Utiliser la page NODES

Étapes

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

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

1. Sélectionnez **NODES**.
2. Sélectionnez ***nom de la grille*** > **ILM**.
3. Placez votre curseur 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 d'opérations client (par exemple, l'ingestion).
   - **Objets en file d'attente (de toutes les opérations)** : Le nombre total d'objets en attente d'évaluation ILM.
   - **Taux d'analyse (objets/s)** : Le taux auquel les objets de la grille sont analysés et mis en file d'attente pour ILM.
   - **Taux d'évaluation (objets/sec)** : Le taux actuel auquel les objets sont évalués par rapport à la politique ILM dans la grille.
4. Dans la section File d'attente ILM, examinez les attributs suivants.

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

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

     Une analyse complète ne garantit pas que l'ILM a été appliqué à tous les objets.

   - **Réparations tentées** : Nombre total d'opérations de réparation d'objets pour les données répliquées qui ont été tentées. Ce nombre augmente chaque fois qu'un nœud de stockage tente de réparer un objet à haut risque. Les réparations ILM à haut risque sont prioritaires si le réseau devient occupé.

     La même réparation d'objet peut s'incrémenter à nouveau si la réplication échoue après la réparation.

   Ces attributs peuvent être utiles lorsque vous surveillez la progression de la récupération du 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 grille individuels, sont essentielles à des opérations efficaces.

Surveiller les connexions et les performances du réseau

La connectivité réseau et la bande passante sont particulièrement importantes si votre politique de gestion du cycle de vie des informations (ILM) copie les objets répliqués entre les sites ou stocke les objets codés par effacement à l'aide d'un schéma offrant une protection contre la perte de site. Si le réseau entre les sites n'est pas disponible, la latence du réseau est trop élevée ou la bande passante du réseau est insuffisante, certaines règles ILM peuvent ne pas être en mesure de 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 des retards ILM.

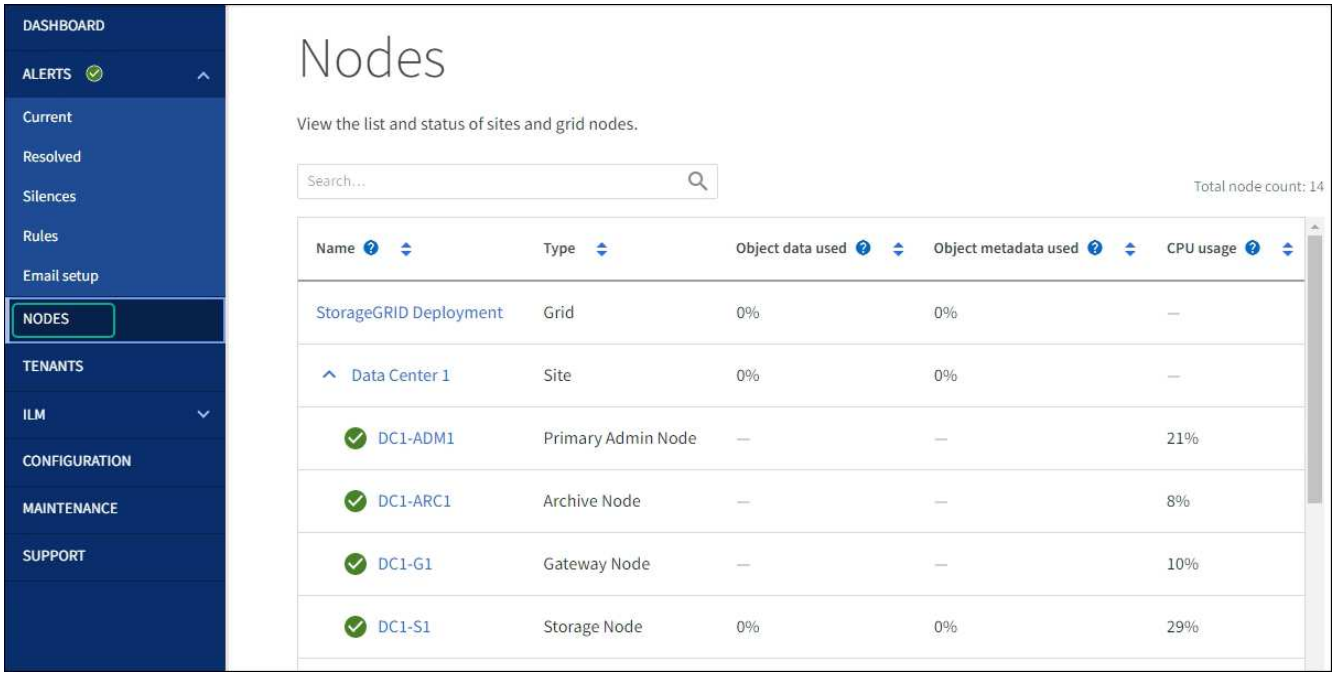
Utilisez Grid Manager pour surveiller la connectivité et les performances du réseau, afin de pouvoir résoudre rapidement tout problème.

En outre, considérez"création de politiques de classification du trafic réseau" afin que vous puissiez surveiller le trafic lié à des locataires, des buckets, des sous-réseaux ou des points de terminaison d'équilibrage de charge spécifiques. Vous pouvez définir des politiques de limitation du trafic selon vos besoins.

Étapes

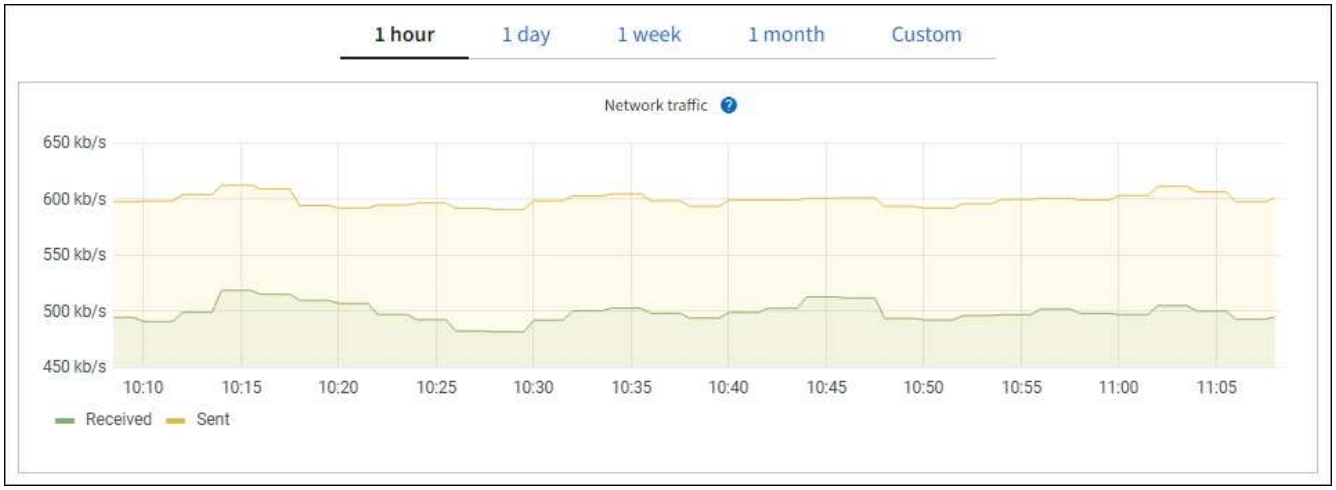
1. Sélectionnez **NODES**.

   La page Nœuds apparaît. Chaque nœud de la grille est répertorié sous forme de tableau.

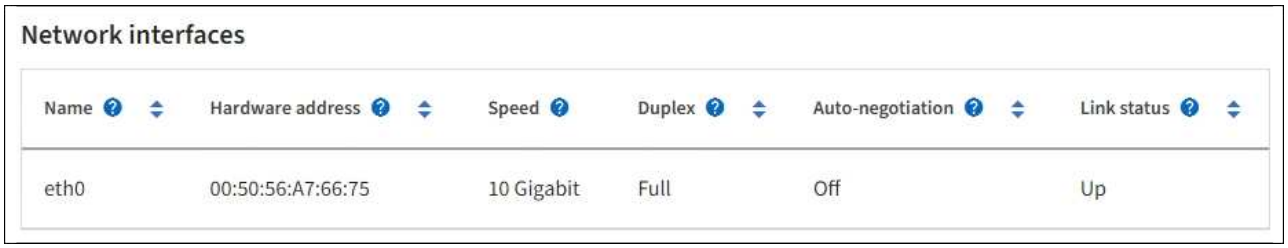


2. Sélectionnez le nom de la grille, un site de centre de données spécifique ou un nœud de grille, puis sélectionnez l'onglet **Réseau**.

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

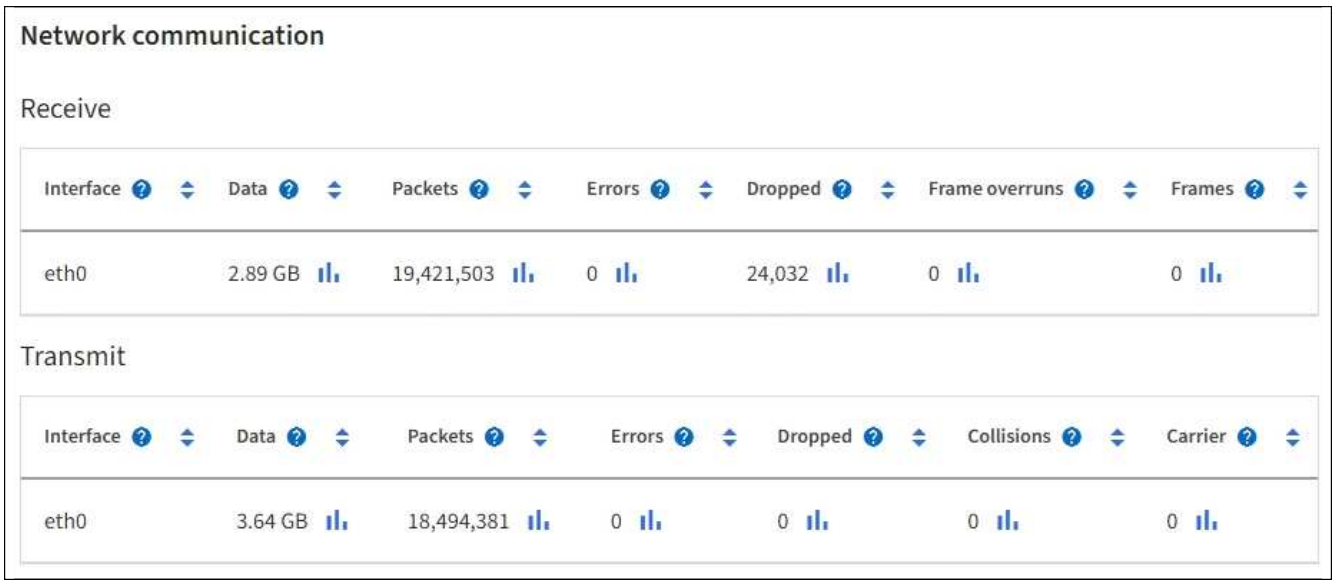


   a. Si vous avez sélectionné un nœud de grille, faites défiler vers le bas pour consulter la section **Interfaces réseau** de la page.



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

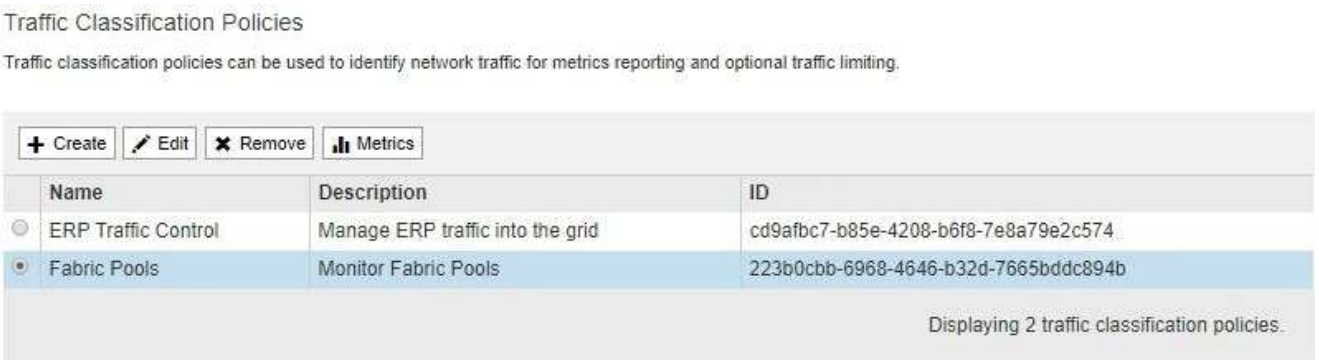
Les tableaux de réception et de transmission indiquent le nombre d'octets et de paquets reçus et envoyés sur chaque réseau, ainsi que d'autres mesures de réception et de transmission.



3. Utilisez les mesures associées à vos stratégies de classification du trafic pour surveiller le trafic réseau.

a. Sélectionnez **CONFIGURATION** > **Réseau** > **Classification du trafic**.

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



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

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

Si une politique de classification du trafic est conçue pour limiter le trafic réseau, analysez la fréquence

à laquelle le trafic est limité et décidez si la politique continue de répondre à vos besoins. De temps en temps,"ajuster chaque politique de classification du trafic selon les besoins" .

Informations connexes

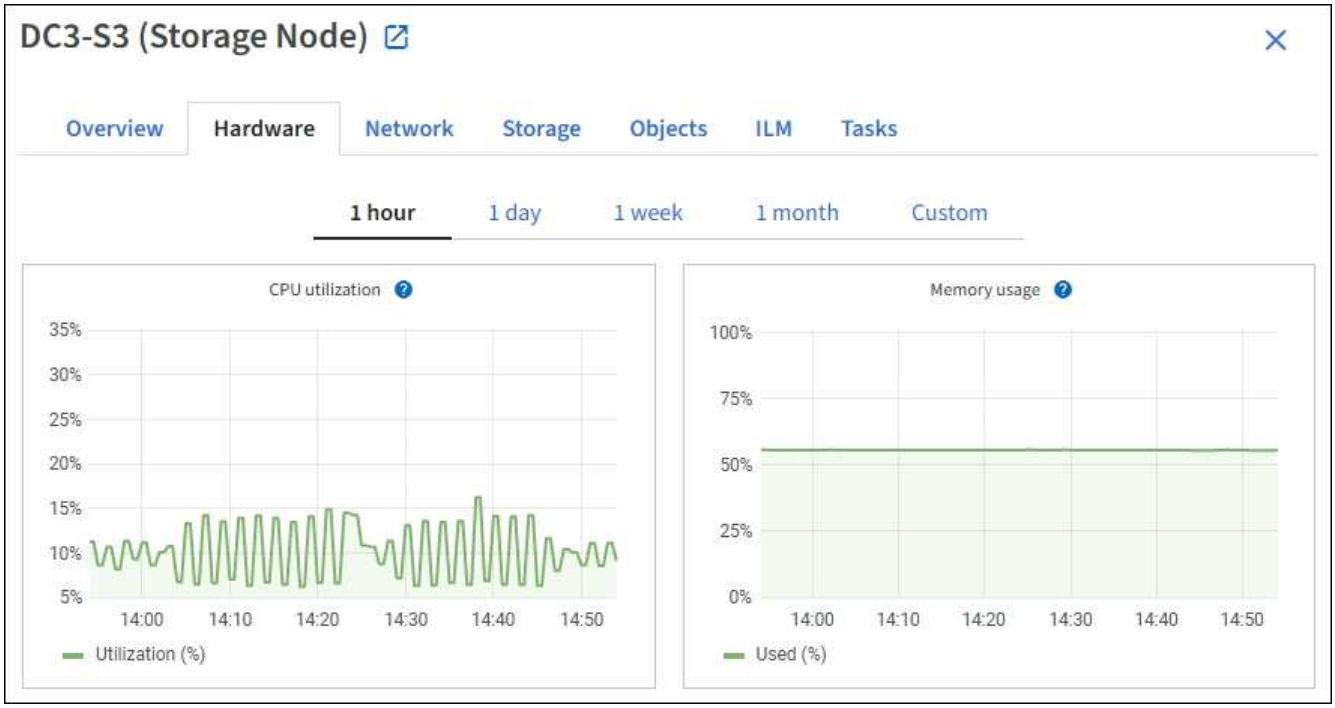
- "Afficher l'onglet Réseau"
- "Surveiller les états de connexion des nœuds"

Surveiller les ressources au niveau des nœuds

Surveillez les nœuds de grille individuels pour vérifier leurs niveaux d'utilisation des ressources. Si les nœuds sont constamment surchargés, davantage de nœuds peuvent être nécessaires pour des opérations efficaces.

Étapes

1. Depuis la page **NODES**, sélectionnez le nœud.
2. Sélectionnez l'onglet **Matériel** pour afficher les graphiques d'utilisation du processeur et de l'utilisation de la mémoire.



3. Pour afficher un intervalle de temps différent, sélectionnez l'un des contrôles au-dessus du graphique ou du diagramme. Vous pouvez afficher les informations disponibles pour des 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 dates et d'heures.
4. Si le nœud est hébergé sur un dispositif de stockage ou un dispositif de services, faites défiler vers le bas pour afficher les tableaux des composants. Le statut de tous les composants doit être « Nominal ». Examinez les composants qui ont un autre statut.

Informations connexes

- "Afficher les informations sur les nœuds de stockage de l'appliance"
- "Afficher les informations sur les nœuds d'administration et les nœuds de passerelle de l'appareil"

Surveiller l'activité des locataires

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

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"Accès root ou autorisation des comptes locataires" .

Voir tous les locataires

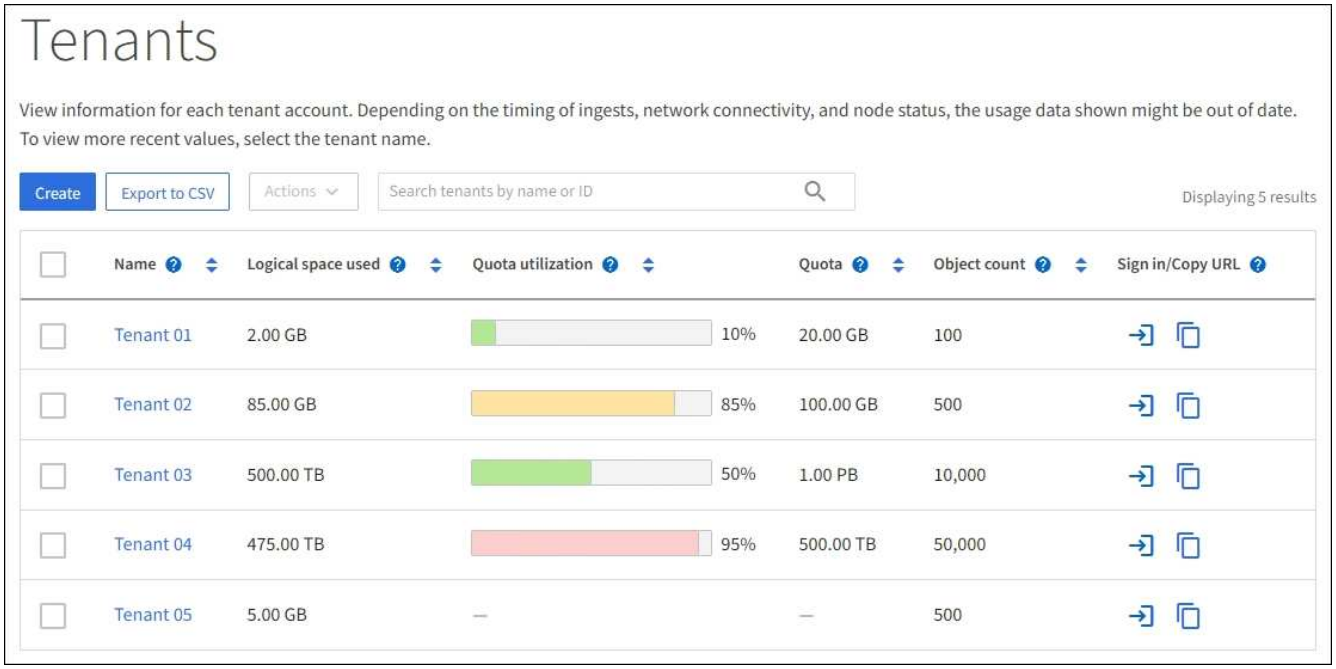
La page Locataires affiche les informations de base pour tous les comptes locataires actuels.

Étapes

1. Sélectionnez **LOCATAIRES**.
2. Consultez les informations affichées sur les pages Locataire.

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

   > Les valeurs d'espace utilisées sont des estimations. Ces estimations sont affectées par le moment des ingestions, la connectivité réseau et l'état du nœud.



3. Vous pouvez également vous connecter à un compte locataire en sélectionnant le lien de connexion. dans la colonne * Sign in/ Copier l'URL*.
4. Vous pouvez également copier l'URL de la page de connexion d'un locataire en sélectionnant le lien Copier l'URL. dans la colonne * Sign in/ Copier l'URL*.

5. En option, sélectionnez **Exporter vers CSV** pour afficher et exporter un `.csv` fichier contenant les valeurs d'utilisation pour tous les locataires.

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

   Le contenu de la `.csv` le 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 le `.csv` fichier dans une application de feuille de calcul ou utilisez-le dans l'automatisation.

6. Si aucun objet n'est répertorié, vous pouvez également sélectionner **Actions** > **Supprimer** pour supprimer un ou plusieurs locataires. Voir "Supprimer le compte locataire" .

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

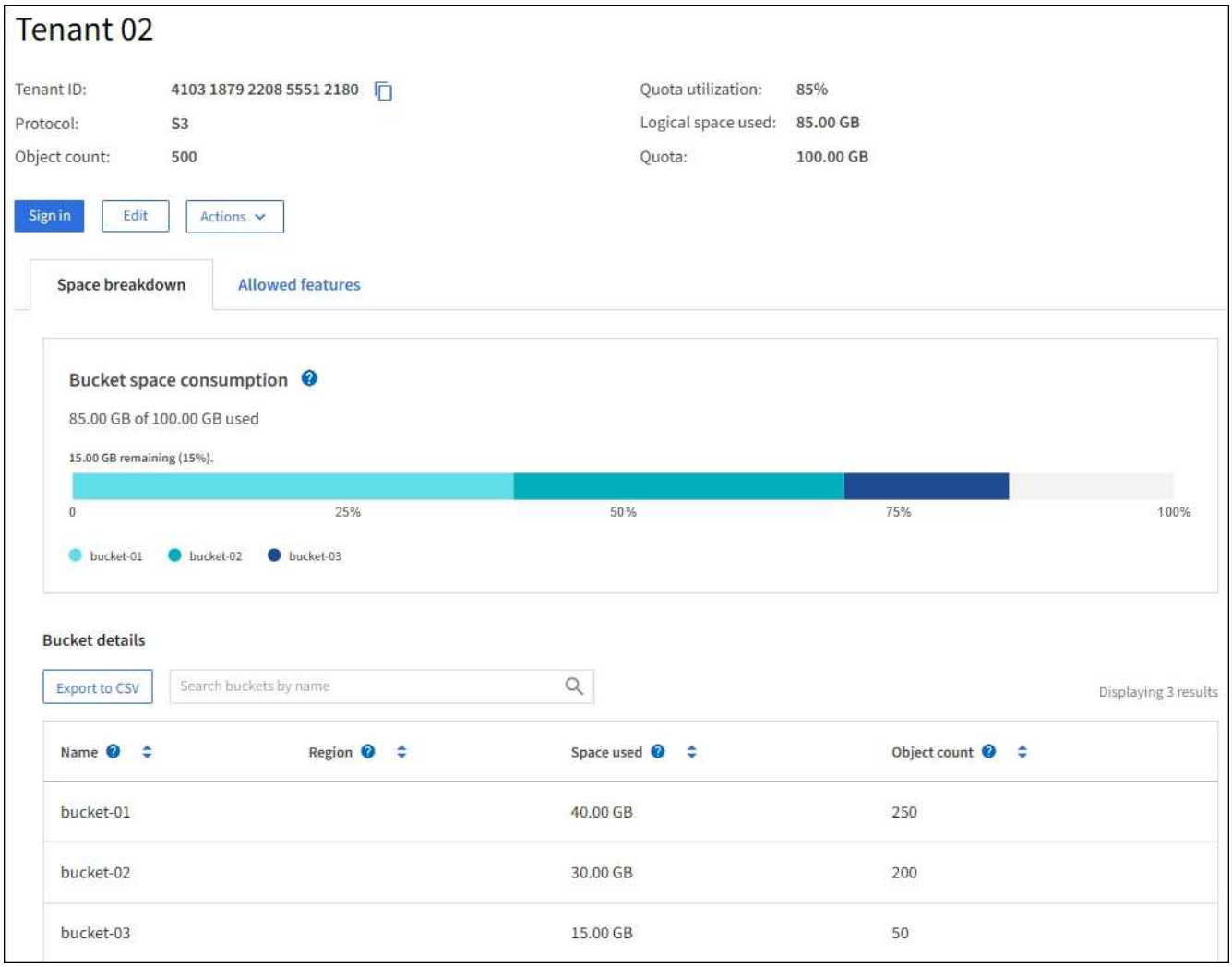
Afficher un locataire spécifique

Vous pouvez afficher les détails d'un locataire spécifique.

Étapes

1. Sélectionnez le nom du locataire sur la page Locataires.

   La page des détails du locataire apparaît.



2. Consultez l'aperçu du locataire en haut de la page.

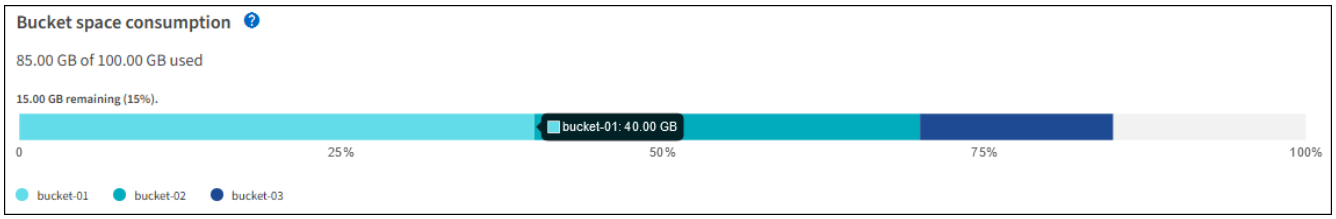
   Cette section de la page de détails fournit des informations récapitulatives sur le locataire, notamment le nombre d'objets du locataire, l'utilisation du quota, l'espace logique utilisé et le paramètre de quota.

3. Dans l'onglet **Répartition de l'espace**, consultez le graphique **Consommation d'espace**.

   Ce graphique montre la consommation totale d'espace pour tous les compartiments S3 du locataire.

   Si un quota a été défini pour ce locataire, la quantité de quota utilisée et restante est affichée sous forme de texte (par exemple, `85.00 GB of 100 GB used`). Si aucun quota n'a été défini, le locataire dispose d'un quota illimité et le texte n'inclut qu'une quantité d'espace utilisée (par exemple, `85.00 GB used`). Le graphique à barres montre le pourcentage de quota dans chaque bucket ou conteneur. Si le locataire a dépassé le quota de stockage de plus de 1 % et d'au moins 1 Go, le graphique affiche le quota total et le montant excédentaire.

   Vous pouvez placer votre curseur sur le graphique à barres pour voir le stockage utilisé par chaque bucket ou conteneur. Vous pouvez placer votre curseur sur le segment d'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 télécharger des objets et rejette les nouvelles acquisitions si le locataire a dépassé le quota. Cependant, StorageGRID ne prend pas en compte la taille du téléchargement actuel pour déterminer si le quota a été dépassé. Si des objets sont supprimés, un locataire peut être temporairement empêché de télécharger de nouveaux objets jusqu'à ce que l'utilisation du quota soit recalculée. Les calculs d'utilisation des quotas peuvent prendre 10 minutes ou plus.

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

Vous pouvez activer la règle d'alerte **Utilisation élevée du quota du locataire** pour déterminer si les locataires consomment leurs quotas. Si cette option est activée, cette alerte est déclenchée lorsqu'un locataire a utilisé 90 % de son quota. Pour les instructions, voir"Modifier les règles d'alerte" .

4. Dans l'onglet **Répartition de l'espace**, examinez les **Détails du bucket**.

   Ce tableau répertorie les compartiments S3 pour le locataire. L'espace utilisé correspond à la quantité totale de données d'objet dans le bucket 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 vers CSV** pour afficher et exporter un fichier .csv contenant les valeurs d'utilisation de chaque bucket ou conteneur.

   Le contenu d'un locataire S3 individuel `.csv` le fichier ressemble à l'exemple suivant :

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 le `.csv` fichier dans une application de feuille de calcul ou utilisez-le dans l'automatisation.

6. Vous pouvez également sélectionner l'onglet **Fonctionnalités autorisées** pour afficher la liste des autorisations et des fonctionnalités activées pour le locataire. Voir"Modifier le compte locataire" si vous devez modifier l'un de ces paramètres.
7. Si le locataire dispose de l'autorisation **Utiliser la connexion à la 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 réseau ?" et"Gérer les locataires autorisés pour la fédération de

réseau" .

Afficher le trafic réseau

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

Étapes

1. Sélectionnez **CONFIGURATION** > **Réseau** > **Classification du trafic**.

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

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

Voir "Gérer les politiques de classification du trafic" pour plus d'informations.

Utiliser le journal d'audit

En option, vous pouvez utiliser le journal d'audit pour une surveillance plus précise des activités d'un locataire.

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

- Opérations client spécifiques, telles que PUT, GET ou DELETE
- Tailles des objets
- La règle ILM appliquée aux objets
- L'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 de journaux de votre choix. Cela vous permet de mieux comprendre les activités des clients ou de mettre en œuvre des modèles de rétrofacturation et de facturation sophistiqués.

Voir "Examiner les journaux d'audit" pour plus d'informations.

Utiliser les métriques Prometheus

Vous pouvez également utiliser les métriques Prometheus pour générer des rapports sur l'activité des locataires.

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

  > Les outils disponibles sur la page Métriques sont principalement destinés à être utilisés par le support technique. Certaines fonctionnalités et éléments de menu de ces outils sont intentionnellement non fonctionnels.

- En haut du gestionnaire de grille, sélectionnez l'icône d'aide et sélectionnez **Documentation API**. Vous pouvez utiliser les métriques de la section Métriques de l'API Grid Management pour créer des règles

d’alerte et des tableaux de bord personnalisés pour l’activité des locataires.

Voir "Examiner les mesures de support" pour plus d’informations.

Surveiller les opérations du client S3

Vous pouvez surveiller les taux d’ingestion et de récupération d’objets ainsi que les mesures relatives au nombre d’objets, aux requêtes et à la vérification. Vous pouvez afficher le nombre de tentatives réussies et infructueuses des applications clientes pour lire, écrire et modifier des objets dans le système StorageGRID .

Avant de commencer

- Vous êtes connecté au Grid Manager à l’aide d’un"navigateur Web pris en charge" .

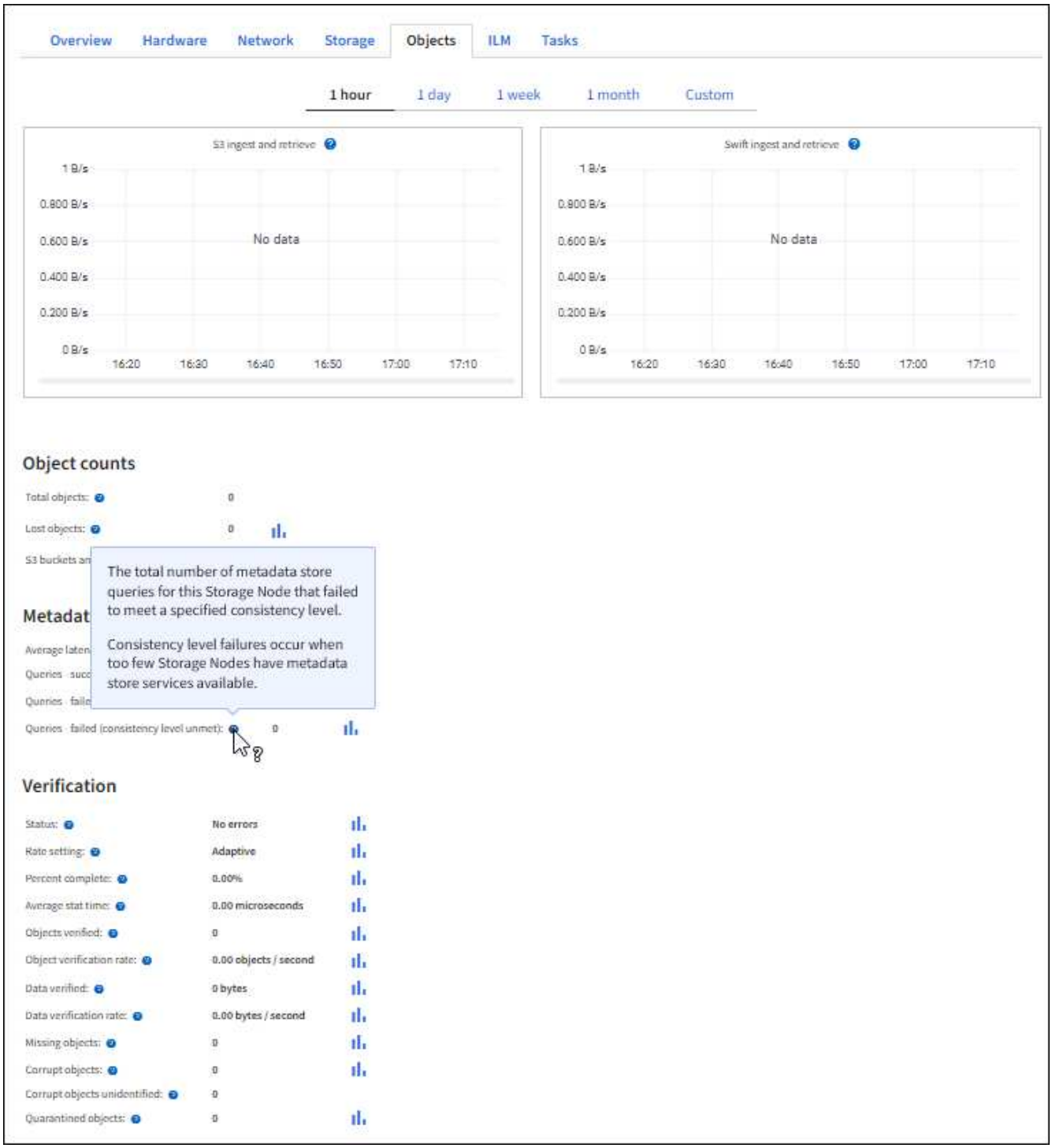
Étapes

1. Depuis le tableau de bord, sélectionnez l’onglet **Performance**.
2. Consultez les graphiques S3, qui résument le nombre d’opérations client effectuées par les nœuds de stockage et le nombre de requêtes API reçues par les nœuds de stockage pendant la période sélectionnée.
3. Sélectionnez **NODES** pour accéder à la page Nœuds.
4. Depuis la page d’accueil des nœuds (niveau de la grille), sélectionnez l’onglet **Objets**.

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

5. Pour afficher les informations d’un nœud de stockage particulier, sélectionnez le nœud dans la liste de gauche, puis sélectionnez l’onglet **Objets**.

   Le graphique montre 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 apporté des modifications de configuration ou effectué une extension.

À propos de cette 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 répartir les demandes des clients sur plusieurs nœuds de stockage.

Après avoir configuré l'équilibrage de charge, vous devez confirmer que les opérations d'ingestion et de récupération d'objets sont réparties uniformément sur les nœuds de stockage. Des demandes réparties uniformément garantissent que StorageGRID reste réactif aux demandes des clients sous charge et peut aider à maintenir les performances des clients.

Si vous avez configuré un groupe haute disponibilité (HA) de nœuds de passerelle ou de nœuds d'administration en mode de sauvegarde active, un seul nœud du groupe distribue activement les demandes des clients.

Pour plus d'informations, consultez la section "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 prévu :
   a. Sélectionnez **NODES**.
   b. Sélectionnez un nœud de passerelle ou un nœud d'administration.
   c. Dans l'onglet **Vue d'ensemble**, vérifiez si une interface de nœud se trouve dans un groupe HA et si l'interface de nœud a le rôle de Principal.

      Les nœuds avec le rôle principal et les nœuds qui ne font pas partie d'un groupe HA doivent distribuer activement les demandes aux clients.

   d. Pour chaque nœud qui doit distribuer activement les demandes des clients, sélectionnez l'option"Onglet Équilibreur de charge" .
   e. Consultez le graphique du trafic des demandes d'équilibrage de charge de la semaine dernière pour vous assurer que le nœud a distribué activement les demandes.

      Les nœuds d'un groupe HA de sauvegarde active peuvent assumer le rôle de sauvegarde de temps à autre. Pendant ce temps, les nœuds ne distribuent pas les requêtes des clients.

   f. Consultez le graphique du taux de demandes entrantes de l'équilibreur de charge de la semaine dernière pour évaluer le débit d'objet du nœud.
   g. Répétez ces étapes pour chaque nœud d'administration ou nœud de passerelle dans le système StorageGRID .
   h. Vous pouvez également utiliser des stratégies de classification du trafic pour afficher une analyse plus détaillée du trafic traité par le service Load Balancer.
2. Vérifiez que ces demandes sont réparties uniformément entre les nœuds de stockage.
   a. Sélectionnez ***Nœud de stockage*** > **LDR** > **HTTP**.
   b. Consultez le nombre de **sessions entrantes actuellement établies**.
   c. Répétez l'opération pour chaque nœud de stockage dans la grille.

      Le nombre de sessions doit être à peu près égal sur tous les nœuds de stockage.

Surveiller les connexions de la fédération de réseau

Vous pouvez surveiller les informations de base sur tous"connexions de fédération de réseau" , des informations détaillées sur une connexion spécifique ou des mesures Prometheus sur les opérations de réplication inter-grille. 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 ou l'autre grille à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"Autorisation d'accès root" pour la grille à laquelle vous êtes connecté.

Voir toutes les connexions

La page Fédération de grille 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

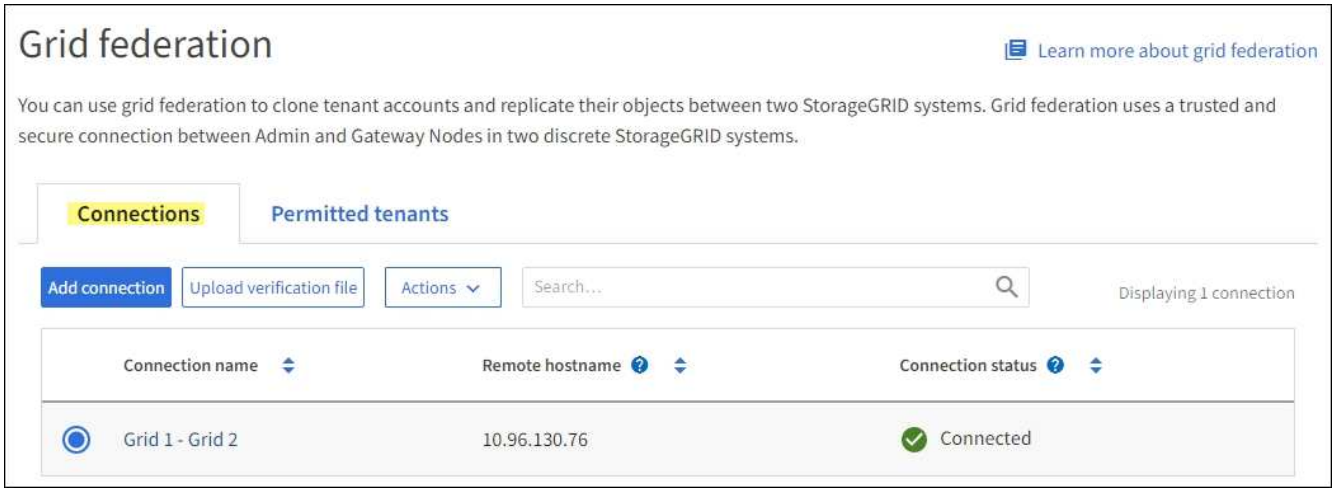
1. Sélectionnez **CONFIGURATION** > **Système** > **Fédération de grille**.

   La page de la fédération Grid apparaît.

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

   Depuis cet onglet, vous pouvez :

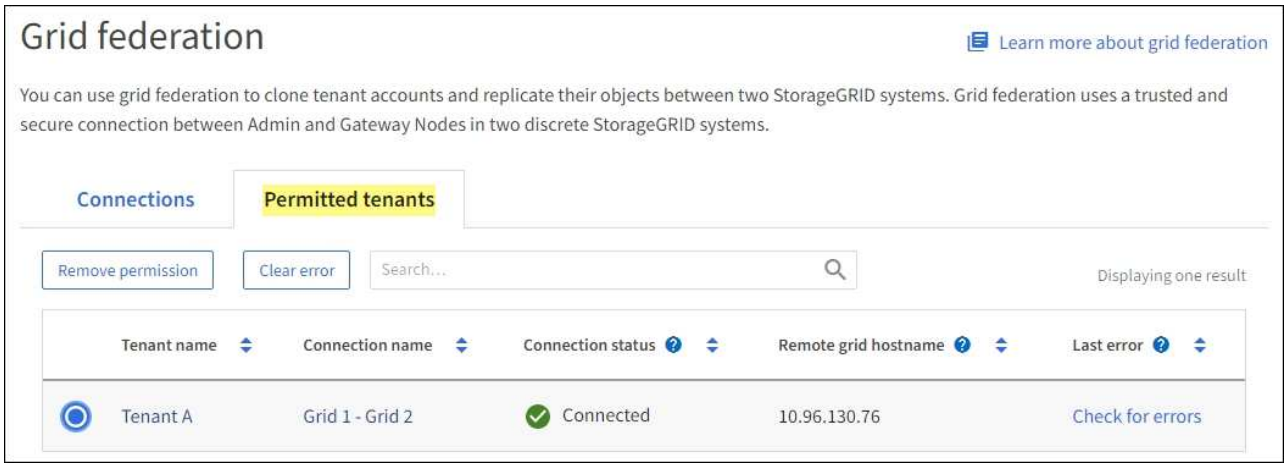
   - "Créer une nouvelle connexion" .
   - Sélectionnez une connexion existante pour"modifier ou tester" .



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

   Depuis cet onglet, vous pouvez :

   - "Consultez la page de détails pour chaque locataire autorisé" .
   - Consultez la page de détails pour chaque connexion. Voir Afficher une connexion spécifique .
   - Sélectionnez un locataire autorisé et"supprimer l'autorisation" .
   - Vérifiez les erreurs de réplication inter-grille et effacez la dernière erreur, le cas échéant. Voir "Résoudre les erreurs de fédération de grille" .



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.

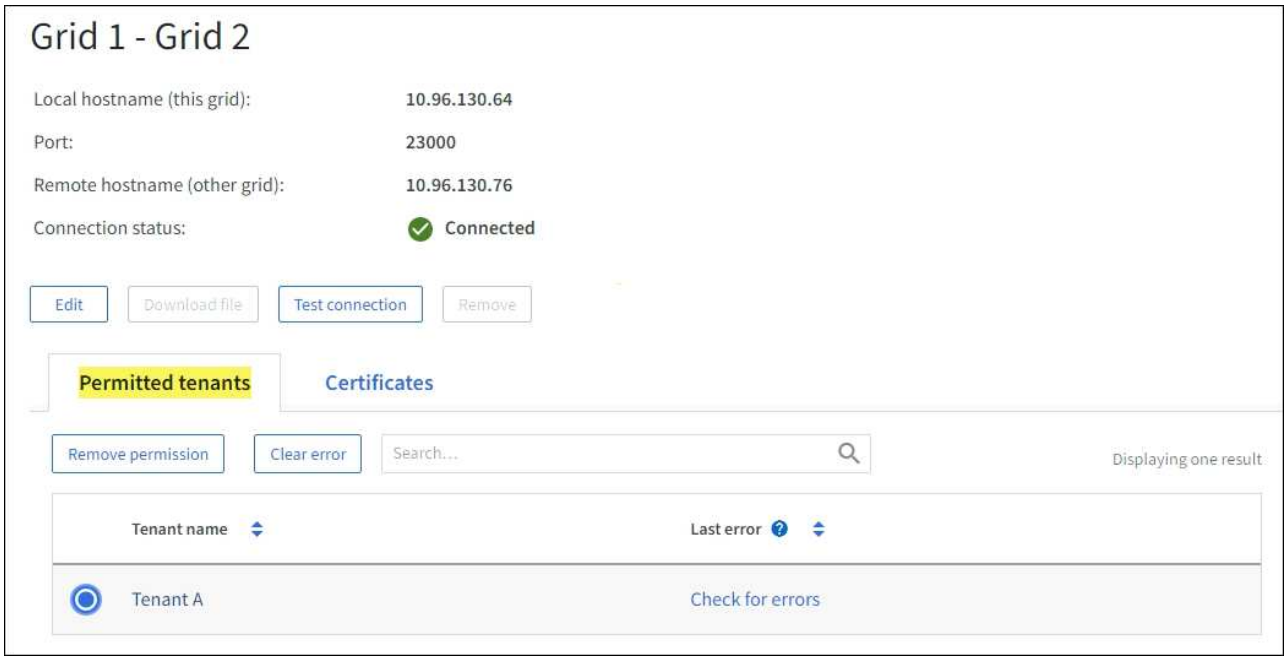
   Depuis la page de détails de la connexion, vous pouvez :

   - 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. Lorsque vous visualisez une connexion spécifique, sélectionnez l'onglet * Locataires autorisés * pour afficher les détails sur les locataires autorisés pour la connexion.

   Depuis cet onglet, vous pouvez :

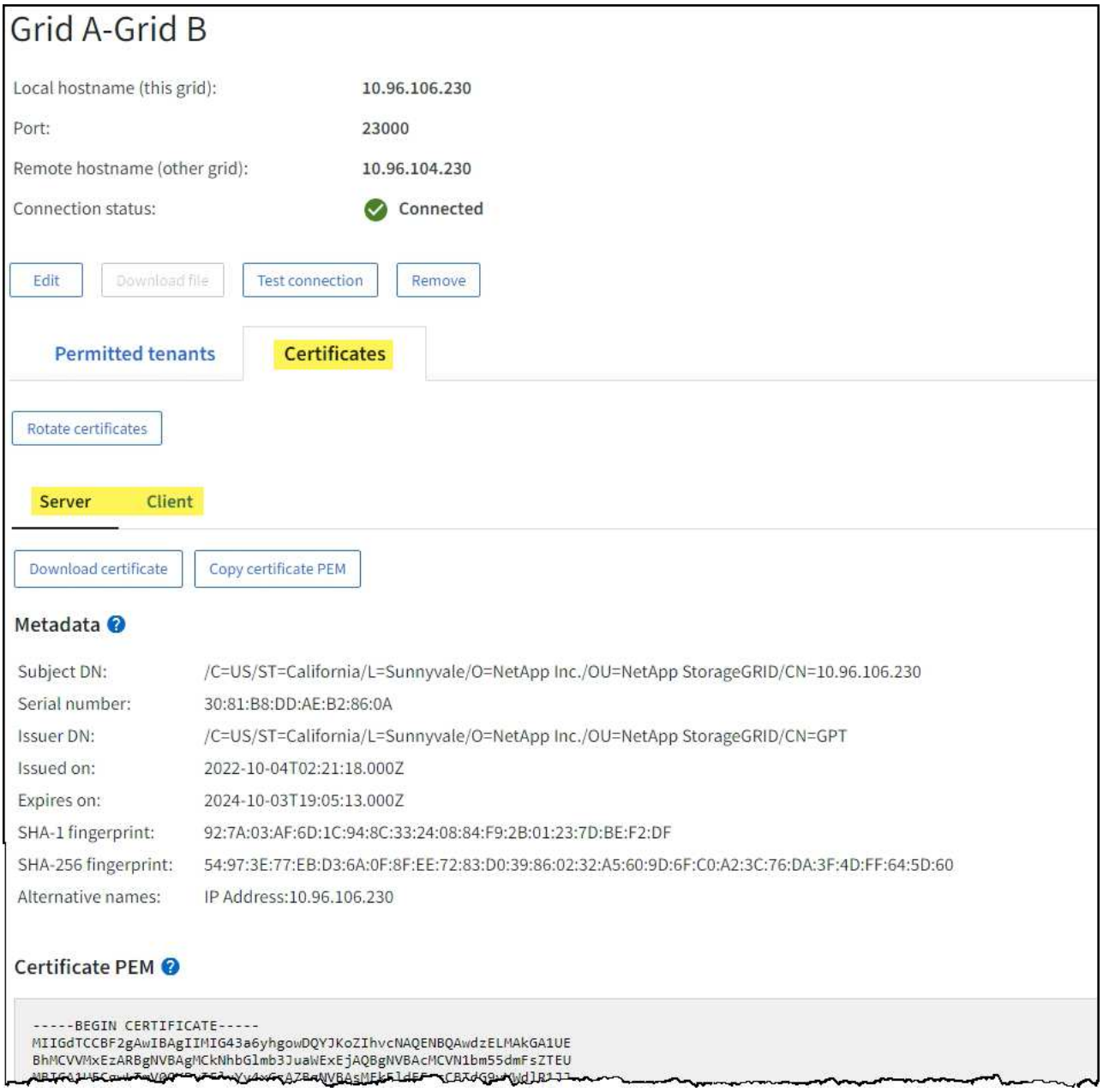
   - "Consultez la page de détails pour chaque locataire autorisé" .
   - "Supprimer l'autorisation d'un locataire"pour utiliser la connexion.
   - Vérifiez les erreurs de réplication inter-grille et effacez la dernière erreur. Voir "Résoudre les erreurs de fédération de grille" .



3. Lorsque vous affichez une connexion spécifique, sélectionnez l'onglet **Certificats** pour afficher les certificats serveur et client générés par le système pour cette connexion.

   Depuis cet onglet, vous pouvez :

   - "Faire tourner les certificats de connexion" .
   - Sélectionnez **Serveur** ou **Client** pour afficher ou télécharger le certificat associé ou copier le certificat PEM.



Examiner les mesures de réplication inter-grille

Vous pouvez utiliser le tableau de bord de réplication inter-grille dans Grafana pour afficher les métriques Prometheus sur les opérations de réplication inter-grille sur votre grille.

Étapes

1. Depuis le gestionnaire de grille, sélectionnez **SUPPORT** > **Outils** > **Métriques**.

   Les outils disponibles sur la page Métriques sont destinés à être utilisés par le support technique. Certaines fonctionnalités et éléments de menu de ces outils sont intentionnellement non fonctionnels et sont susceptibles d'être modifiés. Voir la liste des"métriques Prometheus couramment utilisées" .

2. Dans la section Grafana de la page, sélectionnez **Réplication inter-grille**.

   Pour des instructions détaillées, voir"Examiner les mesures de support" .

3. Pour réessayer la réplication des objets dont la réplication a échoué, voir"Identifier et réessayer les opérations de réplication ayant échoué" .

Gérer les alertes

Gérer les alertes

Le système d'alerte fournit une interface facile à utiliser pour détecter, évaluer et résoudre les problèmes pouvant survenir pendant le fonctionnement de StorageGRID .

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

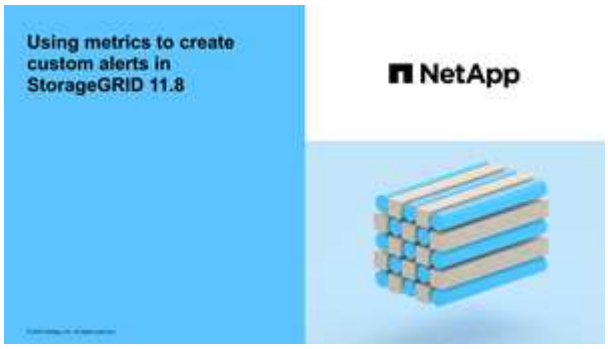
- Une icône de gravité d'alerte s'affiche sur le tableau de bord dans le gestionnaire de grille et le nombre d'alertes actuelles est incrémenté.
- L'alerte s'affiche sur la page de résumé **NODES** et sur l'onglet **NODES** > ***node*** > **Aperçu**.
- Une notification par e-mail est envoyée, en supposant que vous ayez 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 ayez 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 :

- Revoir la vidéo : "Vidéo : Aperçu des alertes"

- Revoir la vidéo : "Vidéo : Alertes personnalisées"



- Voir le"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 telles quelles ou 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 déclencheront chaque alerte et pour voir si des alertes sont désactivées.

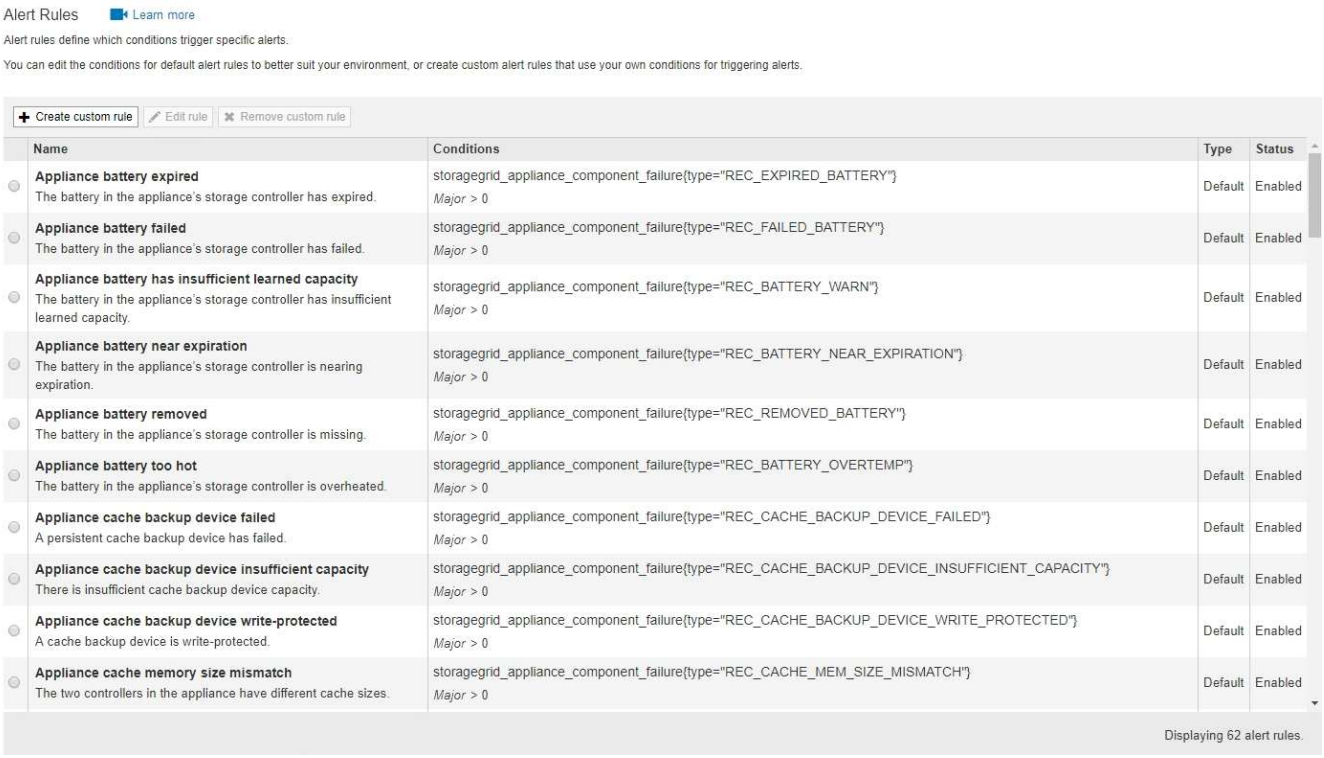
Avant de commencer

- Vous êtes connecté au Grid Manager à l’aide d’un"navigateur Web pris en charge" .
- Vous avez le"Gérer les alertes ou l’autorisation d’accès root" .
- En option, vous avez regardé la vidéo : "Vidéo : Aperçu des alertes"

Étapes

1. Sélectionnez **ALERTES** > **Règles**.

   La page Règles d’alerte s’affiche.



2. Consultez les informations dans le tableau des règles d'alerte :

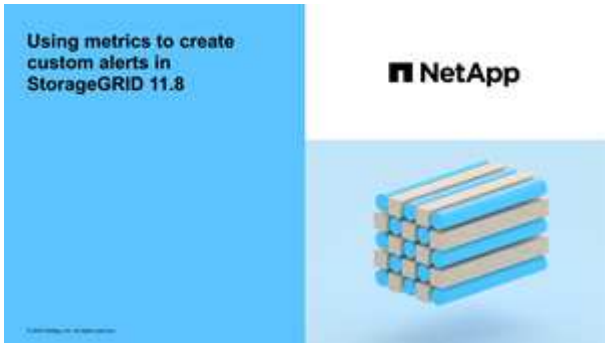
En-tête de colonne	Description
Nom	Le nom unique et la description de la règle d'alerte. Les règles d'alerte personnalisées sont répertoriées en premier, suivies des règles d'alerte par défaut. Le nom de la règle d'alerte est l'objet des notifications par e-mail.
Conditions	Les expressions Prometheus qui déterminent quand cette alerte est déclenchée. Une alerte peut être déclenchée à un ou plusieurs des niveaux de gravité suivants, mais une condition pour chaque gravité n'est pas requise. • *Critique* :Une condition anormale existe qui a arrêté les opérations normales d'un nœud ou d'un service StorageGRID . Vous devez résoudre le problème sous-jacent immédiatement. Une interruption de service et une perte de données peuvent survenir si le problème n'est pas résolu. • *Majeur* :Une condition anormale existe qui affecte les opérations en cours ou approche le seuil d'une alerte critique. Vous devez enquêter sur les alertes majeures et résoudre tous les problèmes sous-jacents pour garantir que la condition anormale n'arrête pas le fonctionnement normal d'un nœud ou d'un service StorageGRID . • *Mineure* :Le système fonctionne normalement, mais une condition anormale existe qui pourrait affecter la capacité du système à fonctionner si elle persiste. Vous devez surveiller et résoudre les alertes mineures qui ne disparaissent pas d'elles-mêmes pour vous assurer qu'elles n'entraînent pas un problème plus grave.
Type	Le type de règle d'alerte : • **Par défaut** : une 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. • **Par défaut*** : une règle d'alerte par défaut qui inclut une condition ou une durée modifiée. Si nécessaire, vous pouvez facilement rétablir une condition modifiée à la valeur par défaut d'origine. • **Personnalisé** : une règle d'alerte que vous avez créée. Vous pouvez désactiver, modifier et supprimer des règles d'alerte personnalisées.
Statut	Si cette règle d'alerte est actuellement activée ou désactivée. Les conditions des règles d'alerte désactivées ne sont pas évaluées, donc aucune alerte n'est déclenchée.

Créer des règles d'alerte personnalisées

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

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"Gérer les alertes ou l'autorisation d'accès root" .
- Vous connaissez le"métriques Prometheus couramment utilisées" .
- Vous comprenez le "syntaxe des requêtes Prometheus" .
- En option, vous avez regardé la vidéo : "Vidéo : Alertes personnalisées" .



À propos de cette tâche

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

- 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. Ensuite, modifiez la valeur seuil pour chaque condition.
- Vérifiez soigneusement chaque condition pour détecter les fautes de frappe et les erreurs de logique.
- Utilisez uniquement les métriques répertoriées dans l'API Grid Management.
- Lorsque vous testez une expression à l'aide de l'API Grid Management, sachez qu'une réponse « réussie » peut être un corps de réponse vide (aucune alerte déclenchée). Pour voir si l'alerte est réellement déclenchée, vous pouvez définir temporairement un seuil sur une valeur que vous pensez être vraie actuellement.

  Par exemple, pour tester l'expression `node_memory_MemTotal_bytes < 24000000000` , exécuter d'abord `node_memory_MemTotal_bytes >= 0` et assurez-vous d'obtenir les résultats attendus (tous les nœuds renvoient une valeur). Ensuite, modifiez l'opérateur et le seuil aux valeurs prévues et exécutez à nouveau. Aucun résultat n'indique qu'il n'y a aucune alerte actuelle pour cette expression.

- Ne présumez pas qu'une alerte personnalisée fonctionne à moins d'avoir validé que l'alerte est déclenchée au moment prévu.

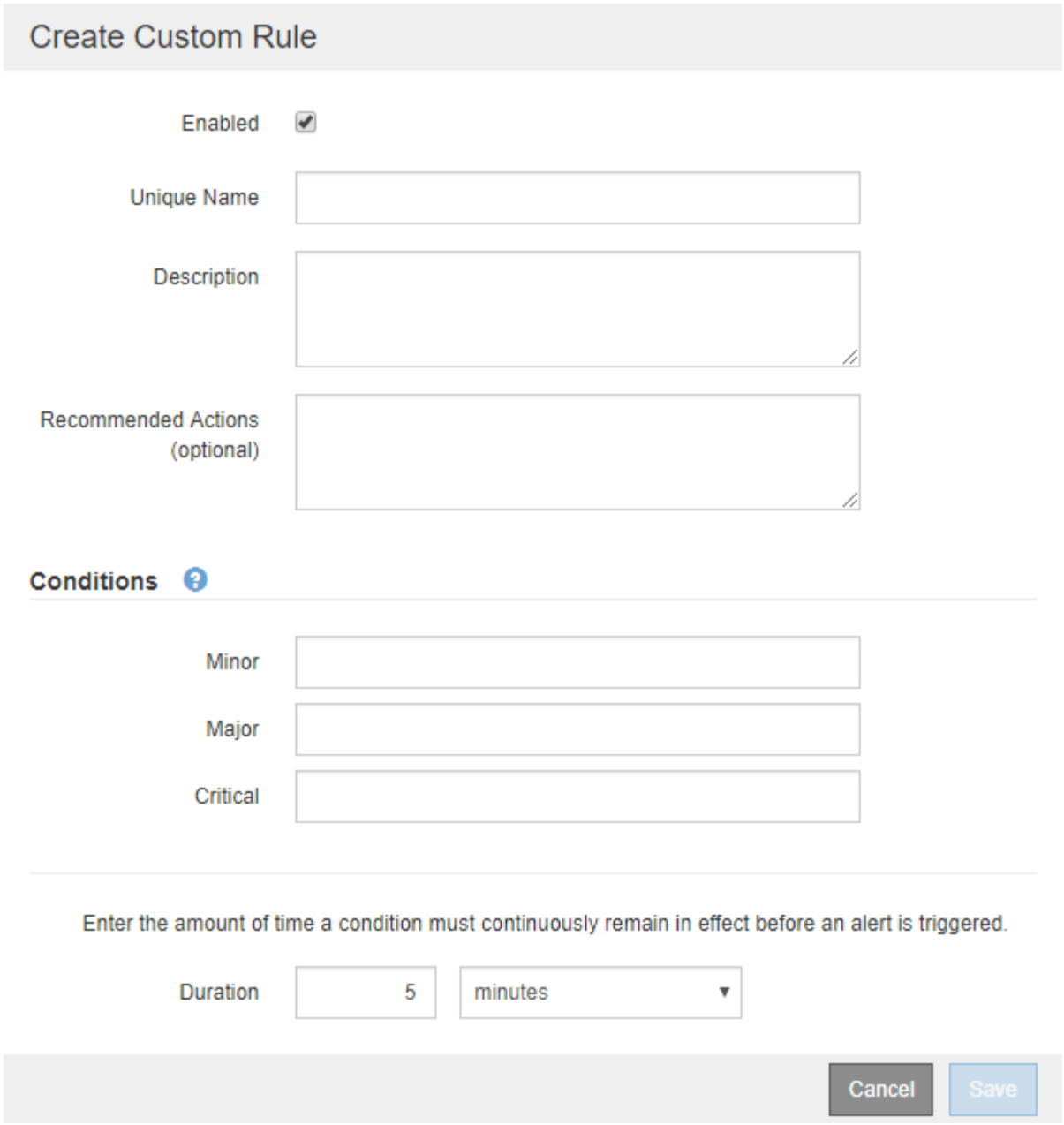
Étapes

1. Sélectionnez **ALERTES** > **Règles**.

   La page Règles d'alerte s'affiche.

2. Sélectionnez **Créer une règle personnalisée**.

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



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 est affiché sur la page Alertes et constitue également l'objet des notifications par e-mail. Les noms des règles d'alerte peuvent comporter entre 1 et 64 caractères.

Champ	Description
Description	Une description du problème qui se produit. 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	Facultativement, les actions recommandées à entreprendre lorsque cette alerte est déclenchée. Saisissez les actions recommandées sous forme de texte brut (sans codes de formatage). Les actions recommandées pour les règles d'alerte peuvent être comprises entre 0 et 1 024 caractères.

5. Dans la section Conditions, saisissez 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 avoir n'importe quelle longueur, mais apparaissent sur une seule ligne dans l'interface utilisateur. Au moins une expression est requise.

   Cette expression provoque le déclenchement d'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 voir les métriques disponibles et tester les expressions Prometheus, sélectionnez l'icône d'aide et suivez le lien vers la section Métriques de l'API de gestion de grille.

6. Dans le champ **Durée**, saisissez la durée pendant laquelle une condition doit rester en vigueur en continu avant que l'alerte ne soit déclenchée, puis sélectionnez une unité de temps.

   Pour déclencher une alerte immédiatement lorsqu'une condition devient vraie, entrez **0**. Augmentez cette valeur pour empêcher des conditions temporaires de déclencher des alertes.

   La valeur par défaut est de 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.

Modifier les règles d'alerte

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

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .

- Vous avez le"Gérer les alertes ou l'autorisation d'accès root" .

À propos de cette tâche

Lorsque vous modifiez une règle d'alerte par défaut, vous pouvez modifier les conditions des 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, vous risquez de ne pas détecter un problème sous-jacent jusqu'à ce qu'il empêche une opération critique de se terminer.

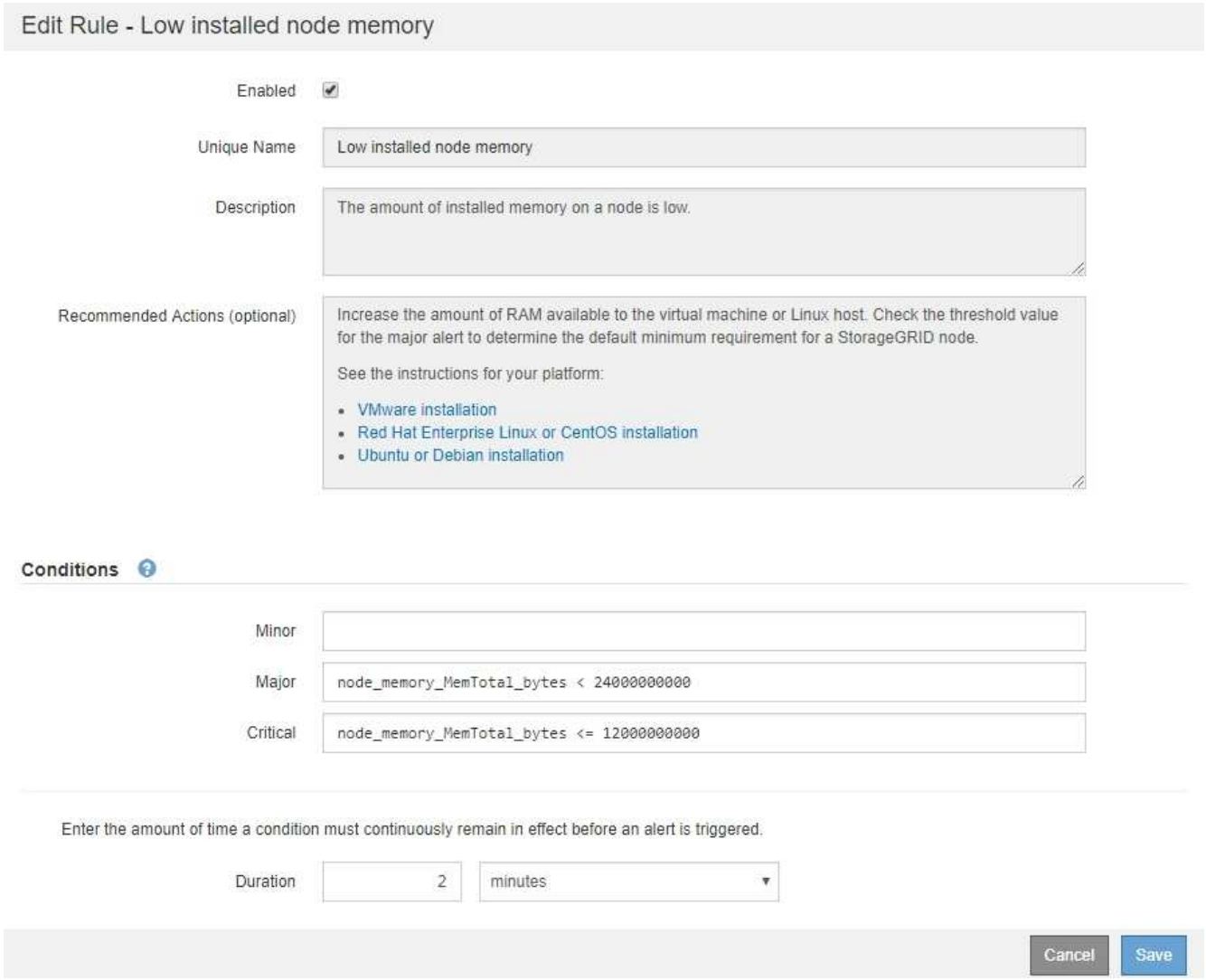
Étapes

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.



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 pour que l'alerte n'apparaisse plus comme une alerte active.

   > En général, il n'est pas recommandé de désactiver une règle d'alerte par défaut. Si une règle d'alerte est désactivée, vous risquez de ne pas détecter un problème sous-jacent jusqu'à ce qu'il empêche une opération critique de se terminer.

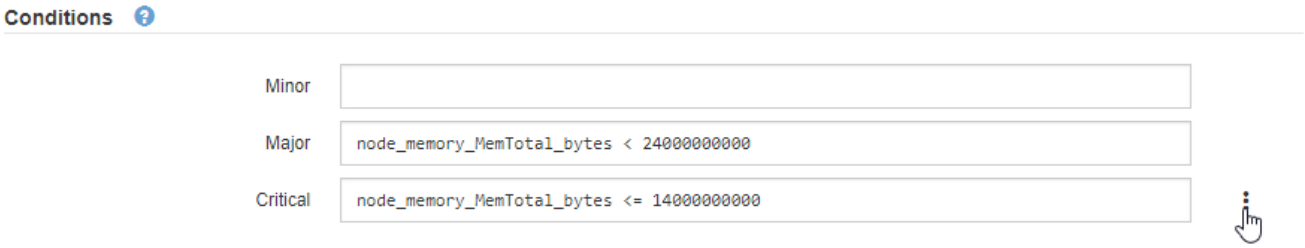
5. Pour les règles d'alerte personnalisées, mettez à jour les informations suivantes selon vos besoins.

   > 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 est affiché sur la page Alertes et constitue également l'objet des notifications par e-mail. Les noms des règles d'alerte peuvent comporter entre 1 et 64 caractères.
Description	Une description du problème qui se produit. 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	Facultativement, les actions recommandées à entreprendre lorsque cette alerte est déclenchée. Saisissez les actions recommandées sous forme de texte brut (sans codes de formatage). Les actions recommandées pour les règles d'alerte peuvent être comprises entre 0 et 1 024 caractères.

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

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



> Si vous mettez à jour les conditions d'une alerte actuelle, 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 reflétera les valeurs mises à jour.

Une expression de base est généralement de la forme :

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

Les expressions peuvent avoir n'importe quelle longueur, mais apparaissent sur une seule ligne dans l'interface utilisateur. Au moins une expression est requise.

Cette expression provoque le déclenchement d'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**, saisissez la durée pendant laquelle une condition doit rester en vigueur en continu avant que l'alerte ne soit déclenchée, puis sélectionnez l'unité de temps.

Pour déclencher une alerte immédiatement lorsqu'une condition devient vraie, entrez **0**. Augmentez cette valeur pour empêcher des conditions temporaires de déclencher des alertes.

La valeur par défaut est de 5 minutes.

8. Sélectionnez **Enregistrer**.

   Si vous avez modifié une règle d'alerte par défaut, **Par défaut*** apparaît dans la colonne Type. Si vous avez désactivé une règle d'alerte par défaut ou personnalisée, **Désactivé** apparaît dans la colonne **Statut**.

Désactiver les règles d'alerte

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

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"Gérer les alertes ou l'autorisation d'accès root" .

À propos de cette tâche

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

> En général, il n'est pas recommandé de désactiver une règle d'alerte par défaut. Si une règle d'alerte est désactivée, vous risquez de ne pas détecter un problème sous-jacent jusqu'à ce qu'il empêche une opération critique de se terminer.

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 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 pour que l'alerte ne s'affiche plus comme une alerte active.

5. Sélectionnez **Enregistrer**.

   Désactivé apparaît dans la colonne **Statut**.

Supprimer 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 Grid Manager à l’aide d’un"navigateur Web pris en charge" .
- Vous avez le"Gérer les alertes ou l’autorisation d’accès root" .

Étapes

1. Sélectionnez **ALERTES** > **Règles**.

   La page Règles d’alerte s’affiche.

2. Sélectionnez le bouton radio correspondant à 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 apparaît.

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

   Toutes les instances actives de l’alerte seront résolues dans les 10 minutes.

Gérer les notifications d’alerte

Configurer 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 points de terminaison 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, consultez"Utiliser la surveillance SNMP" .

Après avoir configuré l’agent SNMP StorageGRID , deux types de notifications basées sur des 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 informer le système de gestion qu’un événement s’est produit dans StorageGRID, comme le déclenchement d’une alerte. Les interruptions sont prises 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 délai, il renvoie l’information jusqu’à ce qu’un accusé de réception soit reçu ou que la valeur de nouvelle tentative maximale soit atteinte. Les informations sont prises en charge dans SNMPv2c et SNMPv3.

Les 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 silencieuses" .

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 et les interruptions et informations SNMP. Si le nœud d'administration principal devient indisponible, des notifications sont temporairement envoyées par d'autres nœuds d'administration. Voir "Qu'est-ce qu'un nœud d'administration ?" .

Configurer des 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 les adresses e-mail des destinataires des notifications d'alerte.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"Gérer les alertes ou l'autorisation d'accès root" .

À propos de cette tâche

La configuration de messagerie 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 et les interruptions et informations SNMP. Si le nœud d'administration principal devient indisponible, des notifications sont temporairement envoyées par d'autres nœuds d'administration. Voir "Qu'est-ce qu'un nœud d'administration ?" .

Étapes

1. Sélectionnez **ALERTES** > **Configuration de la messagerie électronique**.

   La page de configuration de la messagerie électronique s'affiche.

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

   Les sections Serveur de messagerie (SMTP), Sécurité de la couche de transport (TLS), Adresses de messagerie et Filtres s'affichent.

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

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

Champ	Entrer
Serveur de messagerie	Le nom de domaine complet (FQDN) ou l'adresse IP du serveur SMTP.

Champ	Entrer
Port	Le 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, saisissez le nom d'utilisateur avec lequel vous souhaitez vous authentifier.
Mot de passe (facultatif)	Si votre serveur SMTP nécessite une authentification, saisissez le mot de passe pour vous authentifier.

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

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

   b. Dans la section Destinataires, saisissez une adresse e-mail pour chaque liste de diffusion ou personne qui doit 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).
   a. Dans le champ **Certificat CA**, indiquez le certificat CA qui sera utilisé pour vérifier l'identité du serveur SMTP.

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

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

   b. Cochez la case **Envoyer un certificat client** si votre serveur de messagerie SMTP exige que les expéditeurs de messagerie fournissent des certificats clients pour l'authentification.
   c. Dans le champ **Certificat client**, indiquez 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.

   d. Dans le champ **Clé privée**, saisissez la clé privée du certificat client dans un encodage 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 électronique, sélectionnez l'icône en forme de crayon pour mettre à jour ce champ.

6. Dans la section Filtres, sélectionnez les niveaux de gravité des alertes qui doivent entraîner des

notifications par e-mail, sauf si la règle d'une alerte spécifique a été désactivée.

Gravité	Description
Mineur, majeur, critique	Une notification par courrier électronique est envoyée lorsque la condition mineure, majeure ou critique d'une règle d'alerte est remplie.
Majeur, critique	Une notification par e-mail est envoyée lorsque la condition majeure 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 un e-mail de test**.

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

   b. Vérifiez les boîtes de réception de tous les destinataires de courrier électronique et confirmez qu'un courrier électronique de test a été reçu.

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

   c. Sign in à n'importe quel 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'alerte, vous devez vous connecter à chaque nœud d'administration pour vérifier la connectivité. Ceci est en contraste avec les tests des packages AutoSupport , où tous les nœuds d'administration envoient l'e-mail de test.

8. Sélectionnez **Enregistrer**.

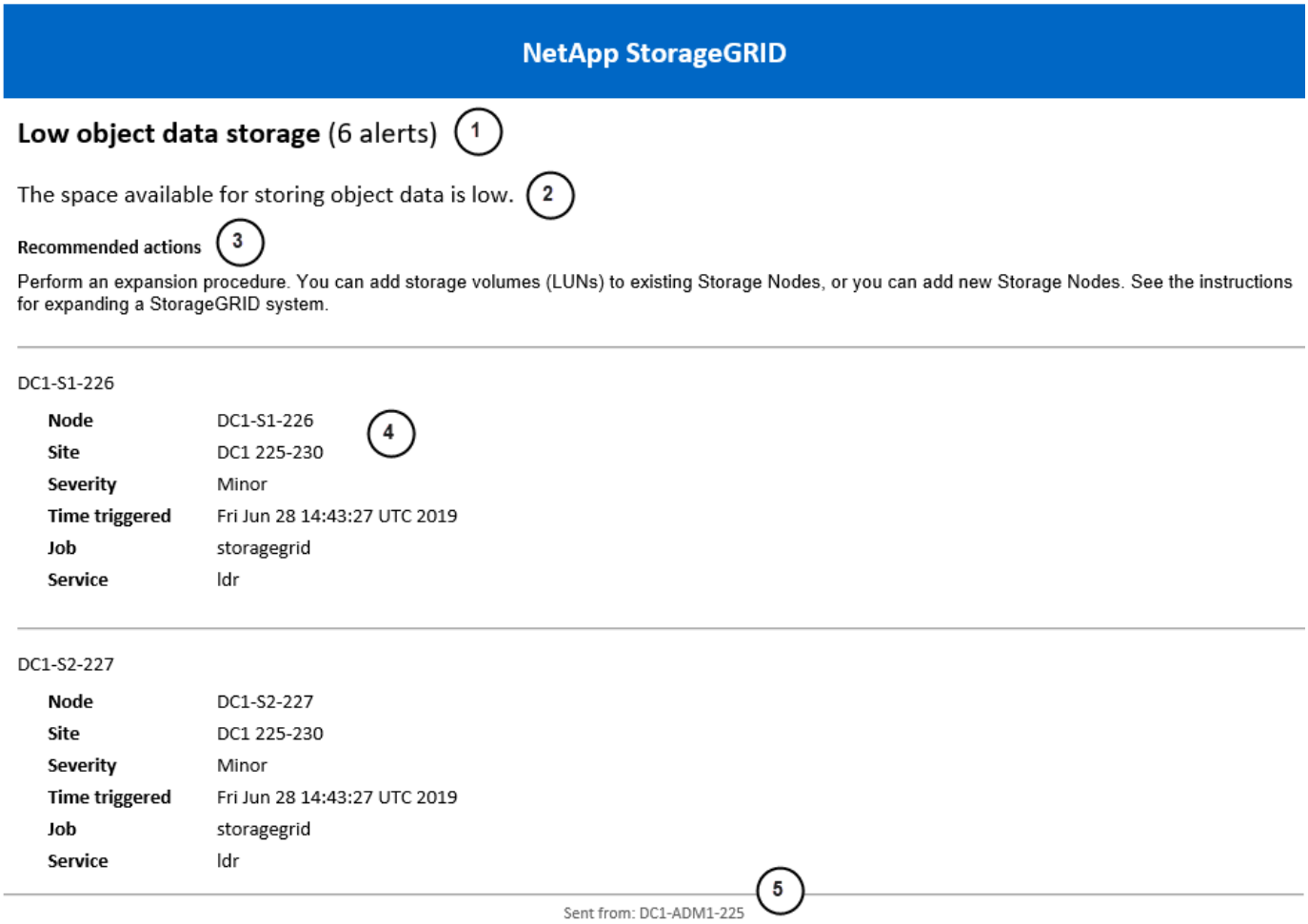
   L'envoi d'un e-mail de test n'enregistre pas vos paramètres. Vous devez sélectionner **Enregistrer**.

   Les paramètres de messagerie sont enregistrés.

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

Une fois le serveur de messagerie SMTP configuré, des notifications par courrier électronique sont envoyées aux destinataires désignés lorsqu'une alerte est déclenchée, sauf si la règle d'alerte est supprimée par un silence. Voir "Notifications d'alerte silencieuses" .

Les notifications par e-mail incluent les informations suivantes :



Appeler	Description
1	Le nom de l'alerte, suivi du nombre d'instances actives de cette alerte.
2	La 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 à laquelle la règle d'alerte a été déclenchée et le nom du travail et du service affectés.
5	Le nom d'hôte du nœud d'administration qui a envoyé la notification.

Comment les alertes sont regroupées

Pour éviter 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 courrier électronique.

Comportement	Exemple
Chaque notification d'alerte s'applique uniquement aux alertes portant le même nom. Si deux alertes portant des noms différents sont déclenchées en même temps, deux notifications par e-mail sont envoyées.	• L'alerte A est déclenchée sur deux nœuds en même temps. Une seule notification est envoyée. • L'alerte A est déclenchée sur le nœud 1 et l'alerte B est déclenchée sur le nœud 2 en même temps. Deux notifications sont envoyées : une pour chaque alerte.
Pour une alerte spécifique sur un nœud spécifique, si les seuils sont atteints pour plusieurs niveaux de gravité, une notification est envoyée uniquement pour l'alerte la plus grave.	• L'alerte A est déclenchée et les seuils d'alerte mineure, majeure et critique sont atteints. Une notification est envoyée pour l'alerte critique.
La première fois qu'une alerte est déclenchée, StorageGRID attend 2 minutes avant d'envoyer une notification. Si d'autres alertes portant le même nom sont déclenchées pendant cette période, StorageGRID regroupe toutes les alertes dans la notification initiale.	1. L'alerte A est déclenchée sur le nœud 1 à 08h00. Aucune notification n'est envoyée. 2. L'alerte A est déclenchée sur le nœud 2 à 08h01. Aucune notification n'est envoyée. 3. À 08h02, une notification est envoyée pour signaler les deux instances de l'alerte.
Si une autre alerte portant le même nom est déclenchée, StorageGRID attend 10 minutes avant d'envoyer une nouvelle notification. La nouvelle notification signale toutes les alertes actives (alertes actuelles qui n'ont pas été désactivées), même si elles ont été signalées précédemment.	1. L'alerte A est déclenchée sur le nœud 1 à 08h00. Une notification est envoyée à 08h02. 2. L'alerte A est déclenchée sur le nœud 2 à 08h05. Une deuxième notification est envoyée à 08h15 (10 minutes plus tard). Les deux nœuds sont signalés.
S'il existe plusieurs alertes actuelles portant 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.	1. L'alerte A est déclenchée pour le nœud 1. Une notification est envoyée. 2. L'alerte A est déclenchée pour le nœud 2. Une deuxième notification est envoyée. 3. L'alerte A est résolue pour le nœud 2, mais elle reste active pour le nœud 1. 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.
StorageGRID continue d'envoyer des notifications par e-mail une fois tous les 7 jours jusqu'à ce que toutes les instances de l'alerte soient résolues ou que la règle d'alerte soit désactivée.	1. L'alerte A est déclenchée pour le nœud 1 le 8 mars. Une notification est envoyée. 2. L'alerte A n'est pas résolue ou réduite au silence. Des notifications supplémentaires sont envoyées le 15 mars, le 22 mars, le 29 mars, etc.

Dépannage des notifications d'alerte par e-mail

Si l'alerte **Échec de la notification par e-mail** est déclenchée ou si vous ne parvenez pas à recevoir la notification par e-mail d'alerte de test, suivez ces étapes pour résoudre le problème.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"Gérer les alertes ou l'autorisation d'accès root" .

Étapes

1. Vérifiez vos paramètres.
   a. Sélectionnez **ALERTES** > **Configuration de la messagerie électronique**.
   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 anti-spam et assurez-vous que l'e-mail n'a pas été envoyé dans un dossier indésirable.
3. Demandez à votre administrateur de messagerie de confirmer que les e-mails provenant 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 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 que vous avez spécifié.

   Voir "Collecter les fichiers journaux et les données système" .

Notifications d'alerte silencieuses

En option, vous pouvez configurer des silences pour supprimer temporairement les notifications d'alerte.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"Gérer les alertes ou l'autorisation d'accès root" .

À propos de cette tâche

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

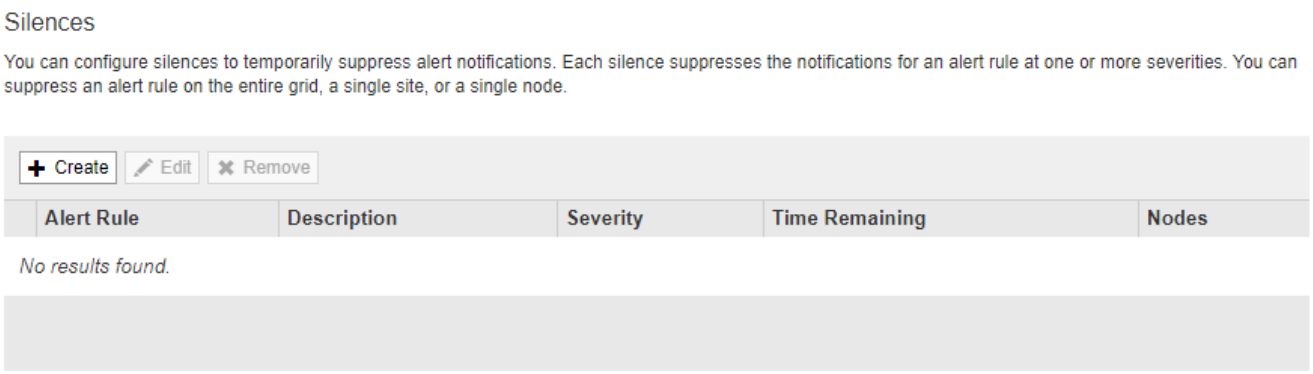
Si vous avez activé l'agent SNMP, les silences suppriment également les interruptions et les informations SNMP.

> Soyez prudent lorsque vous décidez de désactiver une règle d'alerte. Si vous désactivez une alerte, vous risquez de ne pas détecter un problème sous-jacent jusqu'à ce qu'il empêche une opération critique de se terminer.

Étapes

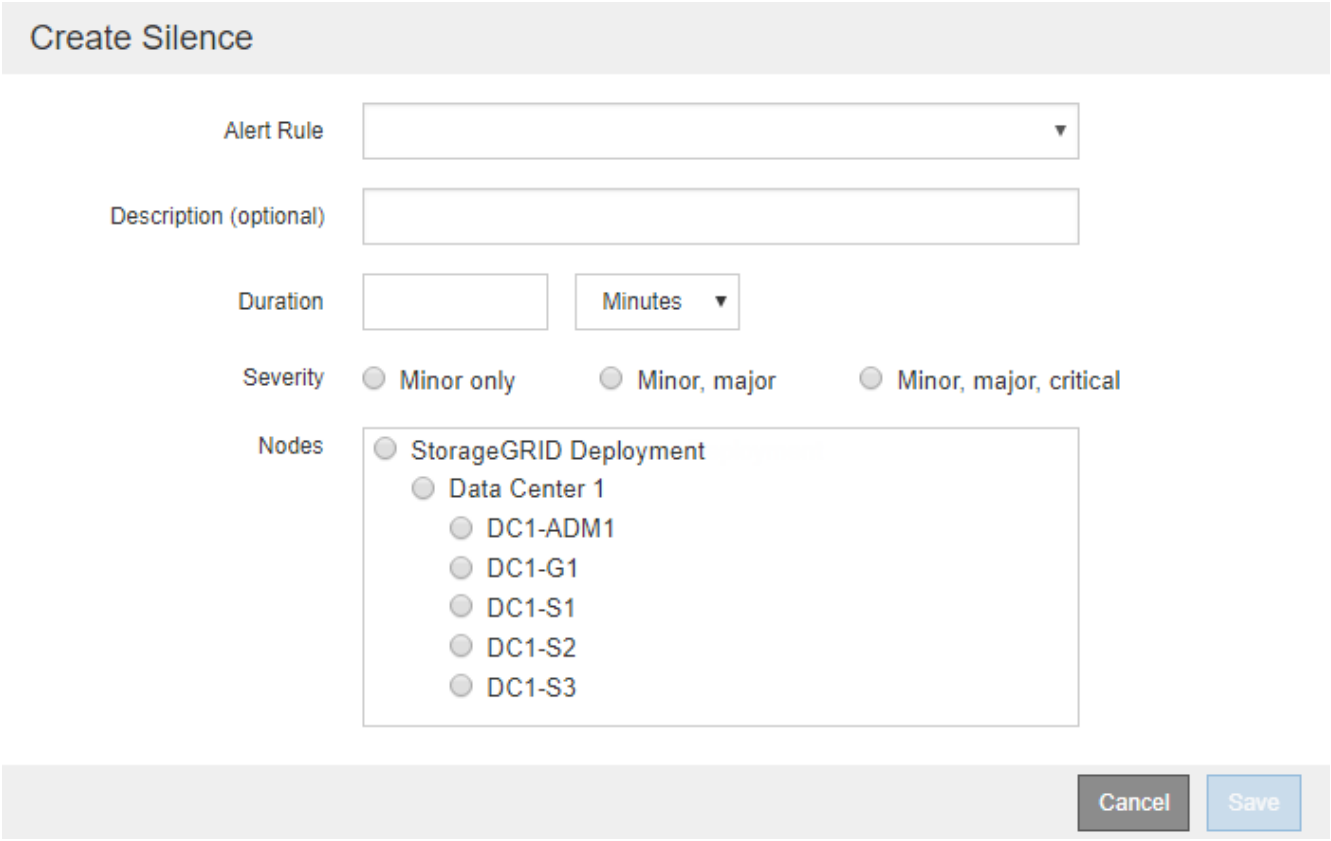
1. Sélectionnez **ALERTES** > **Silences**.

La page Silences apparaît.



2. Sélectionnez **Créer**.

La boîte de dialogue Créer un silence s'affiche.



3. Sélectionnez ou saisissez les informations suivantes :

Champ	Description
Règle d'alerte	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. **Remarque :** sélectionnez **Toutes les règles** si vous souhaitez désactiver toutes les règles d'alerte à l'aide des critères spécifiés dans cette boîte de dialogue.

Champ	Description
Description	En option, une description du silence. Par exemple, décrivez le but de ce silence.
Durée	Combien de temps souhaitez-vous que ce silence reste en vigueur, en minutes, en heures ou en jours. Un silence peut être en vigueur de 5 minutes à 1 825 jours (5 ans). **Remarque :** vous ne devez pas désactiver une règle d'alerte pendant une période prolongée. Si une règle d'alerte est désactivée, vous risquez de ne pas détecter un problème sous-jacent jusqu'à ce qu'il empêche une opération critique de se terminer. Cependant, vous devrez peut-être utiliser un silence prolongé si une alerte est déclenchée par une configuration spécifique et intentionnelle, comme cela peut être le cas pour les alertes **Lien de l'appliance de services interrompu** et les alertes **Lien de l'appliance de stockage interrompu**.
Gravité	Quelle(s) gravité(s) d'alerte doit(vent) être désactivée(s) ? Si l'alerte est déclenchée à l'un des niveaux de gravité sélectionnés, aucune notification n'est envoyée.
Nœuds	À quel(s) nœud(s) souhaitez-vous que ce silence s'applique. Vous pouvez supprimer une règle d'alerte ou toutes les règles sur l'ensemble de la grille, un seul site ou un seul nœud. Si vous sélectionnez la grille entière, 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. **Remarque :** 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	a. Sélectionnez **ALERTES** > **Silences**. b. Dans le tableau, sélectionnez le bouton radio correspondant au silence que vous souhaitez modifier. c. Sélectionnez **Modifier**. d. Modifiez la description, la durée restante, les niveaux de gravité sélectionnés ou le nœud affecté. e. Sélectionnez **Enregistrer**.

Option	Description
Supprimer un silence	a. Sélectionnez **ALERTES** > **Silences**. b. Dans le tableau, sélectionnez le bouton radio correspondant au silence que vous souhaitez supprimer. c. Sélectionnez **Supprimer**. d. Sélectionnez **OK** pour confirmer que vous souhaitez supprimer ce silence. **Remarque** : les notifications seront désormais envoyées lorsque cette alerte est déclenchée (sauf si elle est supprimée par un autre silence). Si cette alerte est actuellement déclenchée, l'envoi des notifications par e-mail ou SNMP et la mise à jour de la page Alertes peuvent prendre quelques minutes.

Informations connexes

"Configurer 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.

Selon vos besoins, vous pouvez créer des règles d'alerte personnalisées adaptées à votre approche de gestion du système.

Certaines des alertes par défaut utilisent"Métriques Prometheus" .

Alertes sur les appareils électroménagers

Nom de l'alerte	Description
La batterie de l'appareil est expirée	La batterie du contrôleur de stockage de l'appareil est épuisée.
La batterie de l'appareil est défectueuse	La batterie du contrôleur de stockage de l'appareil est défectueuse.
La batterie de l'appareil a une capacité d'apprentissage insuffisante	La batterie du contrôleur de stockage de l'appareil a une capacité d'apprentissage insuffisante.
Batterie d'appareil presque expirée	La batterie du contrôleur de stockage de l'appareil est sur le point d'expirer.
Batterie de l'appareil retirée	La batterie du contrôleur de stockage de l'appareil est manquante.
La batterie de l'appareil est trop chaude	La batterie du contrôleur de stockage de l'appareil est surchauffée.

Nom de l’alerte	Description
Erreur de communication du BMC de l’appareil	La communication avec le contrôleur de gestion de la carte mère (BMC) a été perdue.
Défaut du périphérique de démarrage de l’appareil détecté	Un problème a été détecté avec le périphérique de démarrage de l’appareil.
Échec du périphérique de sauvegarde du cache de l’appareil	Un périphérique de sauvegarde de cache persistant est tombé en panne.
Capacité insuffisante du périphérique de sauvegarde du cache de l’appareil	La capacité du périphérique de sauvegarde du cache est insuffisante.
Dispositif de sauvegarde du cache de l’appareil protégé en écriture	Un périphérique de sauvegarde de cache est protégé en écriture.
Incompatibilité de taille de mémoire cache de l’appareil	Les deux contrôleurs de l’appareil ont des tailles de cache différentes.
Défaut de batterie CMOS de l’appareil	Un problème a été détecté avec la batterie CMOS de l’appareil.
La température du châssis du contrôleur de calcul de l’appareil est trop élevée	La température du contrôleur de calcul d’un dispositif StorageGRID a dépassé un seuil nominal.
La température du processeur du contrôleur de calcul de l’appareil est trop élevée	La température du processeur dans le contrôleur de calcul d’un dispositif StorageGRID a dépassé un seuil nominal.
Le contrôleur de calcul de l’appareil nécessite une attention particulière	Une panne matérielle a été détectée dans le contrôleur de calcul d’un dispositif StorageGRID .
L’alimentation du contrôleur de calcul de l’appareil A présente un problème	L’alimentation A du contrôleur de calcul présente un problème.
L’alimentation B du contrôleur de calcul de l’appareil présente un problème	L’alimentation B du contrôleur de calcul présente un problème.
Le service de surveillance du matériel informatique de l’appareil est bloqué	Le service qui surveille l’état du matériel de stockage est bloqué.

Nom de l’alerte	Description
Le lecteur DAS de l’appareil dépasse la limite de données écrites par jour	Une quantité excessive de données est écrite sur un lecteur chaque jour, ce qui peut annuler sa garantie.
Défaut détecté sur le lecteur DAS de l’appareil	Un problème a été détecté avec un lecteur de stockage à connexion directe (DAS) dans l’appareil.
Voyant de localisation du lecteur DAS de l’appareil allumé	Le voyant de localisation de lecteur pour un ou plusieurs lecteurs de stockage à connexion directe (DAS) dans un nœud de stockage d’appliance est allumé.
Reconstruction du lecteur DAS de l’appareil	Un lecteur de stockage à connexion directe (DAS) est en cours de reconstruction. Ceci est attendu s’il a été récemment remplacé ou retiré/réinséré.
Défaut du ventilateur de l’appareil détecté	Un problème avec un bloc ventilateur de l’appareil a été détecté.
Défaut de l’appareil Fibre Channel détecté	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’appareil	Un port HBA Fibre Channel est défaillant ou a échoué.
Les lecteurs de cache flash de l’appareil ne sont pas optimaux	Les disques utilisés pour le cache SSD ne sont pas optimaux.
Boîtier d’interconnexion/de batterie de l’appareil retiré	Le boîtier d’interconnexion/batterie est manquant.
Port LACP de l’appareil manquant	Un port sur un dispositif StorageGRID ne participe pas à la liaison LACP.
Défaut de carte réseau de l’appareil détecté	Un problème avec une carte d’interface réseau (NIC) dans l’appareil a été détecté.
Alimentation électrique globale de l’appareil dégradée	La puissance d’un appareil StorageGRID s’écarte de la tension de fonctionnement recommandée.
Avertissement critique du SSD de l’appareil	Un SSD d’appareil signale un avertissement critique.
Défaillance du contrôleur de stockage de l’appareil A	Le contrôleur de stockage A d’un dispositif StorageGRID est tombé en panne.
Défaillance du contrôleur de stockage de l’appareil B	Le contrôleur de stockage B d’un dispositif StorageGRID est en panne.

Nom de l’alerte	Description
Panne du lecteur du contrôleur de stockage de l’appareil	Un ou plusieurs disques d’un dispositif StorageGRID sont en panne ou ne sont pas optimaux.
Problème matériel du contrôleur de stockage de l’appareil	Le logiciel SANtricity signale « Nécessite une attention particulière » pour un composant d’un dispositif StorageGRID .
Panne d’alimentation du contrôleur de stockage de l’appareil	L’alimentation A d’un dispositif StorageGRID s’écarte de la tension de fonctionnement recommandée.
Panne d’alimentation du contrôleur de stockage de l’appareil B	L’alimentation B d’un dispositif StorageGRID s’écarte de la tension de fonctionnement recommandée.
Le service de surveillance du matériel de stockage des appareils est bloqué	Le service qui surveille l’état du matériel de stockage est bloqué.
Étagères de rangement des appareils dégradées	L’état de l’un des composants de l’étagère de stockage d’un dispositif 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 retiré.
Erreur de démarrage sécurisé UEFI de l’appareil	Un appareil n’a pas été démarré en toute sécurité.
Les E/S du disque sont très lentes	Des E/S de disque très lentes peuvent avoir un impact sur les performances de la grille.
Défaut de ventilateur de l’appareil de stockage détecté	Un problème avec une unité de ventilation dans le contrôleur de stockage d’un appareil a été détecté.
Connectivité de stockage dégradée	Il y a un problème avec 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 de syslog

Nom de l’alerte	Description
Les 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 en mémoire se remplit.

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 du disque pour les messages d’audit est pleine. Si cette condition n’est pas résolue, les opérations S3 ou Swift peuvent échouer.
Les 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 se remplit.

Alertes de seau

Nom de l’alerte	Description
Le bucket FabricPool a un paramètre de cohérence de bucket non pris en charge	Un bucket FabricPool utilise le niveau de cohérence Disponible ou Site fort, qui n’est pas pris en charge.
Le bucket FabricPool a un paramètre de contrôle de version non pris en charge	Un bucket FabricPool a le contrôle de version ou le verrouillage d’objet S3 activé, qui ne sont pas pris en charge.

Alertes Cassandra

Nom de l’alerte	Description
Erreur du compacteur automatique Cassandra	Le compacteur automatique Cassandra a rencontré une erreur.
Les mesures du compacteur automatique Cassandra sont obsolètes	Les métriques qui décrivent l’auto-compacteur Cassandra sont obsolètes.
Erreur de communication Cassandra	Les nœuds qui exécutent le service Cassandra ont des difficultés à communiquer entre eux.
Les compactions de Cassandra sont surchargées	Le processus de compactage de Cassandra est surchargé.
Erreur d’écriture surdimensionnée de Cassandra	Un processus StorageGRID interne a envoyé une demande d’écriture à Cassandra qui était trop volumineuse.
Les mesures de réparation de Cassandra sont obsolètes	Les métriques qui décrivent les travaux de réparation de Cassandra sont obsolètes.
La réparation de Cassandra progresse lentement	La progression des réparations de la base de données Cassandra est lente.

Nom de l’alerte	Description
Service de réparation Cassandra non disponible	Le service de réparation Cassandra n’est pas disponible.
Corruption de la table Cassandra	Cassandra a détecté une corruption de table. Cassandra redémarre automatiquement s’il détecte une corruption de table.

Alertes du pool de stockage cloud

Nom de l’alerte	Description
Erreur de connectivité du pool de stockage cloud	Le contrôle d’intégrité des pools de stockage cloud a détecté une ou plusieurs nouvelles erreurs.
Expiration de la certification d’entité finale IAM Roles Anywhere	Le certificat d’entité finale IAM Roles Anywhere est sur le point d’expirer.

Alertes de réplication inter-réseaux

Nom de l’alerte	Description
Échec permanent de la réplication inter-réseau	Une erreur de réplication inter-grille s’est produite et nécessite l’intervention de l’utilisateur pour être résolue.
Ressources de réplication inter-réseaux indisponibles	Les demandes de réplication inter-grille sont en attente car une ressource n’est pas disponible.

Alertes DHCP

Nom de l’alerte	Description
Le bail DHCP a expiré	Le bail DHCP sur une interface réseau a expiré.
Le bail 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 traçage

Nom de l’alerte	Description
Impact sur les performances de débogage	Lorsque le mode de 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 négativement.

Alertes par e-mail et AutoSupport

Nom de l'alerte	Description
Échec de l'envoi du message AutoSupport	Le message AutoSupport le plus récent n'a pas pu être envoyé.
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	La notification par e-mail d'une alerte n'a pas pu être envoyée.
SNMP informe les erreurs	Erreurs lors de l'envoi de notifications d'information SNMP à une destination d'interruption.
Connexion SSH ou console détectée	Au cours des dernières 24 heures, un utilisateur s'est connecté avec la console Web ou SSH.

Alertes de codage d'effacement (EC)

Nom de l'alerte	Description
Échec du rééquilibrage de l'EC	La procédure de rééquilibrage de la CE a échoué ou a été arrêtée.
Échec de la réparation de l'EC	Une tâche de réparation des données EC a échoué ou a été arrêtée.
Réparation de l'EC bloquée	Une tâche de réparation des données EC est bloquée.
Erreur de vérification des fragments codés par effacement	Les fragments codés par effacement ne peuvent plus être vérifiés. Les fragments corrompus peuvent ne pas être réparés.

Alertes d'expiration des certificats

Nom de l'alerte	Description
Expiration du certificat CA du proxy administrateur	Un ou plusieurs certificats du groupe CA du serveur proxy d'administration sont sur le point d'expirer.
Expiration du certificat client	Un ou plusieurs certificats clients 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 du point de terminaison de l'équilibreur de charge	Un ou plusieurs certificats de point de terminaison d'équilibrage de charge sont sur le point d'expirer.

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

Alertes du réseau Grid

Nom de l’alerte	Description
Inadéquation du MTU du réseau de grille	Le paramètre MTU pour l’interface du réseau de grille (eth0) diffère considérablement selon les nœuds de la grille.

Alertes de la fédération du réseau

Nom de l’alerte	Description
Expiration du certificat de fédération de réseau	Un ou plusieurs certificats de fédération de grille sont sur le point d’expirer.
Échec de la connexion à la fédération de réseau	La connexion de fédération de réseau entre le réseau local et le réseau distant ne fonctionne pas.

Alertes d’utilisation élevée ou de latence élevée

Nom de l’alerte	Description
Utilisation élevée du tas Java	Un pourcentage élevé de l’espace du tas Java est utilisé.
Latence élevée pour les requêtes de métadonnées	Le temps moyen des requêtes de métadonnées Cassandra est trop long.

Alertes de fédération d’identité

Nom de l’alerte	Description
Échec de la synchronisation de la fédération d’identité	Impossible de synchroniser les groupes fédérés et les utilisateurs à partir de la source d’identité.

Nom de l’alerte	Description
Échec de la synchronisation de la fédération d’identité pour un locataire	Impossible de synchroniser les groupes fédérés et les utilisateurs à partir de la source d’identité configurée par un locataire.

Alertes de gestion du cycle de vie de l’information (ILM)

Nom de l’alerte	Description
Placement ILM irréalisable	Une instruction de placement dans une règle ILM ne peut pas être réalisée pour certains objets.
Taux de balayage ILM faible	Le taux de numérisation ILM est défini sur moins de 100 objets/seconde.

Alertes du serveur de gestion des clés (KMS)

Nom de l’alerte	Description
Expiration du certificat KMS CA	Le certificat de l’autorité de certification (CA) utilisé pour signer le certificat du serveur de gestion de clés (KMS) est sur le point d’expirer.
Expiration du certificat client KMS	Le certificat client d’un serveur de gestion de clés est sur le point d’expirer
Échec du chargement de la configuration KMS	La configuration du serveur de gestion des clés existe mais n’a pas pu être chargée.
Erreur de connectivité KMS	Un nœud d’appareil n’a pas pu se connecter au serveur de gestion des clés de son site.
Nom de la clé de chiffrement KMS introuvable	Le serveur de gestion de clés configuré ne dispose pas de clé de chiffrement correspondant au nom fourni.
Échec de la rotation de la clé de chiffrement KMS	Tous les volumes de l’appareil ont été déchiffrés avec succès, mais un ou plusieurs volumes n’ont pas pu pivoter vers la dernière clé.
KMS n’est pas configuré	Aucun serveur de gestion de clés n’existe pour ce site.
La clé KMS n’a pas réussi à déchiffrer un volume d’appareil	Un ou plusieurs volumes sur un appareil avec chiffrement de nœud activé n’ont pas pu être déchiffrés 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.
Échec de connectivité du serveur KMS	Un nœud d’appareil n’a pas pu se connecter à un ou plusieurs serveurs du cluster de serveurs de gestion de clés pour son site.

Alertes de l’équilibreur de charge

Nom de l’alerte	Description
Connexions d’équilibrage de charge sans demande élevée	Un pourcentage élevé de connexions aux points de terminaison de l’équilibreur de charge se sont déconnectées sans exécuter de requêtes.

Alertes de décalage d’horloge locale

Nom de l’alerte	Description
Grand décalage horaire de l’horloge locale	Le décalage entre l’horloge locale et l’heure du protocole NTP (Network Time Protocol) est trop important.

Alertes de faible mémoire ou d’espace insuffisant

Nom de l’alerte	Description
Faible capacité du disque du journal d’audit	L’espace disponible pour les journaux d’audit est faible. Si cette condition n’est pas résolue, les opérations S3 ou Swift peuvent échouer.
Faible mémoire de nœud disponible	La quantité de RAM disponible sur un nœud est faible.
Faible espace libre pour le pool de stockage	L’espace disponible pour stocker les données d’objet dans le nœud de stockage est faible.
Faible mémoire de nœud installée	La quantité de mémoire installée sur un nœud est faible.
Stockage de métadonnées faibles	L’espace disponible pour stocker les métadonnées des objets est faible.
Faible capacité de disque métrique	L’espace disponible pour la base de données des métriques est faible.
Faible stockage de données d’objets	L’espace disponible pour stocker les données des objets est faible.
Remplacement du filigrane en lecture seule	Le remplacement du filigrane en lecture seule du volume de stockage est inférieur au filigrane optimisé minimum pour un nœud de stockage.
Faible capacité du disque racine	L’espace disponible sur le disque racine est faible.
Faible capacité de données du système	L’espace disponible pour /var/local est faible. Si cette condition n’est pas résolue, les opérations S3 ou Swift peuvent échouer.
Espace libre dans le répertoire tmp faible	L’espace disponible dans le répertoire /tmp est faible.

Alertes de nœud ou de réseau de nœuds

Nom de l'alerte	Description
Utilisation de réception du réseau d'administration	L'utilisation de réception sur le réseau d'administration est élevée.
Utilisation de la transmission du réseau administrateur	L'utilisation de la transmission sur le réseau d'administration est élevée.
Échec de la configuration du pare-feu	Échec de l'application de la configuration du pare-feu.
Points de terminaison de l'interface de gestion en mode de secours	Tous les points de terminaison de l'interface de gestion reviennent depuis trop longtemps aux ports par défaut.
Erreur de connectivité du réseau de nœuds	Des erreurs se sont produites lors du transfert de données entre les nœuds.
Erreur de trame de réception du réseau de nœuds	Un pourcentage élevé de trames réseau reçues par un nœud comportaient des erreurs.
Le nœud n'est pas synchronisé avec le serveur NTP	Le nœud n'est pas synchronisé avec le serveur de protocole de temps réseau (NTP).
Nœud non verrouillé avec le serveur NTP	Le nœud n'est pas verrouillé sur un serveur de protocole de temps réseau (NTP).
Réseau de nœuds non-appareils en panne	Un ou plusieurs périphériques réseau sont en panne ou déconnectés.
Liaison de l'appareil de services en panne sur le réseau d'administration	L'interface de l'appareil avec le réseau d'administration (eth1) est en panne ou déconnectée.
Liaison de l'appareil de services interrompue sur le port 1 du réseau d'administration	Le port réseau administrateur 1 de l'appareil est en panne ou déconnecté.
Liaison de l'appareil de services en panne sur le réseau client	L'interface de l'appareil avec le réseau client (eth2) est en panne ou déconnectée.
Liaison de l'appareil de services interrompue sur le port réseau 1	Le port réseau 1 de l'appareil est hors service ou déconnecté.
Liaison de l'appareil de services interrompue sur le port réseau 2	Le port réseau 2 de l'appareil est hors service ou déconnecté.

Nom de l’alerte	Description
Liaison de l’appareil de services interrompue sur le port réseau 3	Le port réseau 3 de l’appareil est hors service ou déconnecté.
Liaison de l’appareil de services interrompue sur le port réseau 4	Le port réseau 4 de l’appareil est hors service ou déconnecté.
Liaison du dispositif de stockage interrompue sur le réseau d’administration	L’interface de l’appareil avec le réseau d’administration (eth1) est en panne ou déconnectée.
Liaison du dispositif de stockage interrompue sur le port 1 du réseau administrateur	Le port réseau administrateur 1 de l’appareil est en panne ou déconnecté.
Liaison du dispositif de stockage interrompue sur le réseau client	L’interface de l’appareil avec le réseau client (eth2) est en panne ou déconnectée.
Liaison du dispositif de stockage interrompue sur le port réseau 1	Le port réseau 1 de l’appareil est hors service ou déconnecté.
Liaison du dispositif de stockage interrompue sur le port réseau 2	Le port réseau 2 de l’appareil est hors service ou déconnecté.
Liaison du dispositif de stockage interrompue sur le port réseau 3	Le port réseau 3 de l’appareil est hors service ou déconnecté.
Liaison du dispositif de stockage interrompue sur le port réseau 4	Le port réseau 4 de l’appareil est hors service ou déconnecté.
Le nœud de stockage n’est pas dans l’état de stockage souhaité	Le service LDR sur 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 approche le nombre maximum pouvant être suivi.
Impossible de communiquer avec le nœud	Un ou plusieurs services ne répondent pas ou le nœud ne peut pas être atteint.
Redémarrage inattendu du nœud	Un nœud a redémarré de manière inattendue au cours des dernières 24 heures.

Alertes d’objets

Nom de l’alerte	Description
La vérification de l’existence de l’objet a échoué	La tâche de vérification de l’existence de l’objet a échoué.
Vérification de l’existence de l’objet 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 PUT 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 d’objets répliqués qui n’a pas pu être identifié comme un objet répliqué.

Alertes des services de la plateforme

Nom de l’alerte	Description
Faible capacité des demandes en attente des services de la plateforme	Le nombre de demandes de services de plateforme en attente approche de sa capacité.
Services de plateforme indisponibles	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 une attention particulière	Un volume de stockage est hors ligne et nécessite une attention particulière.
Le volume de stockage doit être restauré	Un volume de stockage a été récupéré 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 était hors ligne et a déclenché un remontage automatique. Cela pourrait indiquer un problème de lecteur ou des erreurs de système de fichiers.
La restauration du volume n’a pas réussi à 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 désormais utilisée.
service nginx-gw utilisant la configuration de sauvegarde	La configuration du service nginx-gw n'est pas valide. La configuration précédente est désormais utilisée.
Redémarrage requis pour désactiver FIPS	La politique de sécurité ne nécessite pas le mode FIPS, mais le module de sécurité cryptographique NetApp est activé.
Redémarrage requis pour activer FIPS	La politique 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 désormais utilisée.

Alertes locataires

Nom de l'alerte	Description
Utilisation élevée des quotas des locataires	Un pourcentage élevé d'espace de quota est utilisé. Cette règle est désactivée par défaut car elle pourrait entraîner trop de notifications.

Métriques Prometheus couramment utilisées

Consultez cette liste de mesures Prometheus couramment utilisées pour mieux comprendre les conditions des règles d'alerte par défaut ou pour créer les conditions des règles d'alerte personnalisées.

Vous pouvez également obtenir une liste complète de toutes les métriques .

Pour plus de détails sur la syntaxe des requêtes Prometheus, voir "Interroger Prométhée" .

Quelles sont les métriques Prometheus ?

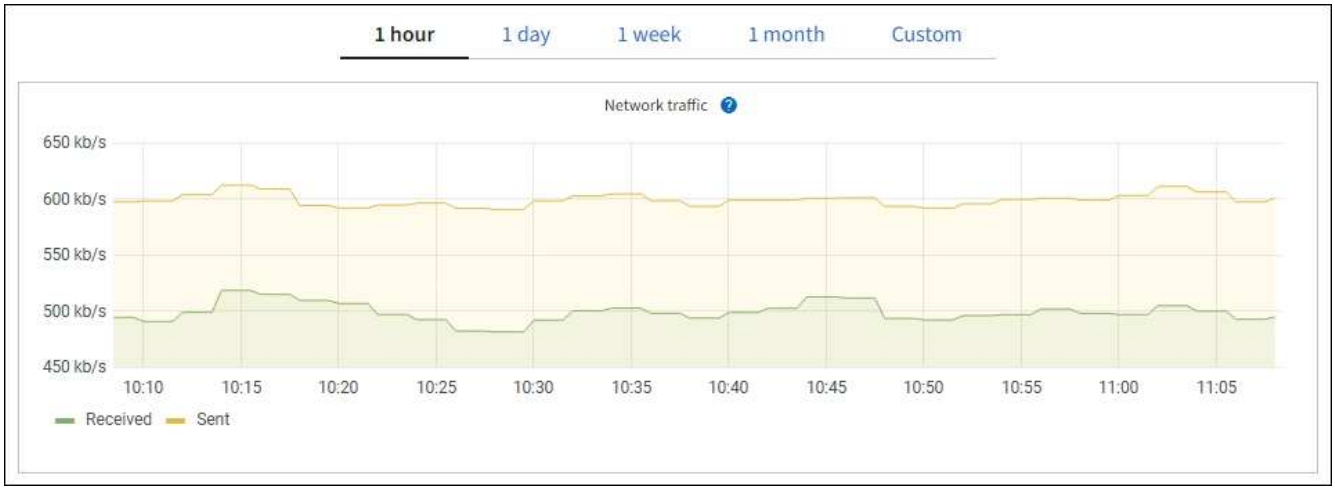
Les métriques Prometheus sont des mesures de séries chronologiques. Le service Prometheus sur les nœuds d'administration collecte ces métriques à partir des services sur tous les nœuds. Les métriques sont stockées sur chaque nœud d'administration jusqu'à ce que l'espace réservé aux données Prometheus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

Où sont utilisées les métriques Prometheus ?

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

- **Page Nœuds** : Les graphiques et diagrammes des onglets disponibles sur la page Nœuds utilisent l'outil de visualisation Grafana pour afficher les métriques de séries chronologiques collectées par Prometheus. Grafana affiche les données de séries chronologiques sous forme de graphiques et de tableaux, tandis

que Prometheus sert de source de données principale.



- **Alertes** : les alertes sont déclenchées à des niveaux de gravité spécifiques lorsque les conditions de règle d'alerte qui utilisent les métriques Prometheus sont évaluées comme vraies.
- **API de gestion de grille** : vous pouvez utiliser les métriques Prometheus dans des règles d'alerte personnalisées ou avec des outils d'automatisation externes pour surveiller votre système StorageGRID . Une liste complète des métriques Prometheus est disponible à partir de l'API Grid Management. (En haut du gestionnaire de grille, sélectionnez l'icône d'aide et sélectionnez **Documentation API** > **métriques**.) Bien que plus d'un millier de mesures soient disponibles, seul un nombre relativement restreint est nécessaire pour surveiller les opérations StorageGRID les plus critiques.

> Les métriques qui incluent *private* dans leurs noms sont destinées à un usage interne uniquement et sont susceptibles d'être modifiées entre les versions de StorageGRID sans préavis.

- La page **SUPPORT** > **Outils** > **Diagnostics** et la page **SUPPORT** > **Outils** > **Métriques** : Ces pages, qui sont principalement destinées à être utilisées par le support technique, fournissent plusieurs outils et graphiques qui utilisent les valeurs des métriques Prometheus.

> Certaines fonctionnalités et éléments de menu de la page Métriques sont intentionnellement non fonctionnels et sont susceptibles d'être modifiés.

Liste des mesures les plus courantes

La liste suivante contient les métriques Prometheus les plus couramment utilisées.

> Les métriques qui incluent *private* dans leurs noms sont destinées à un usage interne uniquement et sont susceptibles d'être modifiées sans préavis entre les versions de StorageGRID .

alertmanager_notifications_échec_total
Le nombre total de notifications d'alerte ayant échoué.

node_filesystem_avail_bytes
La quantité d'espace du système de fichiers disponible pour les utilisateurs non root en octets.

node_memory_MemAvailable_bytes

Champ d'informations sur la mémoire MemAvailable_bytes.

nœud_réseau_opérateur

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

noeud_réseau_réception_erreurs_total

Statistiques du périphérique réseau `receive_errs`.

erreurs_de_transmission_réseau_nœud_total

Statistiques du périphérique réseau `transmit_errs`.

storagegrid_administrativement_en_arrêt

Le nœud n'est pas connecté au réseau pour une raison attendue. Par exemple, le nœud ou les services sur le nœud ont été arrêtés correctement, le nœud redémarre ou le logiciel est en cours de mise à niveau.

état_matériel_du_contrôleur_de_calcul_de_l'appareil_de_grille_de_stockage

L'état du matériel du contrôleur de calcul dans un appareil.

disques_défaillants_de_l'appareil_de_grille_de_stockage

Pour le contrôleur de stockage d'un appareil, le nombre de lecteurs qui ne sont pas optimaux.

état_matériel_du_contrôleur_de_stockage_de_l'appareil_de_grille_de_stockage

L'état général du matériel du contrôleur de stockage dans un appareil.

buckets_et_conteneurs_de_contenu_de_grille_de_stockage

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

objets_de_contenu_de_grille_de_stockage

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

storagegrid_content_objects_lost

Le nombre total d'objets que ce service détecte comme manquants dans le système StorageGRID . Des mesures doivent être prises pour déterminer la cause de la perte et si une récupération est possible.

"Résoudre les problèmes de données d'objets perdues ou manquantes"

storagegrid_http_sessions_entrantes_tentatives

Le nombre total de sessions HTTP qui ont été tentées sur un nœud de stockage.

storagegrid_http_sessions_entrantes_actuellement_établies

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

storagegrid_http_sessions_incoming_failed

Le nombre total de sessions HTTP qui n'ont pas abouti, soit en raison d'une requête HTTP mal formée, soit en raison d'un échec lors du traitement d'une opération.

storagegrid_http_sessions_entrantes_réussies

Le nombre total de sessions HTTP qui se sont terminées avec succès.

storagegrid_ilm_attend_des_objets_d'arrière-plan

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

storagegrid_ilm_en_attente_d'évaluation_client_objets_par_seconde

Le taux actuel auquel les objets sont évalués par rapport à la politique ILM sur ce nœud.

storagegrid_ilm_en_attente_d'objets_client

Nombre total d'objets sur ce nœud en attente d'évaluation ILM à partir des opérations client (par exemple, l'ingestion).

storagegrid_ilm_en_attente_du_nombre_total_d'objets

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

storagegrid_ilm_scan_objets_par_seconde

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

storagegrid_ilm_scan_period_estimated_minutes

Le temps estimé pour effectuer une analyse ILM complète sur ce nœud.

Remarque : une analyse complète ne garantit pas que l'ILM a été appliqué à tous les objets appartenant à ce nœud.

heure d'expiration du certificat du point de terminaison de l'équilibreur de charge de la grille de stockage

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

storagegrid_metadata_queries_average_latency_milliseconds

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

storagegrid_network_received_bytes

La quantité totale de données reçues depuis l'installation.

octets_transmis_réseau_grille_de_stockage

La quantité totale de données envoyées depuis l'installation.

pourcentage_d'utilisation_du_processeur_du_nœud_de_grille_de_stockage

Le pourcentage de temps CPU disponible actuellement utilisé par ce service. Indique à quel point le service est occupé. La quantité de temps CPU disponible dépend du nombre de CPU du serveur.

storagegrid_ntp_chosen_time_source_offset_millisecondes

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

storagegrid_ntp_locked

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 vers 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 nœud de stockage depuis la dernière réinitialisation de l'attribut.

storagegrid_s3_operations_failed

Nombre total d'opérations S3 ayant échoué (codes d'état HTTP 4xx et 5xx), à l'exclusion de celles causées par un 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, résultant d'un échec d'autorisation.

jours d'expiration du certificat de l'interface de gestion du certificat du serveur de grille de stockage

Le nombre de jours avant l'expiration du certificat de l'interface de gestion.

certificat_serveur_grille_de_stockage_points_de_terminaison_API_de_stockage_jours_expiration_du_certificat

Le nombre de jours avant l'expiration du certificat API Object Storage.

service_grille_stockage_cpu_secondes

La durée cumulée pendant laquelle le processeur a été utilisé par ce service depuis l'installation.

utilisation_mémoire_octets_service_grille_de_stockage

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

service_grille_de_stockage_réseau_octets_reçus

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

réseau_de_services_de_grille_de_stockage_octets_transmis

La quantité totale de données envoyées par ce service.

redémarrages du service storagegrid

Le nombre total de fois où le service a été redémarré.

storagegrid_service_runtime_seconds

La durée totale d'exécution du service depuis l'installation.

storagegrid_service_uptime_seconds

La durée totale d'exécution du service depuis son dernier redémarrage.

grille_de_stockage_état_courant

L'état actuel des services de stockage. Les valeurs des attributs sont :

- 10 = Hors ligne
- 15 = Entretien
- 20 = Lecture seule

- 30 = En ligne

état_stockage_grille_de_stockage

L'état actuel des services de stockage. Les valeurs des attributs sont :

- 0 = Aucune erreur
- 10 = En transition
- 20 = Espace libre insuffisant
- 30 = Volume(s) indisponible(s)
- 40 = Erreur

grille_de_stockage_utilisation_du_stockage_octets_de_données

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

storagegrid_storage_utilisation_métadonnées_autorisées_octets

L'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 la base de données (telles que le compactage et la réparation) et les futures mises à niveau matérielles et logicielles. L'espace autorisé pour les métadonnées d'objet contrôle la capacité globale de l'objet.

grille_de_stockage_utilisation_du_stockage_métadonnées_octets

La quantité de métadonnées d'objet sur le volume de stockage 0, en octets.

storagegrid_storage_utilisation_total_espace_octets

La quantité totale d'espace de stockage allouée à tous les magasins d'objets.

grille_de_stockage_utilisation_espace_utilisable_octets

La quantité totale d'espace de stockage d'objets restant. Calculé en additionnant la quantité d'espace disponible pour tous les magasins d'objets sur le nœud de stockage.

storagegrid_swift_data_transfers_bytes_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_transfers_bytes_récupérés

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

échec des opérations de storagegrid_swift

Nombre total d'opérations Swift ayant échoué (codes d'état HTTP 4xx et 5xx), à l'exclusion de celles causées par un échec d'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, résultant d'un échec d'autorisation (codes d'état HTTP 401, 403, 405).

octets de données d'utilisation du locataire de la grille de stockage
La taille logique de tous les objets pour le locataire.

nombre_d'objets_d'utilisation_locataire_de_grille_de_stockage
Le nombre d'objets pour le locataire.

quota_d'utilisation_locataire_de_grille_de_stockage_octets
La 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 métriques

Pour obtenir la liste complète des métriques, utilisez l'API Grid Management.

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

Référence des fichiers journaux

Référence des fichiers journaux

StorageGRID fournit des journaux utilisés pour capturer des événements, des messages de diagnostic et des conditions d'erreur. Il peut vous être demandé de collecter des fichiers journaux et de les transmettre au support technique pour aider au dépannage.

Les journaux sont classés comme suit :

- "Journaux du logiciel StorageGRID"
- "Journaux de déploiement et de maintenance"
- "À propos du bycast.log"

> Les détails fournis pour chaque type de journal sont fournis à titre indicatif 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 d'application dépassent le cadre de ces instructions.

Accéder aux journaux

Pour accéder aux journaux, vous pouvez"collecter les fichiers journaux et les données système" à partir d'un ou plusieurs nœuds sous forme d'archive de fichier journal unique. Ou, si le nœud d'administration principal n'est pas disponible ou ne peut pas atteindre un nœud spécifique, vous pouvez accéder aux fichiers journaux individuels pour chaque nœud de grille comme suit :

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

4. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

Exporter les journaux vers le serveur syslog

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

- Recevez une 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 causé par les méthodes de journalisation d'audit.
- Accès aux requêtes de la couche HTTP et aux codes d'erreur faciles à analyser.
- Meilleure visibilité sur les requêtes bloquées par les classificateurs de trafic au niveau de l'équilibreur de charge.

Pour exporter les journaux, reportez-vous à"Configurer les messages d'audit et les destinations des journaux" .

Catégories de fichiers journaux

L'archive du fichier journal StorageGRID contient les journaux décrits pour chaque catégorie et des fichiers supplémentaires contenant des métriques et la sortie des commandes de débogage.

Emplacement des archives	Description
audit	Messages d'audit générés pendant le fonctionnement normal du système.
journaux du système d'exploitation de base	Informations sur le système d'exploitation de base, y compris les versions d'image StorageGRID .
paquets	Informations de configuration globale (bundles).
Cassandre	Informations sur la base de données Cassandra et journaux de réparation Reaper.
ec	Informations VCS sur le nœud actuel et informations sur le groupe EC par ID de profil.
grille	Journaux de grille généraux, y compris le débogage(`bycast.log`) et `servermanager` journaux.
grille.json	Fichier de configuration de grille partagé entre tous les nœuds. En plus, `node.json` est spécifique au nœud actuel.
hagroupes	Mesures et journaux des groupes de haute disponibilité.
installer	`Gdu-server`et installer les journaux.
Arbitre lambda	Journaux liés à la demande de proxy S3 Select.

Emplacement des archives	Description
bûcheron.log	Messages de débogage liés à la collecte de journaux.
Métrique	Journaux de service pour Grafana, Jaeger, l'exportateur de nœuds et Prometheus.
divers	Journaux d'accès et d'erreurs Miscd.
MySQL	La configuration de la base de données mariaDB et les journaux associés.
filet	Journaux générés par les scripts liés au réseau et le service Dynip.
nginx	Fichiers et journaux de configuration de l'équilibreur de charge et de la fédération de grille. Inclut également les journaux de trafic Grid Manager et Tenant Manager.
nginx-gw	• `access.log`:Messages du journal des demandes du gestionnaire de grille et du gestionnaire de locataires. ◦ Ces messages sont préfixés par `mgmt:` lorsqu'il est exporté à l'aide de syslog. ◦ Le format de ces messages de journal est `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$request" "$http_host" "$http_user_agent" "$http_referer"` • `cgr-access.log.gz`:Demandes de réplication inter-grille entrantes. ◦ Ces messages sont préfixés par `cgr:` lorsqu'il est exporté à l'aide de syslog. ◦ Le format de ces messages de journal est `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$upstream_addr" "$request" "$http_host"` • `endpoint-access.log.gz`:S3 et Swift demandent aux points de terminaison de l'équilibreur de charge. ◦ Ces messages sont préfixés par `endpoint:` lorsqu'il est exporté à l'aide de syslog. ◦ Le format de ces messages de journal est `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$upstream_addr" "$request" "$http_host"` • `nginx-gw-dns-check.log`:En rapport avec la nouvelle alerte de vérification DNS.
ntp	Fichier de configuration et journaux NTP.

Emplacement des archives	Description
Objets orphelins	Journaux relatifs aux objets orphelins.
os	Fichier d'état des nœuds et des grilles, y compris les services `pid` .
autre	Fichiers journaux sous `/var/local/log` qui ne sont pas collectés dans d'autres dossiers.
performances	Informations sur les performances du processeur, du réseau et des E/S disque.
données de Prometheus	Métriques Prometheus actuelles, si la collecte de journaux inclut des données Prometheus.
approvisionnement	Journaux liés au processus de provisionnement du réseau.
radeau	Journaux du cluster Raft utilisés dans les services de la plateforme.
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 de sockets pour le débogage du réseau.
commandes-système.txt	Sortie des commandes du conteneur StorageGRID . Contient des informations système, telles que la mise en réseau et l'utilisation du disque.
synchronisation-recuperation-package	Lié au maintien de la cohérence du dernier package de récupération sur tous les nœuds d'administration et nœuds de stockage qui hébergent le service ADC.

Journaux du logiciel StorageGRID

Vous pouvez utiliser les journaux StorageGRID pour résoudre les problèmes.

Si vous souhaitez envoyer vos journaux à un serveur syslog externe ou modifier la destination des informations d'audit telles que le `bycast.log` et `nms.log` , voir"Configurer les messages d'audit et les destinations des journaux" .

Journaux généraux StorageGRID

Nom des fichiers	Remarques	Trouvé sur
/var/local/log/bycast.log	Le fichier de dépannage principal de StorageGRID . Sélectionnez **SUPPORT** > **Outils** > **Topologie de grille**. Sélectionnez ensuite ***Site*** > ***Node*** > **SSM** > **Événements**.	Tous les nœuds
/var/local/log/bycast-err.log	Contient un sous-ensemble de `bycast.log` (messages de gravité ERREUR et CRITIQUE). Des messages CRITIQUES sont également affichés dans le système. Sélectionnez **SUPPORT** > **Outils** > **Topologie de grille**. Sélectionnez ensuite ***Site*** > ***Node*** > **SSM** > **Événements**.	Tous les nœuds
/var/local/core/	Contient tous les fichiers de vidage de mémoire créés si le programme se termine anormalement. Les causes possibles incluent les échecs d'assertion, les violations ou les délais d'expiration des threads. **Remarque** : Le fichier `` `/var/local/core/kexec_cmd `` existe généralement sur les nœuds d'appareil et n'indique pas d'erreur.	Tous les nœuds

Journaux liés au chiffrement

Nom des fichiers	Remarques	Trouvé sur
/var/local/log/ssh-config-generation.log	Contient les journaux liés à la génération de configurations SSH et au rechargement des services SSH.	Tous les nœuds
/var/local/log/nginx/config-generation.log	Contient les journaux liés à la génération de configurations nginx et au rechargement des services nginx.	Tous les nœuds
/var/local/log/nginx-gw/config-generation.log	Contient les journaux liés à la génération de configurations nginx-gw (et au rechargement des services nginx-gw).	Nœuds d'administration et de passerelle
/var/local/log/update-cipher-configurations.log	Contient les journaux liés à la configuration des politiques TLS et SSH.	Tous les nœuds

Journaux de la fédération de grille

Nom des fichiers	Remarques	Trouvé sur
/var/local/log/update_grid_federation_config.log	Contient les journaux liés à la génération de configurations nginx et nginx-gw pour les connexions de fédération de grille.	Tous les nœuds

Journaux NMS

Nom des fichiers	Remarques	Trouvé sur
/var/local/log/nms.log	• Capture les notifications du gestionnaire de grille et du gestionnaire de locataires. • Capture les événements liés au fonctionnement du service NMS. Par exemple, les notifications par e-mail et les modifications de configuration. • Contient les mises à jour du bundle XML résultant des modifications de configuration apportées au système. • Contient des messages d'erreur liés au sous-échantillonnage des attributs effectué une fois par jour. • Contient des messages d'erreur du serveur Web Java, par exemple, des erreurs de génération de page et des erreurs d'état HTTP 500.	Nœuds d'administration
/var/local/log/nms.errlog	Contient des messages d'erreur liés aux mises à niveau de la base de données MySQL. Contient le flux d'erreur standard (stderr) des services correspondants. Il y a un fichier journal par service. Ces fichiers sont généralement vides, sauf en cas de problèmes avec le service.	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 du gestionnaire de serveur

Nom des fichiers	Remarques	Trouvé sur
/var/local/log/servermanager.log	Fichier journal pour l'application Gestionnaire de serveur exécutée sur le serveur.	Tous les nœuds
/var/local/log/GridstatBackend.errlog	Fichier journal pour l'application backend de l'interface graphique du gestionnaire de serveur.	Tous les nœuds
/var/local/log/gridstat.errlog	Fichier journal pour l'interface graphique du gestionnaire de serveur.	Tous les nœuds

Journaux des services StorageGRID

Nom des fichiers	Remarques	Trouvé sur
/var/local/log/acct.errlog		Nœuds de stockage exécutant le service ADC
/var/local/log/adc.errlog	Contient le flux d'erreur standard (stderr) des services correspondants. Il y a un fichier journal par service. Ces fichiers sont généralement vides, sauf en cas de problèmes 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 sur le magasin de métadonnées (base de données Cassandra) qui peuvent être utilisées si des problèmes surviennent lors de l'ajout de nouveaux nœuds de stockage ou si la tâche de réparation de nodetool se bloque.	Nœuds de stockage
/var/local/log/cassandra-reaper.log	Informations sur le service Cassandra Reaper, qui effectue des réparations des données dans 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 des fichiers	Remarques	Trouvé sur
/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/dynip*	Contient les journaux liés au service dynip, qui surveille la grille pour les changements IP dynamiques et met à jour la configuration locale.	Tous les nœuds
/var/local/log/grafana.log	Le journal associé au service Grafana, qui est utilisé pour la visualisation des métriques dans le gestionnaire de grille.	Nœuds d'administration
/var/local/log/hagroups.log	Le journal associé aux groupes de 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 BACKUP à MASTER ou FAULT.	Nœuds d'administration et nœuds de passerelle
/var/local/log/idnt.errlog		Nœuds de stockage exécutant le service ADC
/var/local/log/jaeger.log	Le 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 le"S3 Sélectionnez les exigences et les limitations pour les nœuds d'administration et de passerelle" .

Nom des fichiers	Remarques	Trouvé sur
/var/local/log/ldr.errlog		Nœuds de stockage
/var/local/log/miscd/*.log	Contient les journaux du service MISCd (Information Service Control Daemon), qui fournit une interface pour interroger et gérer les services sur d'autres nœuds et pour gérer les configurations environnementales sur le nœud, telles que l'interrogation de l'état des services exécutés sur d'autres nœuds.	Tous les nœuds
/var/local/log/nginx/*.log	Contient les journaux du service nginx, qui agit comme un mécanisme d'authentification et de communication sécurisé pour divers services de grille (tels que Prometheus et Dynip) pour pouvoir communiquer avec des services sur d'autres nœuds via des API HTTPS.	Tous les nœuds
/var/local/log/nginx-gw/*.log	Contient les journaux généraux liés 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 les journaux d'accès liés au trafic de réplication inter-grille.	Nœuds d'administration, nœuds de passerelle ou les deux, en fonction de la configuration de la fédération de grille. Trouvé uniquement sur la grille de destination pour la réplication inter-grille.
/var/local/log/nginx-gw/endpoint-access.log.gz	Contient les journaux d'accès pour le service Load Balancer, qui fournit l'équilibrage de la charge du trafic S3 des clients vers les nœuds de stockage.	Nœuds d'administration et nœuds de passerelle
/var/local/log/persistence*	Contient les journaux du service de persistance, qui gère les fichiers sur le disque racine qui doivent persister après un redémarrage.	Tous les nœuds

Nom des fichiers	Remarques	Trouvé sur
/var/local/log/prometheus.log	Pour tous les nœuds, contient le journal du service d'exportation de nœuds et le journal du service de métriques d'exportation de nœuds. Pour les nœuds d'administration, contient également les journaux des services Prometheus et Alert Manager.	Tous les nœuds
/var/local/log/raft.log	Contient la sortie de la bibliothèque utilisée par le service RSM pour le protocole Raft.	Nœuds de stockage avec service RSM
/var/local/log/rms.errlog	Contient les journaux du service Replicated State Machine Service (RSM), qui est utilisé pour les services de la plate-forme S3.	Nœuds de stockage avec service RSM
/var/local/log/ssm.errlog		Tous les nœuds
/var/local/log/update-s3vs-domains.log	Contient les journaux liés au traitement des mises à jour pour la configuration des noms de domaine hébergés virtuels S3. Consultez les instructions pour implémenter les applications clientes S3.	Nœuds d'administration et de passerelle
/var/local/log/mise à jour-pare-feu-snmp.*	Contient les journaux liés aux ports de pare-feu gérés pour SNMP.	Tous les nœuds
/var/local/log/update-sysl.log	Contient les journaux liés aux modifications apportées à la configuration syslog du système.	Tous les nœuds
/var/local/log/update-traffic-classes.log	Contient les journaux liés aux modifications apportées à la configuration des classificateurs de trafic.	Nœuds d'administration et de passerelle
/var/local/log/update-utcn.log	Contient les journaux liés au mode réseau client non approuvé sur ce nœud.	Tous les nœuds

Informations connexes

- "À propos du bycast.log"
- "Utiliser 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 des fichiers	Remarques	Trouvé sur
/var/local/log/install.log	Créé lors de l'installation du logiciel. Contient un enregistrement des événements d'installation.	Tous les nœuds
/var/local/log/expansion-progress.log	Créé lors d'opérations d'agrandissement. Contient un enregistrement des événements d'extension.	Nœuds de stockage
/var/local/log/pa-move.log	Créé lors de l'exécution du `pa-move.sh` scénario.	Nœud d'administration principal
/var/local/log/pa-move-new_pa.log	Créé lors de l'exécution du `pa-move.sh` scénario.	Nœud d'administration principal
/var/local/log/pa-move-old_pa.log	Créé lors de l'exécution du `pa-move.sh` scénario.	Nœud d'administration principal
/var/local/log/gdu-server.log	Créé par le service GDU. Contient les événements liés aux procédures de provisionnement et de maintenance gérées par le nœud d'administration principal.	Nœud d'administration principal
/var/local/log/send_admin_hw.log	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
/var/local/log/upgrade.log	Créé lors de la mise à niveau du logiciel. Contient un enregistrement des événements de mise à jour du logiciel.	Tous les nœuds

À propos du bycast.log

Le fichier `/var/local/log/bycast.log` est le fichier de dépannage principal pour le logiciel StorageGRID . Il y a un `bycast.log` fichier pour chaque nœud de la 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 de gravité ERREUR et CRITIQUE.

En option, vous pouvez modifier la destination des journaux d'audit et envoyer les informations d'audit à un serveur syslog externe. Les journaux locaux des enregistrements d'audit continuent d'être générés et stockés lorsqu'un serveur syslog externe est configuré. Voir "Configurer les messages d'audit et les destinations des journaux" .

Rotation des fichiers pour bycast.log

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

Le fichier enregistré est renommé `bycast.log.1` , et le nouveau fichier est nommé `bycast.log` . Quand 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` il y a 21 fichiers. Lorsque la 22e version du `bycast.log` le fichier est créé, le fichier le plus ancien est supprimé.

La limite de rotation pour `bycast-err.log` il y a sept fichiers.

> Si un fichier journal a été compressé, vous ne devez pas le décompresser au même emplacement où il a été écrit. La décompression du fichier au même emplacement peut interférer avec les scripts de rotation des journaux.

En option, vous pouvez modifier la destination des journaux d'audit et envoyer les informations d'audit à un serveur syslog externe. Les journaux locaux des enregistrements d'audit continuent d'être générés et stockés lorsqu'un serveur syslog externe est configuré. Voir "Configurer les messages d'audit et les destinations des journaux" .

Informations connexes

"Collecter les fichiers journaux et les données système"

Messages dans bycast.log

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 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
Nœud ID	12455685
ID du processus ADE	0357819531
Nom du module	SVMR
Identifiant du message	Véhicule électrique à évacuation sanitaire (VEHR)

Segment de message	Valeur dans l'exemple
Heure système UTC	2019-05-05T27T17:10:29.784677 (AAAA-MM-JJTHH:MM:SS.uuuuuu)
Niveau de gravité	ERREUR
Numéro de suivi interne	0906
Message	SVMR : Le contrôle de santé du volume 3 a échoué pour la raison « TOUT »

Gravités des messages dans bycast.log

Les messages dans `bycast.log` Des niveaux de gravité sont attribués.

Par exemple:

- **AVIS** — Un événement qui devrait être enregistré s'est produit. La plupart des messages de journal sont à ce niveau.
- **AVERTISSEMENT** — Une condition inattendue s'est produite.
- **ERREUR** — Une erreur majeure s'est produite et aura un impact sur les opérations.
- **CRITIQUE** — Une condition anormale s'est produite, ce qui a interrompu les opérations normales. Vous devez traiter immédiatement le problème sous-jacent.

Codes d'erreur dans `bycast.log`

La plupart des messages d'erreur dans `bycast.log` contenir des codes d'erreur.

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

Code d'erreur	Signification
SUCS	Aucune erreur
GERR	Inconnu
CANC	Annulé
ABRT	Avorté
TOUT	Temps mort
INVL	Invalide
NFND	Non trouvé

Code d’erreur	Signification
VERS	Version
CONF	Configuration
ÉCHOUER	Échec
ICPL	Incomplet
FAIT	Fait
SUNV	Service non disponible

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

Numéro d’erreur	Code d’erreur	Signification
001	EPERM	Opération non autorisée
002	ENOENT	Aucun fichier ou répertoire de ce nom
003	ESCRCH	Aucun processus de ce type
004	EINTR	Appel système interrompu
005	EIO	Erreur d’E/S
006	ENXIO	Aucun appareil ou adresse de ce type
007	E2BIG	Liste d’arguments trop longue
008	ENOEXEC	Erreur de format d’exécution
009	EBADF	Numéro de fichier incorrect
010	ECHILD	Aucun processus enfant
011	ENCORE	Essayer à nouveau
012	ÉNOMÈME	Mémoire insuffisante
013	EACCES	Permission refusée

Numéro d'erreur	Code d'erreur	Signification
014	DÉFAUT	Mauvaise adresse
015	ENOTBLK	Dispositif de blocage requis
016	OCCUPÉ	Appareil ou ressource occupé
017	EEXIST	Le fichier existe
018	EXDEV	Lien entre appareils
019	ENODEV	Aucun appareil de ce type
020	ENOTDIR	Pas un répertoire
021	EISDIR	C'est un répertoire
022	EINVAL	Argument invalide
023	ENFILE	Dépassement de capacité de la table de fichiers
024	E-FILE	Trop de fichiers ouverts
025	ÉNORME	Pas une machine à écrire
026	ETXTBSY	Fichier texte occupé
027	EFBIG	Fichier trop volumineux
028	ENOSPC	Plus d'espace disponible sur l'appareil
029	ESPIPE	Recherche illégale
030	EROFS	Système de fichiers en lecture seule
031	EMLINK	Trop de liens
032	ÉPIPE	Tuyau cassé
033	EDOM	Argument mathématique hors du domaine de la fonction
034	ÉRANGE	Résultat mathématique non représentable

Numéro d'erreur	Code d'erreur	Signification
035	EDEADLK	Une impasse sur les ressources se produirait
036	ÉMAILONG	Nom de fichier trop long
037	ENOLCK	Aucun verrou d'enregistrement disponible
038	ENOSYS	Fonction non implémentée
039	ÉNOTEMPTÉ	Le répertoire n'est pas vide
040	BOUCLE	Trop de liens symboliques rencontrés
041		
042	ENOMSG	Aucun message du type souhaité
043	EIDRM	Identifiant supprimé
044	ECHRNG	Numéro de chaîne hors plage
045	EL2NSYNC	Niveau 2 non synchronisé
046	EL3HLT	Niveau 3 arrêté
047	EL3RST	Réinitialisation de niveau 3
048	ELNRNG	Numéro de lien hors limites
049	EUNATCH	Pilote de protocole non connecté
050	ENOCSI	Aucune structure CSI disponible
051	EL2HLT	Niveau 2 arrêté
052	EBADE	Échange invalide
053	EBADR	Descripteur de demande non valide
054	EXCOMPLET	Échange complet
055	ENOANO	Pas d'anode

Numéro d'erreur	Code d'erreur	Signification
056	EBADRQC	Code de demande invalide
057	EBADSLT	Emplacement invalide
058		
059	EBFONT	Mauvais format de fichier de police
060	ENOSTR	L'appareil n'est pas un flux
061	ENODATA	Aucune donnée disponible
062	ETIME	Le temps a expiré
063	ENOSR	Ressources hors flux
064	ENONET	La machine n'est pas sur le réseau
065	ENOPKG	Paquet non installé
066	EREMOTE	L'objet est distant
067	ENOLINK	Le lien a été rompu
068	EADV	Erreur de publicité
069	ESRMNT	Erreur de montage système
070	ECOMM	Erreur de communication lors de l'envoi
071	ÉPROTO	Erreur de protocole
072	ÉMULTIHOP	Tentative de saut multiple
073	EDOTDOT	Erreur spécifique RFS
074	EBADMSG	Pas un message de données
075	DÉBORDEMENT	Valeur trop grande pour le type de données défini
076	ENOTUNIQ	Le nom n'est pas unique sur le réseau

Numéro d'erreur	Code d'erreur	Signification
077	EBADFD	Descripteur de fichier en mauvais état
078	EREMCHG	Adresse distante modifiée
079	ELIBACC	Impossible d'accéder à une bibliothèque partagée nécessaire
080	ÉLIBBAD	Accéder à une bibliothèque partagée corrompue
081	ELIBSCN	
082	ELIBMAX	Tentative de liaison dans trop de bibliothèques partagées
083	ÉLIBEXEC	Impossible d'exécuter directement une bibliothèque partagée
084	EILSEQ	Séquence d'octets illégale
085	ERESTART	L'appel système interrompu doit être redémarré
086	ESTRPIPE	Erreur de tuyau de flux
087	UTILISATEURS	Trop d'utilisateurs
088	ENOTSOCK	Fonctionnement d'un socket sur un non-socket
089	EDESTADDRREQ	Adresse de destination requise
090	TAILLE EMSGS	Message trop long
091	ÉPROTOTYPE	Protocole de type incorrect pour le socket
092	ÉNOPROTOOPTE	Protocole non disponible
093	EPROTONOSUPPORT	Protocole non pris en charge
094	ESOCKTNOSUPPORT	Type de socket non pris en charge
095	EOPNOTSUPP	Opération non prise en charge sur le point de terminaison de transport
096	SOUTIEN EPFNOS	Famille de protocoles non prise en charge

Numéro d'erreur	Code d'erreur	Signification
097	SOUTIEN EAFNOS	Famille d'adresses non prise en charge par le protocole
098	UTILISATION D'EADDRIN	Adresse déjà utilisée
099	EADDRNOTAVIL	Impossible d'attribuer l'adresse demandée
100	ENETDOWN	Le réseau est en panne
101	ENETUNREACH	Le réseau est inaccessible
102	ENETRESET	La connexion réseau a été interrompue en raison d'une réinitialisation
103	ÉCONNABORTÉ	Le logiciel a provoqué l'interruption de la connexion
104	RÉINITIALISATION ÉCONOMIQUE	Réinitialisation de la connexion par l'homologue
105	ÉNOBUFS	Aucun espace tampon disponible
106	EISCONN	Le point de terminaison de transport est déjà connecté
107	ENOTCONN	Le point de terminaison de transport n'est pas connecté
108	FERMETURE	Impossible d'envoyer après l'arrêt du point de terminaison de transport
109	ETOOOMANYREFS	Trop de références : impossible de les raccorder
110	ETIMEDOUT	La connexion a expiré
111	ÉCONFREINÉ	Connexion rejetée
112	EHOSTDOWN	L'hôte est en panne
113	EHOSTUNREACH	Aucune route vers l'hôte
114	DÉJÀ	Opération déjà en cours
115	PROGRÈS	Opération en cours

Numéro d'erreur	Code d'erreur	Signification
116		
117	EUCLEAN	La structure a besoin d'être nettoyée
118	ENOTNAM	Pas un fichier de type nommé XENIX
119	ENAVAI	Aucun sémaphore XENIX disponible
120	EISNAM	Est un fichier de type nommé
121	EREMOTEIO	Erreur d'E/S à distance
122	EDQUOT	Quota dépassé
123	ÉNOMÉDIUM	Aucun support trouvé
124	TYPE MOYEN	Mauvais type de support
125	ÉANNULÉ	Opération annulée
126	ENOKEY	Clé requise non disponible
127	EKEY EXPIRÉ	La clé a expiré
128	EKEYREVOKED	La clé a été révoquée
129	EKEYREJECTED	La clé a été rejetée par le service
130	PROPRIÉTAIRE MORT	Pour les mutex robustes : le propriétaire est décédé
131	NON RÉCUPÉRABLE	Pour les mutex 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 extérieur à StorageGRID que vous pouvez utiliser pour collecter des informations d'audit système dans un seul emplacement. 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 du paquet de messages syslog sortant est conforme à la RFC 3164.

Les types d'informations d'audit que vous pouvez envoyer au serveur syslog externe incluent :

- 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 les escalades vers la racine
- Journaux d'application qui pourraient être demandés s'il est nécessaire d'ouvrir un dossier d'assistance pour résoudre un problème que vous avez 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'application et les événements de sécurité.
- Réduisez le trafic réseau sur vos nœuds d'administration, car les informations d'audit sont transférées directement des différents nœuds de stockage vers le serveur syslog externe, sans avoir à 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 courantes dans les implémentations de serveur syslog externe.

> Pour maximiser les options de récupération 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 maintenus sur chaque nœud.

Comment configurer un serveur syslog externe

Pour savoir comment configurer un serveur syslog externe, consultez"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 CA du serveur** : un ou plusieurs certificats CA approuvés pour vérifier le serveur syslog externe dans le codage PEM. Si omis, le certificat Grid CA par défaut sera utilisé.
- **Certificat client** : Le certificat client pour l'authentification auprès du serveur syslog externe en codage PEM.
- **Clé privée client** : Clé privée pour le certificat client en 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 secrète. L'utilisation d'une clé privée chiffrée ne présente aucun avantage significatif en termes de sécurité, car la clé et la phrase secrète doivent être stockées. L'utilisation d'une clé privée non chiffrée, si disponible, est recommandée pour plus de simplicité.

Comment estimer la taille du serveur syslog externe

Normalement, votre grille est dimensionnée pour atteindre un débit requis, défini en termes d'opérations S3

par seconde ou d'octets par seconde. Par exemple, vous pouvez avoir besoin que votre grille gère 1 000 opérations S3 par seconde, ou 2 000 Mo par seconde, d'ingestions et de récupérations d'objets. Vous devez dimensionner votre serveur syslog externe en fonction des besoins en données de votre grille.

Cette section fournit quelques formules heuristiques qui vous aident à estimer le taux et la taille moyenne des messages de journal de différents types que votre serveur syslog externe doit être capable de gérer, exprimés en termes de caractéristiques de performances connues ou souhaitées de la grille (opérations S3 par seconde).

Utiliser S3 opérations 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 pour utiliser les formules d'estimation. Pour convertir le débit de la grille, vous devez d'abord déterminer la taille moyenne de votre objet, ce que vous pouvez faire en utilisant les informations des journaux d'audit et des mesures existants (le cas échéant), ou en utilisant vos connaissances des applications qui utiliseront StorageGRID. Par exemple, si votre grille a été dimensionnée pour atteindre un débit de 2 000 Mo/seconde et que la taille moyenne de votre objet est de 2 Mo, alors votre grille a été dimensionnée pour pouvoir gérer 1 000 opérations S3 par seconde (2 000 Mo / 2 Mo).

> Les formules de dimensionnement du serveur syslog externe dans les sections suivantes fournissent des estimations de cas courants (plutôt que des estimations de cas les plus défavorables). Selon votre configuration et votre charge de travail, vous pouvez constater un taux de messages syslog ou un volume de données syslog supérieur ou inférieur à celui prévu par les formules. Les formules sont destinées à être utilisées uniquement à titre indicatif.

Formules d'estimation pour les journaux d'audit

Si vous ne disposez d'aucune information sur votre charge de travail S3 autre que le nombre d'opérations S3 par seconde que votre grille est censée prendre en charge, vous pouvez estimer le volume de journaux d'audit que votre serveur syslog externe devra gérer à l'aide des formules suivantes, en supposant que vous laissiez les niveaux d'audit définis sur les valeurs par défaut (toutes les catégories définies sur Normal, à l'exception du stockage, qui est défini sur Erreur) :

```
Audit Log Rate = 2 x S3 Operations Rate
Audit Log Average Size = 800 bytes
```

Par exemple, si votre grille est dimensionnée 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 de stocker) des données de journal d'audit à un débit 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 qui sont des PUT (par rapport aux GETS) et la taille moyenne, en octets, des champs S3 suivants (les abréviations à 4 caractères utilisées dans le tableau sont les noms des champs du journal d'audit) :

Code	Champ	Description
SACC	Nom du compte locataire S3 (expéditeur de la demande)	Le nom du compte locataire de l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SBAC	Nom du compte locataire S3 (propriétaire du bucket)	Le nom du compte locataire pour le propriétaire du bucket. Utilisé pour identifier l'accès inter-comptes ou anonyme.
S3BK	Godet S3	Le nom du bucket S3.
S3KY	touche S3	Le nom de la clé S3, sans inclure le nom du bucket. Les opérations sur les buckets n'incluent pas ce champ.

Utilisons P pour représenter le pourcentage d'opérations S3 qui sont des PUT, où 0 ≤ P ≤ 1 (donc 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 de compte S3, du bucket S3 et de la clé S3. Supposons que le nom du compte S3 soit toujours my-s3-account (13 octets), que les buckets aient des noms de longueur fixe comme /my/application/bucket-12345 (28 octets) et que les objets aient des clés de longueur fixe comme 5733a5d7-f069-41ef-8fbd-13247494c69c (36 octets). La valeur de K est alors 90 (13+13+28+36).

Si vous pouvez déterminer les valeurs de P et K, vous pouvez estimer le volume de journaux d'audit que votre serveur syslog externe devra gérer à l'aide des formules suivantes, en supposant que vous laissez les niveaux d'audit définis sur les valeurs par défaut (toutes les catégories définies sur Normal, à l'exception du stockage, qui est défini sur Erreur) :

```
Audit Log Rate = ((2 x P) + (1 - P)) x S3 Operations Rate
Audit Log Average Size = (570 + K) bytes
```

Par exemple, si votre grille est dimensionnée pour 1 000 opérations S3 par seconde, que votre charge de travail est composée à 50 % de PUT et que vos noms de compte S3, noms de bucket et noms d'objet font en moyenne 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 de stocker) des données de journal d'audit à un débit 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 de niveau d'audit par défaut (toutes les catégories définies sur Normal, à l'exception de Stockage, qui est défini sur Erreur). Les formules détaillées permettant d'estimer le taux et la taille moyenne des messages d'audit pour les paramètres de niveau d'audit non par défaut ne sont pas disponibles. Cependant, 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 est susceptible d'entraîner une surestimation car les messages d'audit «

supplémentaires » sont, en moyenne, plus petits que les messages d'audit par défaut.

Condition	Formule
Réplication : tous les niveaux d'audit sont définis sur Débogage ou Normal	Taux de journal d'audit = 8 x taux d'opérations S3
Codage d'effacement : niveaux d'audit tous définis sur Débogage ou Normal	Utiliser la même formule que pour les paramètres par défaut

Formules d'estimation des événements de sécurité

Les événements de sécurité ne sont pas corrélés aux 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 sur votre charge de travail S3 autre que le nombre d'opérations S3 par seconde que votre grille est censée prendre en charge, vous pouvez estimer le volume de 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
```

Ainsi, par exemple, si votre grille est dimensionnée 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) des données de journal d'application à un débit d'environ 1,2 Mo par seconde.

Si vous en savez plus sur votre charge de travail, des estimations plus précises sont possibles. Pour les journaux d'application, les variables supplémentaires les plus importantes sont la stratégie de protection des données (réplication ou codage d'effacement), le pourcentage d'opérations S3 qui sont des PUT (par rapport aux GET/autres) et la taille moyenne, en octets, des champs S3 suivants (les abréviations à 4 caractères utilisées dans le tableau sont les noms des champs du journal d'audit) :

Code	Champ	Description
SACC	Nom du compte locataire S3 (expéditeur de la demande)	Le nom du compte locataire de l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SBAC	Nom du compte locataire S3 (propriétaire du bucket)	Le nom du compte locataire pour le propriétaire du bucket. Utilisé pour identifier l'accès inter-comptes ou anonyme.
S3BK	Godet S3	Le nom du bucket S3.

Code	Champ	Description
S3KY	touche S3	Le nom de la clé S3, sans inclure le nom du bucket. Les opérations sur les buckets n'incluent pas ce champ.

Exemples d'estimations de dimensionnement

Cette section explique des exemples de cas d'utilisation des formules d'estimation pour les grilles avec les méthodes de protection des données suivantes :

- Réplication
- Codage d'effacement

Si vous utilisez la réplication pour la protection des données

Soit P représente le pourcentage d'opérations S3 qui sont des PUT, où 0 ≤ P ≤ 1 (donc pour une charge de travail PUT de 100 %, P = 1, et pour une charge de travail GET de 100 %, P = 0).

Laissez K représenter la taille moyenne de la somme des noms de compte S3, du bucket S3 et de la clé S3. Supposons que le nom du compte S3 soit toujours my-s3-account (13 octets), que les buckets aient des noms de longueur fixe comme /my/application/bucket-12345 (28 octets) et que les objets aient des clés de longueur fixe comme 5733a5d7-f069-41ef-8fbd-13247494c69c (36 octets). Alors K a une valeur de 90 (13+13+28+36).

Si vous pouvez déterminer les valeurs de P et K, vous pouvez estimer le volume de journaux d'application que votre serveur syslog externe devra être capable de gérer 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
```

Ainsi, par exemple, si votre grille est dimensionnée pour 1 000 opérations S3 par seconde, que votre charge de travail est composée à 50 % de PUT et que vos noms de compte S3, noms de bucket et noms d'objet font en moyenne 90 octets, votre serveur syslog externe doit être dimensionné pour prendre en charge 1 800 journaux d'application par seconde et recevra (et stockera généralement) les données d'application à un débit de 0,5 Mo par seconde.

Si vous utilisez le codage d'effacement pour la protection des données

Soit P représente le pourcentage d'opérations S3 qui sont des PUT, où 0 ≤ P ≤ 1 (donc pour une charge de travail PUT de 100 %, P = 1, et pour une charge de travail GET de 100 %, P = 0).

Laissez K représenter la taille moyenne de la somme des noms de compte S3, du bucket S3 et de la clé S3. Supposons que le nom du compte S3 soit toujours my-s3-account (13 octets), que les buckets aient des noms de longueur fixe comme /my/application/bucket-12345 (28 octets) et que les objets aient des clés de longueur fixe comme 5733a5d7-f069-41ef-8fbd-13247494c69c (36 octets). Alors K a une valeur de 90 (13+13+28+36).

Si vous pouvez déterminer les valeurs de P et K, vous pouvez estimer le volume de journaux d'application que votre serveur syslog externe devra être capable de gérer 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
```

Ainsi, par exemple, si votre grille est dimensionnée pour 1 000 opérations S3 par seconde, que votre charge de travail est composée à 50 % de PUT et que vos noms de compte S3, noms de bucket et noms d'objet font en moyenne 90 octets, votre serveur syslog externe doit être dimensionné pour prendre en charge 2 250 journaux d'application par seconde et doit être capable de recevoir (et généralement de stocker) des données d'application à un débit 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 du client ; configurer un serveur Syslog externe ; et spécifier où les journaux d'audit, les journaux d'événements de sécurité et les journaux du logiciel StorageGRID sont envoyés.

Les messages et journaux d'audit enregistrent les activités du système et les événements de sécurité et constituent des outils essentiels pour la surveillance et le dépannage. Tous les nœuds StorageGRID génèrent des messages d'audit et des journaux pour suivre l'activité et les événements du système.

En option, vous pouvez configurer un serveur syslog externe pour enregistrer les informations d'audit à distance. L'utilisation d'un serveur externe minimise 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 Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"Autorisation d'accès de maintenance ou root" .
- Si vous envisagez de configurer un serveur syslog externe, vous avez examiné le"considérations relatives à l'utilisation d'un serveur syslog externe" et s'assurer 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 de l'autorité de certification du serveur et des certificats client requis, ainsi que de la clé privée du 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 d'audit	Paramètre par défaut	Plus d'informations
Système	Normal	"Messages d'audit du système"

Catégorie d'audit	Paramètre par défaut	Plus d'informations
Stockage	Erreur	"Messages d'audit du stockage d'objets"
Gestion	Normal	"Message d'audit de gestion"
Le client lit	Normal	"Le client lit les messages d'audit"
Le client écrit	Normal	"Le client écrit des messages d'audit"
ILM	Normal	"Messages d'audit ILM"
Réplication inter-réseaux	Erreur	"CGRR : demande de réplication inter-réseau"

Ces valeurs par défaut s'appliquent si vous avez initialement installé StorageGRID 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 définie sur Normal.

Lors des mises à niveau, les configurations de niveau 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
Désactivé	Aucun message d'audit de la catégorie n'est enregistré.
Erreur	Seuls les messages d'erreur sont enregistrés : les messages d'audit pour lesquels le code de résultat n'était pas « réussi » (SUCS).
Normal	Les messages transactionnels standard sont enregistrés : les messages répertoriés dans ces instructions pour la catégorie.
Déboguer	Obsolète. Ce niveau se comporte de la même manière que le niveau d'audit Normal.

Les messages inclus pour un niveau particulier incluent ceux qui seraient enregistrés 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 client pour vos applications S3, vous pouvez éventuellement modifier le paramètre **Lectures client** sur **Erreur** pour réduire 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.

Définir 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 du 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 correspondre à zéro ou 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 demande du protocole d'audit sont enregistrés uniquement si le niveau d'audit pour **Lectures client** ou **Écritures client** n'est pas **Désactivé**.

3. Sélectionnez **Enregistrer**

   Une bannière verte indique que votre configuration a été enregistrée.

Utiliser un serveur syslog externe

Vous pouvez éventuellement 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 extérieur à votre grille.

> Si vous ne souhaitez pas utiliser un serveur syslog externe, ignorez cette étape et accédez àSélectionner 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 de la `audit-destinations` points de terminaison, qui se trouvent dans la section API privée du"API de gestion de grille" . 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 de configuration du serveur Syslog externe et fournissez les informations dont StorageGRID a besoin pour accéder au serveur Syslog externe.

Étapes

1. Depuis la page Serveur d'audit et syslog, sélectionnez **Configurer un serveur syslog externe**. Ou, si vous avez déjà configuré un serveur syslog externe, sélectionnez **Modifier le serveur syslog externe**.

L'assistant de configuration du serveur syslog externe s'affiche.

2. Pour l'étape **Saisir les informations syslog** de l'assistant, saisissez un nom de domaine complet valide ou une adresse IPv4 ou IPv6 pour le serveur syslog externe dans le champ **Hôte**.
3. Saisissez 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.

   L'utilisation de **TLS** ou **RELP/TLS** est recommandée. 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, consultez la section "Gérer les certificats de sécurité" .

   Toutes les options de protocole nécessitent la prise en charge et la configuration du serveur syslog externe. Vous devez choisir une option compatible avec le serveur syslog externe.

   > Le protocole de journalisation des événements fiable (RELP) étend les fonctionnalités du protocole Syslog pour fournir une livraison fiable des messages d'événements. 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 d'autorité de certification du serveur, le certificat 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 clé.
   c. Sélectionnez **Ouvrir** pour télécharger le fichier.

      Une coche verte apparaît à côté du nom du certificat ou du fichier de clé, vous informant qu'il a été téléchargé avec succès.

7. Sélectionnez **Continuer**.

Gérer le contenu du syslog

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 que lorsqu'un utilisateur non autorisé tente de se connecter ou lorsqu'un utilisateur se connecte en tant que root
   - **Envoyer les journaux d'application** : Envoie"Fichiers journaux du logiciel StorageGRID" utile 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, aux points de terminaison d'équilibrage de charge configurés et aux demandes de fédération de grille à partir de systèmes distants.

2. Utilisez les menus déroulants pour sélectionner la gravité et la facilité (type de message) pour chaque catégorie d'informations d'audit que vous souhaitez envoyer.

   La définition des valeurs de gravité et d'installation peut vous aider à regrouper les journaux de manière personnalisable pour une analyse plus facile.

   a. Pour **Gravité**, sélectionnez **Passthrough** 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 gravités seront perdues si vous remplacez la gravité par une valeur fixe.

Gravité	Description
Passage	Chaque message envoyé au syslog externe doit avoir la même valeur de gravité que lorsqu'il a été enregistré localement sur le nœud : • Pour les journaux d'audit, la gravité est « info ». • Pour les événements de sécurité, les valeurs de gravité sont générées par la distribution Linux sur les nœuds. • 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 une valeur « info », tandis que l'arrêt intentionnel du service SSM ou RSM donne une valeur « notice ». • Pour les journaux d'accès, la gravité est « info ».
0	Urgence : le système est inutilisable
1	Alerte : des mesures doivent être prises immédiatement
2	Critique : Conditions critiques
3	Erreur : conditions d'erreur
4	Avertissement : Conditions d'avertissement
5	Avis : État normal mais significatif
6	Informationnel : Messages d'information

Gravité	Description
7	Débogage : messages de niveau débogage

b. Pour **Facilty**, 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 sur les différentes installations seront perdues si vous remplacez l'installation par une valeur fixe.

Facilité	Description
Passage	Chaque message envoyé au syslog externe doit avoir la même valeur de fonctionnalité que lorsqu'il a été enregistré localement sur le nœud : • Pour les journaux d'audit, l'installation envoyée au serveur syslog externe est « local7 ». • Pour les événements de sécurité, les valeurs des installations sont générées par la distribution Linux sur les nœuds. • Pour les journaux d'application, les journaux d'application envoyés au serveur syslog externe ont les valeurs de fonctionnalité suivantes : ◦ `bycast.log`: utilisateur ou démon ◦ `bycast-err.log`: utilisateur, démon, local3 ou local4 ◦ `jaeger.log`: local2 ◦ `nms.log`: local3 ◦ `prometheus.log`: local4 ◦ `raft.log`: local5 ◦ `hagroups.log`: local6 • Pour les journaux d'accès, l'installation envoyée au serveur syslog externe est « local0 ».
0	kern (messages du noyau)
1	utilisateur (messages au niveau de l'utilisateur)
2	mail
3	démon (démons système)
4	auth (messages de sécurité/autorisation)
5	syslog (messages générés en interne par syslogd)
6	lpr (sous-système d'imprimante en ligne)

Facilité	Description
7	actualités (sous-système d'actualités du réseau)
8	UUCP
9	cron (démon d'horloge)
10	sécurité (messages de sécurité/autorisation)
11	FTP
12	NTP
13	logaudit (audit des journaux)
14	logalert (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. Vous devez utiliser ces messages de test pour vous aider à valider l'ensemble 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 de 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 des messages de test** (recommandé).

   Les résultats des tests apparaissent en continu sur la page jusqu'à ce que vous arrêtiez le test. Pendant que le test est en cours, vos messages d'audit continuent d'être envoyés vers vos destinations précédemment configurées.

3. Si vous recevez des erreurs lors de la configuration du serveur Syslog ou lors de l'exécution, corrigez-les et sélectionnez à nouveau **Envoyer des messages de test**.

   Voir"Dépanner un serveur syslog externe" pour vous aider à résoudre les erreurs.

4. Attendez de voir une bannière verte indiquant que tous les nœuds ont réussi les tests.
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 êtes renvoyé à la page **Serveur d'audit et syslog**. 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 n'avez pas sélectionné une destination incluant le serveur Syslog externe.

Sélectionner les destinations des informations d'audit

Vous pouvez spécifier où se trouvent les journaux d'audit, les journaux d'événements de sécurité et"Journaux du logiciel StorageGRID" sont envoyés.

StorageGRID utilise par défaut les destinations d'audit des nœuds locaux et stocke les informations d'audit dans `/var/local/log/localaudit.log` .

Lors de l'utilisation `/var/local/log/localaudit.log` , les entrées du journal d'audit du Grid Manager et du Tenant Manager peuvent être envoyées à un nœud de stockage. Vous pouvez trouver quel nœud contient les entrées les plus récentes en utilisant le `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** offrent généralement de meilleures performances.

Option	Description
Nœuds locaux uniquement (par défaut)	Les messages d'audit, les journaux d'événements de sécurité et les journaux d'application ne sont pas envoyés aux nœuds d'administration. Au lieu de cela, 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 `/var/local/log/localaudit.log` . **Remarque** : 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 journal sont stockés sur chaque nœud.
Nœuds d'administration/nœuds locaux	Les messages d'audit sont envoyés au journal d'audit sur les nœuds d'administration, et les journaux d'événements de sécurité et les journaux d'application sont stockés sur les nœuds qui les ont générés. Les informations d'audit sont stockées dans les fichiers suivants : • Nœuds d'administration (principaux et non principaux) : `/var/local/audit/export/audit.log` • Tous les nœuds : Le `/var/local/log/localaudit.log` le fichier est généralement vide ou manquant. Il peut contenir des informations secondaires, comme une copie supplémentaire de certains messages.

Option	Description
Serveur syslog externe	Les informations d'audit sont envoyées à un serveur syslog externe et enregistrées sur les nœuds locaux(`/var/local/log/localaudit.log`). Le type d'informations envoyées dépend de la façon dont vous avez configuré le serveur syslog externe. Cette option est activée uniquement après avoir configuré un serveur syslog externe.
Nœud d'administration et serveur syslog externe	Les messages d'audit sont envoyés au journal d'audit(`/var/local/audit/export/audit.log`) sur les nœuds d'administration, et les informations d'audit sont envoyées au serveur syslog externe et enregistrées sur le nœud local(`/var/local/log/localaudit.log`). Le type d'informations envoyées dépend de la façon dont vous avez configuré le serveur syslog externe. Cette option est activée uniquement après avoir configuré un serveur syslog externe.

2. Sélectionnez **Enregistrer**.

   Un message d'avertissement apparaît.

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.

- "Configurer l'agent SNMP"
- "Mettre 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 table et de notification pour les alertes. La MIB contient également des informations de description du système telles que la plate-forme et le numéro de modèle pour chaque nœud. Chaque nœud StorageGRID prend également en charge un sous-ensemble d'objets MIB-II.

Voir"Accéder aux fichiers MIB" si vous souhaitez télécharger les fichiers MIB sur vos nœuds de grille.

Initialement, 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 peut envoyer deux types de notifications basées sur des événements à un système de gestion :

Pièges

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 informer le système de gestion qu’un événement s’est produit dans StorageGRID, comme le déclenchement d’une alerte.

Les interruptions sont prises 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 nouvelle tentative maximale soit 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 n’importe quel 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 le"nœud d’administration de l’expéditeur préféré" .

  Chaque alerte est mappée à l’un des trois types d’interruption en fonction du niveau de gravité de l’alerte : activeMinorAlert, activeMajorAlert et activeCriticalAlert. Pour une liste des alertes qui peuvent déclencher ces pièges, consultez le"Référence des alertes" .

Prise en charge des versions SNMP

Le tableau fournit un résumé de haut niveau de ce qui est pris en charge pour chaque version SNMP.

	SNMPv1	SNMPv2c	SNMPv3
Requêtes (GET et GETNEXT)	Requêtes MIB en lecture seule	Requêtes MIB en lecture seule	Requêtes MIB en lecture seule
Authentification des requêtes	Chaîne communautaire	Chaîne communautaire	Modèle de sécurité basé sur l’utilisateur (USM) utilisateur
Notifications (PIÈGE et INFORME)	Pièges uniquement	Pièges et informations	Pièges et informations

	SNMPv1	SNMPv2c	SNMPv3
Authentification des notifications	Communauté de piège par défaut ou chaîne de communauté personnalisée pour chaque destination de piège	Communauté de piège par défaut ou chaîne de communauté personnalisée pour chaque destination de piège	Utilisateur USM pour chaque destination de trap

Limites

- StorageGRID prend en charge 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 de support de 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.

Configurer l'agent SNMP

Vous pouvez configurer l'agent SNMP StorageGRID pour utiliser un système de gestion SNMP tiers pour l'accès MIB en lecture seule et les notifications.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"Autorisation d'accès root" .

À propos de cette 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 du modèle de sécurité utilisateur (USM) est prise en charge.

Tous les nœuds de la grille utilisent la même configuration SNMP.

Spécifier la configuration de base

Dans un premier temps, activez l'agent SMNP StorageGRID et fournissez des informations de base.

Étapes

1. Sélectionnez **CONFIGURATION** > **Surveillance** > **Agent SNMP**.

   La page de l'agent SNMP apparaît.

2. Pour activer l'agent SNMP sur tous les nœuds de grille, cochez la case **Activer SNMP**.
3. Saisissez 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 sous la forme sysContact. Le contact système est généralement une adresse e-mail. Cette valeur s'applique à tous les nœuds du système StorageGRID . **Contact système** peut contenir jusqu'à 255 caractères.
Emplacement du système	Facultatif. L'emplacement du système StorageGRID , qui est renvoyé dans les messages SNMP sous la forme sysLocation. L'emplacement du système peut être n'importe quelle information utile pour identifier où se trouve votre système StorageGRID . Par exemple, vous pouvez utiliser l'adresse postale d'un établissement. Cette valeur s'applique à tous les nœuds du système StorageGRID . **Emplacement du système** peut contenir jusqu'à 255 caractères.
Activer les notifications de l'agent SNMP	• Si cette option est sélectionnée, l'agent SNMP StorageGRID envoie des notifications d'interruption et d'information. • Si cette option n'est pas sélectionnée, l'agent SNMP prend en charge l'accès MIB en lecture seule, mais il n'envoie aucune notification SNMP.
Activer les pièges d'authentification	Si cette option est sélectionnée, l'agent SNMP StorageGRID envoie des interruptions d'authentification s'il reçoit des messages de protocole mal authentifiés.

Entrez les chaînes de communauté

Si vous utilisez SNMPv1 ou SNMPv2c, complétez la section Chaînes de communauté.

Lorsque le système de gestion interroge le 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 la **Communauté en lecture seule**, saisissez éventuellement 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 « public » comme chaîne de communauté. 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'espacement.

2. Sélectionnez **Ajouter une autre chaîne de communauté** pour ajouter des chaînes supplémentaires.

   Jusqu'à cinq chaînes sont autorisées.

Créer des destinations de pièges

Utilisez l'onglet Destinations d'interruption dans 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. Des notifications standard sont également envoyées pour les entités MIB-II prises en charge (par exemple, ifDown et coldStart).

Étapes

1. Pour le champ **Communauté d'interruption par défaut**, saisissez éventuellement 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 pièges par défaut peut contenir un maximum de 32 caractères et ne peut pas contenir de caractères d'espacement.

2. Pour ajouter une destination de piège, sélectionnez **Créer**.
3. Sélectionnez la version SNMP qui sera utilisée pour cette destination de trap.
4. Remplissez le formulaire Créer une destination de piège pour la version que vous avez sélectionnée.

SNMPv1

Si vous avez sélectionné SNMPv1 comme version, remplissez 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 le piège.
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 trappe SNMP standard, sauf si vous devez utiliser TCP.
Chaîne communautaire	Utilisez la communauté d'interruption par défaut, si elle a été spécifiée, ou entrez une chaîne de communauté personnalisée pour cette destination d'interruption. La chaîne de communauté personnalisée peut comporter au maximum 32 caractères et ne peut pas contenir d'espaces.

SNMPv2c

Si vous avez sélectionné SNMPv2c comme version, remplissez ces champs.

Champ	Description
Type	Si la destination sera utilisée pour les pièges ou les informations.
Hôte	Une adresse IPv4 ou IPv6 ou FQDN pour recevoir le piège.
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 trappe SNMP standard, sauf si vous devez utiliser TCP.
Chaîne communautaire	Utilisez la communauté d'interruption par défaut, si elle a été spécifiée, ou entrez une chaîne de communauté personnalisée pour cette destination d'interruption. La chaîne de communauté personnalisée peut comporter au maximum 32 caractères et ne peut pas contenir d'espaces.

SNMPv3

Si vous avez sélectionné SNMPv3 comme version, remplissez ces champs.

Champ	Description
Type	Si la destination sera utilisée pour les pièges ou les informations.
Hôte	Une adresse IPv4 ou IPv6 ou FQDN pour recevoir le piège.
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 trappe SNMP standard, sauf si vous devez utiliser TCP.
Utilisateur USM	L'utilisateur USM qui sera utilisé pour l'authentification. • Si vous avez sélectionné **Trap**, seuls les utilisateurs USM sans identifiant de moteur faisant autorité sont affichés. • Si vous avez sélectionné **Informer**, seuls les utilisateurs USM avec des ID de moteur faisant autorité sont affichés. • Si aucun utilisateur n'est affiché : i. Créez et enregistrez la destination du piège. ii. Aller àCréer des utilisateurs USM et créer l'utilisateur. iii. Revenez à l'onglet Destinations des pièges, sélectionnez la destination enregistrée dans le tableau et sélectionnez **Modifier**. iv. Sélectionnez l'utilisateur.

5. Sélectionnez **Créer**.

   La destination du piège est créée et ajoutée à la table.

Créer des adresses d'agent

Vous pouvez également utiliser l'onglet Adresses des agents dans 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. Saisissez les informations suivantes.

Champ	Description
Protocole Internet	Si cette adresse utilisera IPv4 ou IPv6. Par défaut, SNMP utilise IPv4.
Protocole de transport	Si cette adresse utilisera UDP ou TCP. Par défaut, SNMP utilise UDP.
Réseau StorageGRID	Sur quel réseau StorageGRID l'agent écoutera. • Réseaux Grid, Admin et Client : l'agent SNMP écoutera les requêtes sur les trois réseaux. • Réseau de grille • Réseau d'administration • Réseau de clients **Remarque** : 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.
Port	En option, le numéro de port sur lequel l'agent SNMP doit écouter. Le port UDP par défaut pour un agent SNMP est 161, mais vous pouvez saisir n'importe quel numéro de port inutilisé. **Remarque** : 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.

Créer des utilisateurs USM

Si vous utilisez SNMPv3, utilisez l'onglet Utilisateurs USM dans 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. La destination SNMPv3 *trap* 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. Saisissez les informations suivantes.

Champ	Description
Nom d’utilisateur	Un nom unique pour cet utilisateur USM. Les noms d’utilisateur peuvent comporter un maximum de 32 caractères et ne peuvent pas contenir de caractères d’espacement. Le nom d’utilisateur ne peut pas être modifié une fois l’utilisateur créé.
Accès MIB en lecture seule	Si cette option est sélectionnée, cet utilisateur doit avoir un accès en lecture seule au MIB.
ID moteur faisant autorité	Si cet utilisateur doit être utilisé dans une destination d’information, l’ID du moteur faisant autorité pour cet utilisateur. Saisissez 10 à 64 caractères hexadécimaux (5 à 32 octets) sans espaces. 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. **Remarque** : ce champ n’est pas affiché si vous avez sélectionné **Accès MIB en lecture seule** car les utilisateurs USM qui ont un accès MIB en lecture seule ne peuvent pas avoir d’ID de moteur.
Niveau de sécurité	Le niveau de sécurité pour l’utilisateur USM : • **authPriv** : Cet utilisateur communique avec authentification et 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. • **authNoPriv** : Cet utilisateur communique avec authentification et sans confidentialité (pas de cryptage). Vous devez spécifier un protocole d’authentification et un mot de passe.
Protocole d’authentification	Toujours défini sur SHA, qui est le seul protocole pris en charge (HMAC-SHA-96).
Mot de passe	Le mot de passe que cet utilisateur utilisera pour l’authentification.
Protocole de confidentialité	Affiché uniquement si vous avez sélectionné **authPriv** et toujours défini sur AES, qui est le seul protocole de confidentialité pris en charge.
Mot de passe	Affiché uniquement si vous avez sélectionné **authPriv**. Le mot de passe que cet utilisateur utilisera pour la confidentialité.

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.

Mettre 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 Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"Autorisation d'accès root" .

À propos de cette tâche

Voir"Configurer l'agent SNMP" pour plus de détails sur chaque champ de la page de l'agent SNMP. Vous devez sélectionner **Enregistrer** au bas de la page pour valider les modifications que vous apportez sur chaque onglet.

Étapes

1. Sélectionnez **CONFIGURATION** > **Surveillance** > **Agent SNMP**.

   La page de l'agent SNMP apparaît.

2. Pour désactiver l'agent SNMP sur tous les nœuds de 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. Vous pouvez également mettre à jour les informations dans la section Configuration de base :
   a. Si nécessaire, mettez à jour le **Contact système** et l'**Emplacement du système**.
   b. Vous pouvez également cocher ou décocher la case **Activer les notifications de l'agent SNMP** pour contrôler si l'agent SNMP StorageGRID envoie des notifications d'interruption et d'information.

      Lorsque cette case à cocher est décochée, l'agent SNMP prend en charge l'accès MIB en lecture seule, mais il n'envoie pas de notifications SNMP.

   c. Vous pouvez également cocher ou décocher 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, mettez à jour ou ajoutez éventuellement 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 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. Des notifications standard sont également envoyées pour les entités MIB-II prises en charge (par exemple,

ifDown et coldStart).

Pour plus de détails sur ce qu'il faut saisir, voir"Créer des destinations de pièges" .

- Vous pouvez également mettre à jour ou supprimer la communauté de pièges par défaut.

  Si vous supprimez la communauté de trap par défaut, vous devez d'abord vous assurer que toutes les destinations de trap existantes utilisent une chaîne de communauté personnalisée.

- Pour ajouter une destination de piège, sélectionnez **Créer**.
- Pour modifier une destination de piège, sélectionnez le bouton radio, puis sélectionnez **Modifier**.
- Pour supprimer une destination de piège, sélectionnez le bouton radio, puis 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 qu'il faut saisir, voir"Créer des adresses d'agent" .

   - Pour ajouter une adresse d'agent, sélectionnez **Créer**.
   - Pour modifier l'adresse d'un agent, sélectionnez le bouton radio, puis 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 le MIB ou à recevoir des interruptions et des informations.

   Pour plus de détails sur ce qu'il faut saisir, voir"Créer des utilisateurs USM" .

   - Pour ajouter un utilisateur USM, sélectionnez **Créer**.
   - Pour modifier un utilisateur USM, sélectionnez le bouton radio, puis 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 supprimer l'utilisateur et en créer un nouveau.

     > Si vous ajoutez ou supprimez l'ID de moteur faisant autorité d'un utilisateur et que cet utilisateur est actuellement sélectionné pour une destination, vous devez modifier ou supprimer la destination. Dans le cas contraire, 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. Dans le cas contraire, 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. Une fois la configuration de l'agent SNMP mise à jour, sélectionnez **Enregistrer**.

Accéder aux fichiers MIB

Les fichiers MIB contiennent des définitions et des informations sur les propriétés des ressources et des 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 surveiller votre réseau.

Voir"Utiliser la surveillance SNMP" pour plus d'informations sur les fichiers SNMP et MIB.

Accéder aux fichiers MIB

Suivez ces étapes pour accéder aux fichiers MIB.

Étapes

1. Sélectionnez **CONFIGURATION** > **Surveillance** > **Agent SNMP**.
2. Sur la page de l'agent SNMP, sélectionnez le fichier que vous souhaitez télécharger :
   - **NETAPP-STORAGEGRID-MIB.txt**: Définit la table d'alerte et les notifications (traps) accessibles sur tous les nœuds d'administration.
   - **ES-NETAPP-06-MIB.mib**: Définit les objets et les notifications pour les appareils basés sur la série E.
   - **MIB_1_10.zip**: Définit les objets et les notifications pour les appliances avec 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. Obtenez l'OID de la racine du 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 l'arbre entier (en utilisant `paste` pour joindre des lignes) :

   ```
   root@user-adm1:~ # snmptranslate -Tso | paste -d " " - - | grep 28669
   ```

> Le `snmptranslate` La commande dispose de nombreuses options utiles pour explorer le MIB. Cette commande est disponible sur n'importe quel nœud StorageGRID .

Contenu du fichier MIB

Tous les objets sont sous l'OID StorageGRID .

Nom de l'objet	ID d'objet (OID)	Description
		Le module MIB pour les entités NetApp StorageGRID .

objets MIB

Nom de l'objet	ID d'objet (OID)	Description
nombre d'alertes actives		Le nombre d'alertes actives dans activeAlertTable.
table d'alertes actives		Un tableau des alertes actives dans StorageGRID.
activeAlertId		L'ID de l'alerte. Unique dans l'ensemble actuel d'alertes actives.
activeAlertName		Le nom de l'alerte.
instance d'alerte active		Le nom de l'entité qui a généré l'alerte, généralement le nom du nœud.
gravité de l'alerte active		La gravité de l'alerte.
heure de début d'alerte active		La date et l'heure auxquelles l'alerte a été déclenchée.

Types de notifications (pièges)

Toutes les notifications incluent les variables suivantes en tant que varbinds :

- activeAlertId
- activeAlertName
- instance d'alerte active
- gravité de l'alerte active
- heure de début d'alerte active

Type de notification	ID d'objet (OID)	Description
alerte mineure active		Une alerte de gravité mineure
alerte majeure active		Une alerte de gravité majeure
alerte critique active		Une alerte de gravité critique

Collecter des données StorageGRID supplémentaires

Utiliser des tableaux et des graphiques

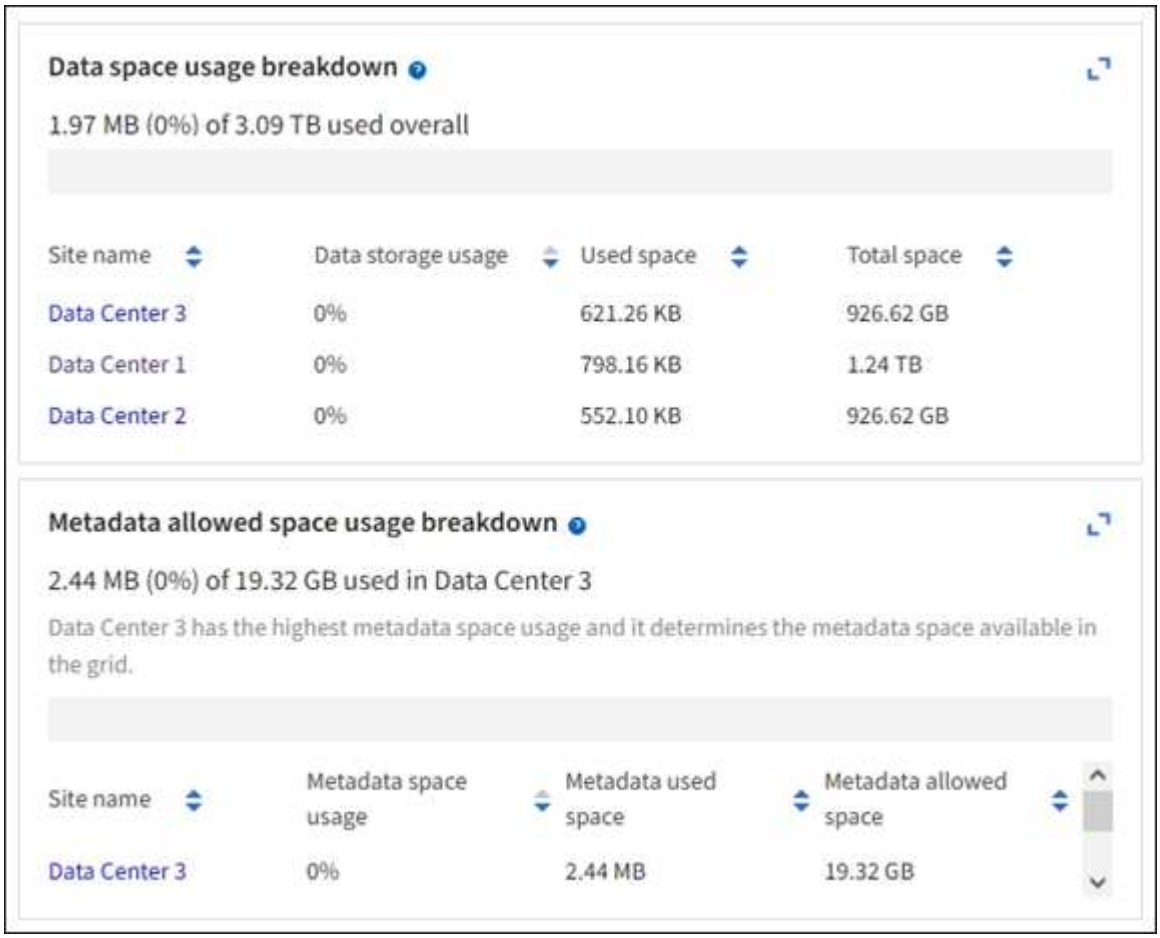
Vous pouvez utiliser des graphiques et des rapports pour surveiller l'état du système StorageGRID et résoudre les problèmes.

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

Types de graphiques

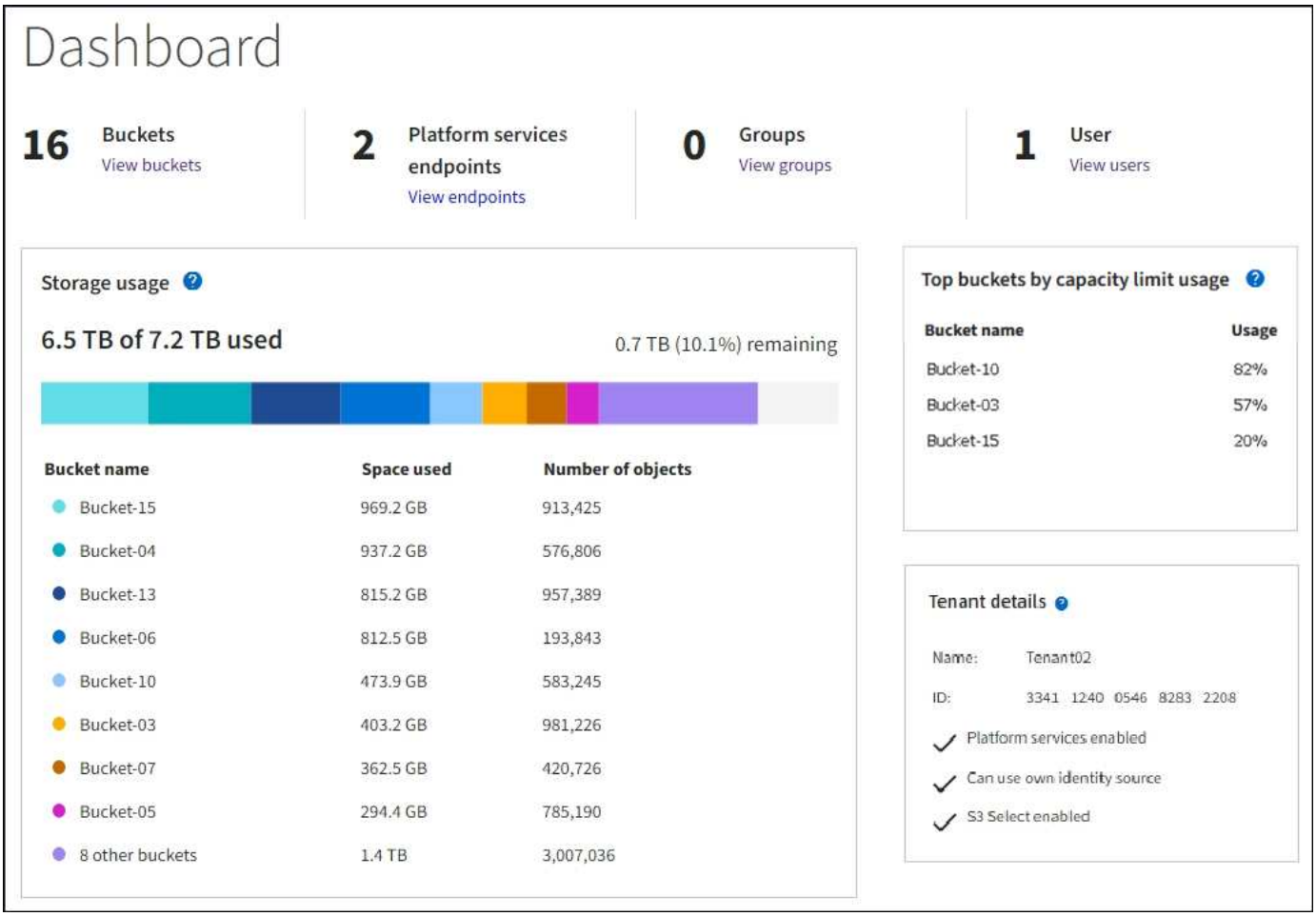
Les graphiques et diagrammes résument les valeurs des métriques et attributs StorageGRID spécifiques.

Le tableau de bord Grid Manager comprend des cartes qui résument le stockage disponible pour la grille et chaque site.



Le panneau d'utilisation du stockage sur le tableau de bord du gestionnaire de locataires affiche les éléments suivants :

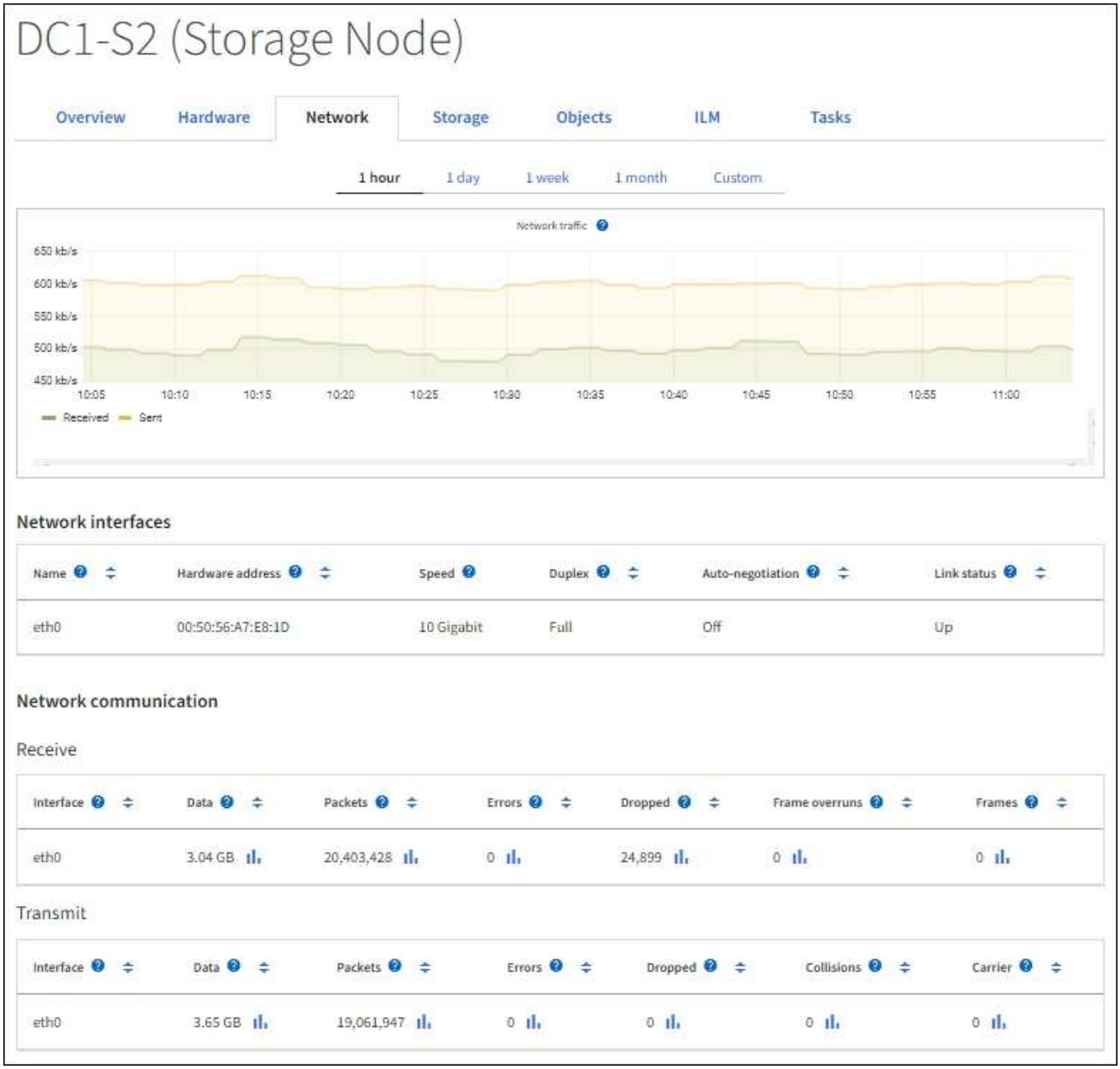
- Une liste des plus grands buckets (S3) ou conteneurs (Swift) pour le locataire
- Un graphique à barres qui représente les tailles relatives des plus grands seaux ou conteneurs
- La quantité totale d'espace utilisé et, si un quota est défini, la quantité et le pourcentage d'espace restant



De plus, des graphiques montrant comment les métriques et les attributs StorageGRID évoluent au fil du temps sont disponibles sur la page Nœuds et sur la page **SUPPORT** > **Outils** > **Topologie de grille**.

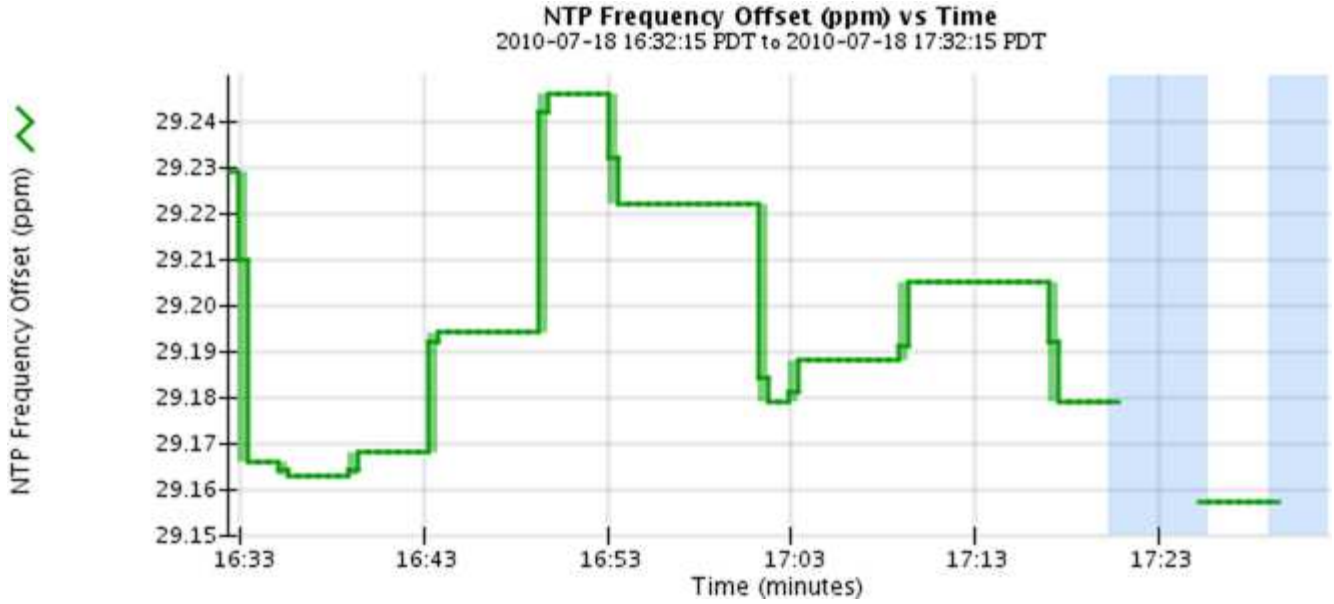
Il existe quatre types de graphiques :

- **Graphiques Grafana** : Affichés sur la page Nœuds, les graphiques Grafana sont utilisés pour tracer les valeurs des métriques Prometheus au fil du temps. Par exemple, l'onglet **NODES** > **Network** pour un nœud de stockage inclut un graphique Grafana pour le trafic réseau.

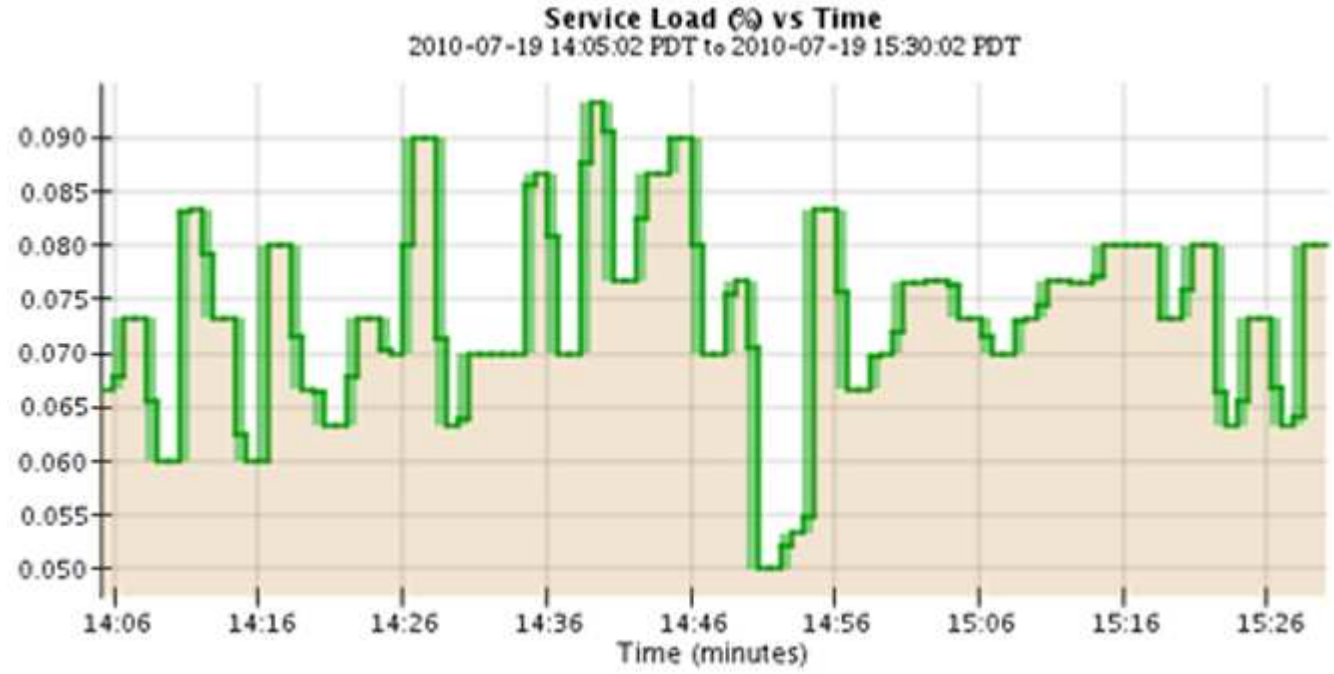


Les graphiques Grafana sont également inclus dans les tableaux de bord pré-construits disponibles sur la page **SUPPORT** > **Outils** > **Métriques**.

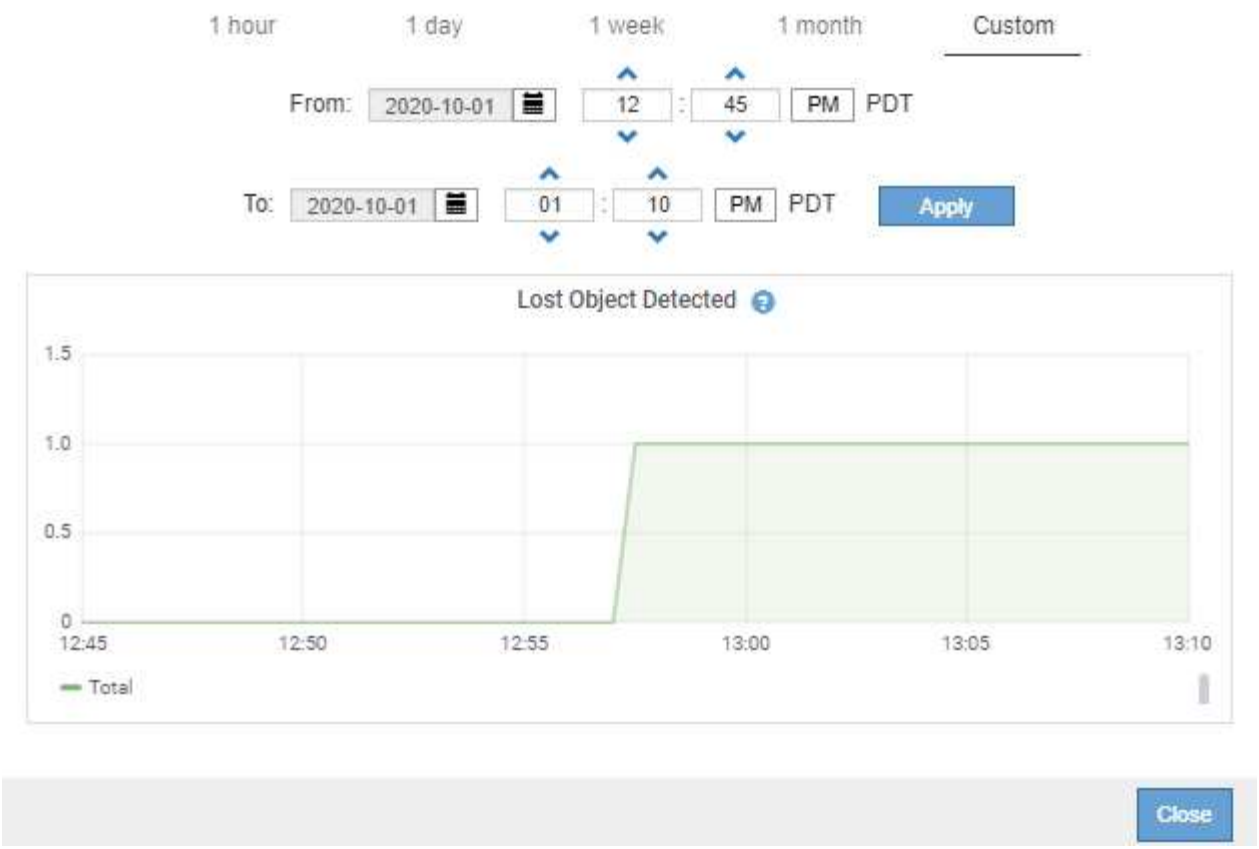
- **Graphiques linéaires** : Disponibles à partir de la page Nœuds et de la page **SUPPORT** > **Outils** > **Topologie de grille** (sélectionnez l'icône du graphique (après une valeur de données), des graphiques linéaires sont utilisés pour tracer les valeurs des attributs StorageGRID qui ont une valeur unitaire (comme le décalage de fréquence NTP, en ppm). Les variations de valeur sont représentées dans des intervalles de données réguliers (bins) au fil du temps.



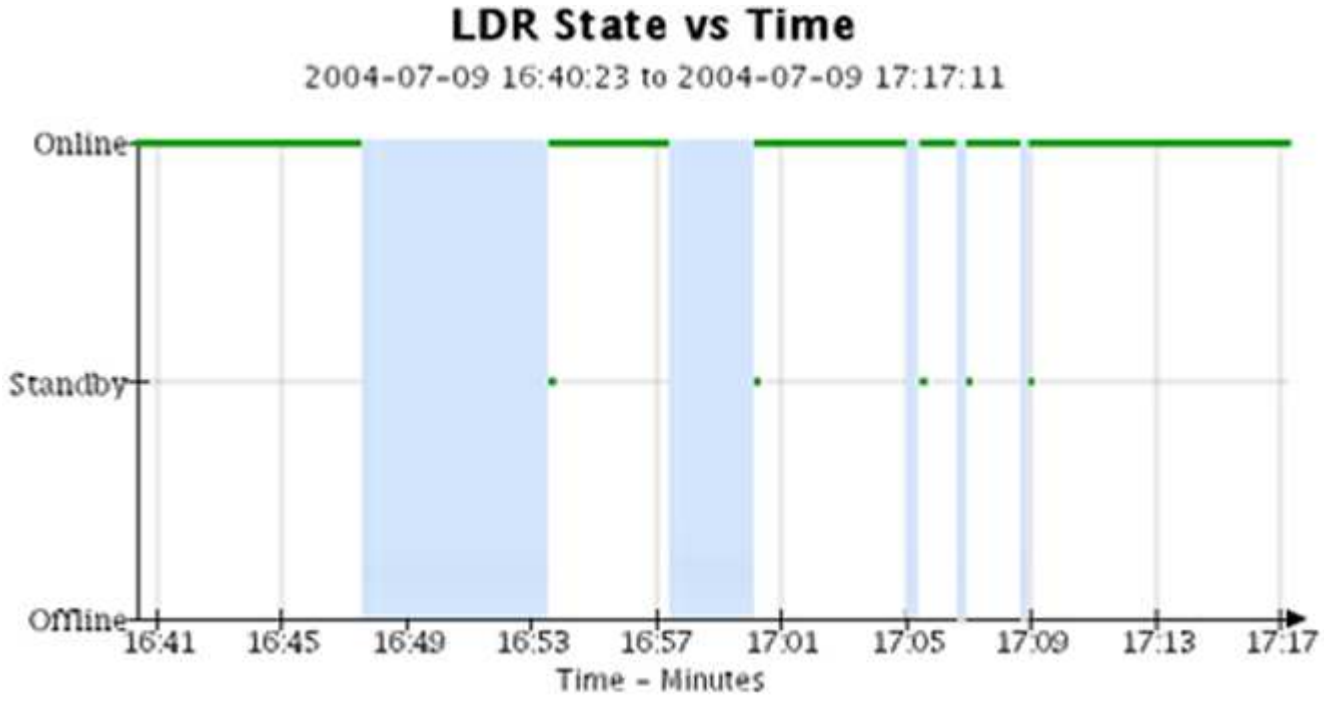
- **Graphiques de zone** : Disponibles à partir de la page Nœuds et de la page **SUPPORT** > **Outils** > **Topologie de grille** (sélectionnez l'icône du graphique (après une valeur de données), les graphiques de zone sont utilisés pour tracer des quantités d'attributs volumétriques, telles que le nombre d'objets ou les valeurs de charge de service. Les graphiques de surface sont similaires aux graphiques linéaires, mais incluent un ombrage marron clair sous la ligne. Les variations de valeur sont représentées dans des intervalles de données réguliers (bins) au fil du temps.



- Certains graphiques sont indiqués par un type d'icône de graphique différent et ont un format différent :



- **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 qui représentent des états distincts tels qu'un état de service qui peut être en ligne, en veille ou hors ligne. Les graphiques d'état sont similaires aux graphiques linéaires, mais la transition est discontinue ; c'est-à-dire que la valeur passe d'une valeur d'état à une autre.

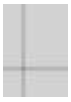


Informations connexes

- "Afficher la page Nœuds"
- "Afficher l'arborescence de la topologie de la grille"
- "Examiner les mesures de support"

Légende du graphique

Les lignes et les couleurs utilisées pour dessiner des cartes ont une signification spécifique.

Exemple	Signification
	Les valeurs d'attribut signalées sont tracées à l'aide de lignes vert foncé.
	Un ombrage vert clair autour des lignes vert foncé indique que les valeurs réelles dans cette plage de temps varient et ont été « regroupées » pour un traçage plus rapide. La ligne sombre représente la moyenne pondérée. La plage en vert clair indique les valeurs maximales et minimales dans le bac. Un ombrage marron clair est utilisé pour les graphiques de zone afin d'indiquer les données volumétriques.
	Les zones vides (aucune donnée tracée) indiquent que les valeurs d'attribut n'étaient 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-là étaient indéterminées ; l'attribut ne rapportait pas de valeurs car le service était dans un état inconnu.
	L'ombrage gris indique que certaines ou toutes les valeurs d'attribut à ce moment-là n'étaient pas connues car le service signalant les attributs était administrativement hors service.
	Un mélange de nuances grises et bleues indique que certaines des valeurs d'attribut à ce moment-là étaient indéterminées (car le service était dans un état inconnu), tandis que d'autres n'étaient pas connues car le service signalant les attributs était administrativement en panne.

Afficher des tableaux et des graphiques

La page Nœuds contient les graphiques et diagrammes auxquels vous devez accéder régulièrement pour surveiller des attributs tels que la capacité de stockage et le débit. Dans certains cas, notamment 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

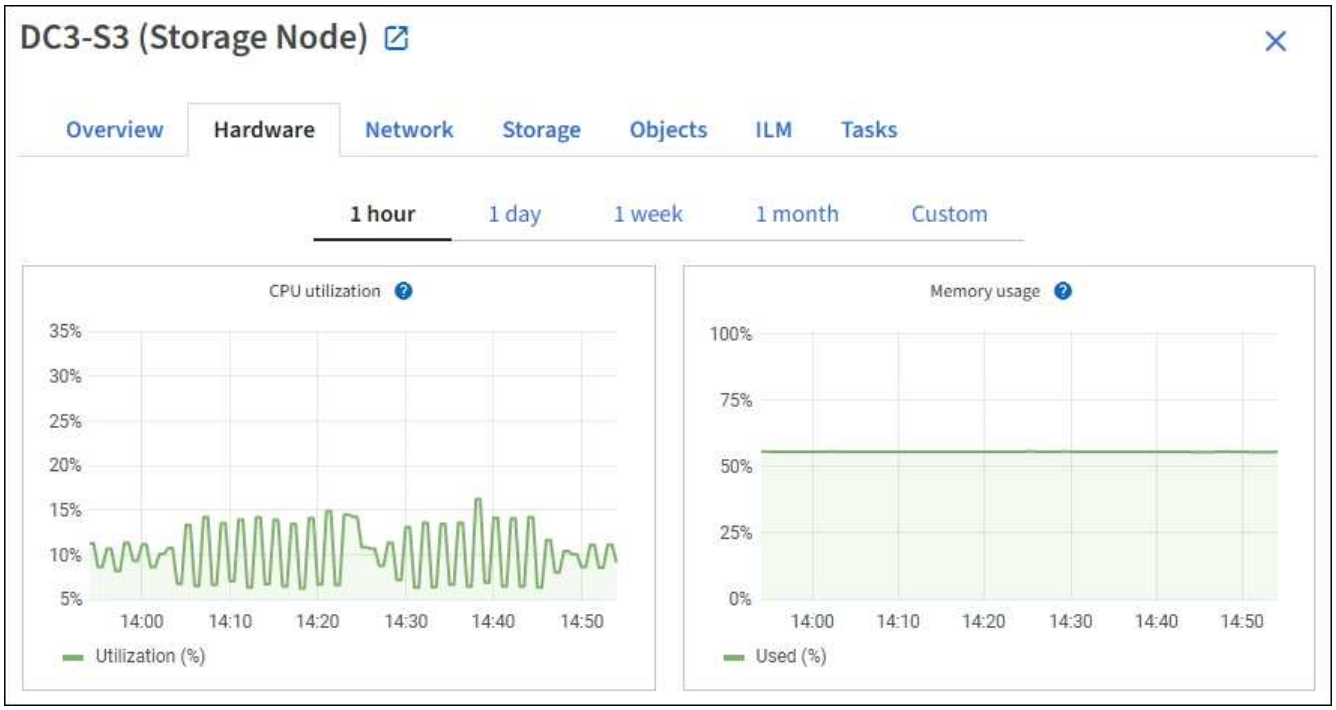
Vous devez être connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .

Étapes

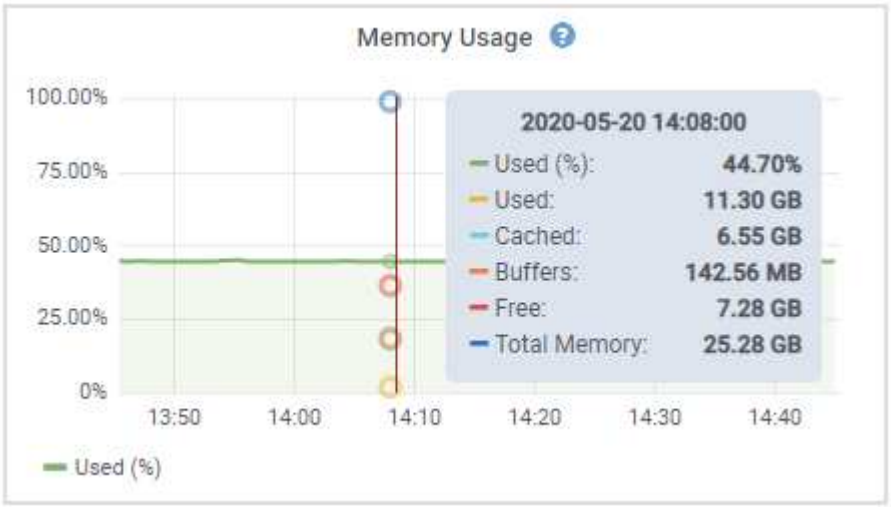
1. Sélectionnez **NODES**. Ensuite, sélectionnez un nœud, un site ou la grille entière.
2. Sélectionnez l'onglet pour lequel vous souhaitez afficher les informations.

   Certains onglets incluent un ou plusieurs graphiques Grafana, qui sont utilisés pour tracer les valeurs des

métriques Prometheus au fil du temps. Par exemple, l'onglet **NODES** > **Hardware** pour un nœud inclut deux graphiques Grafana.



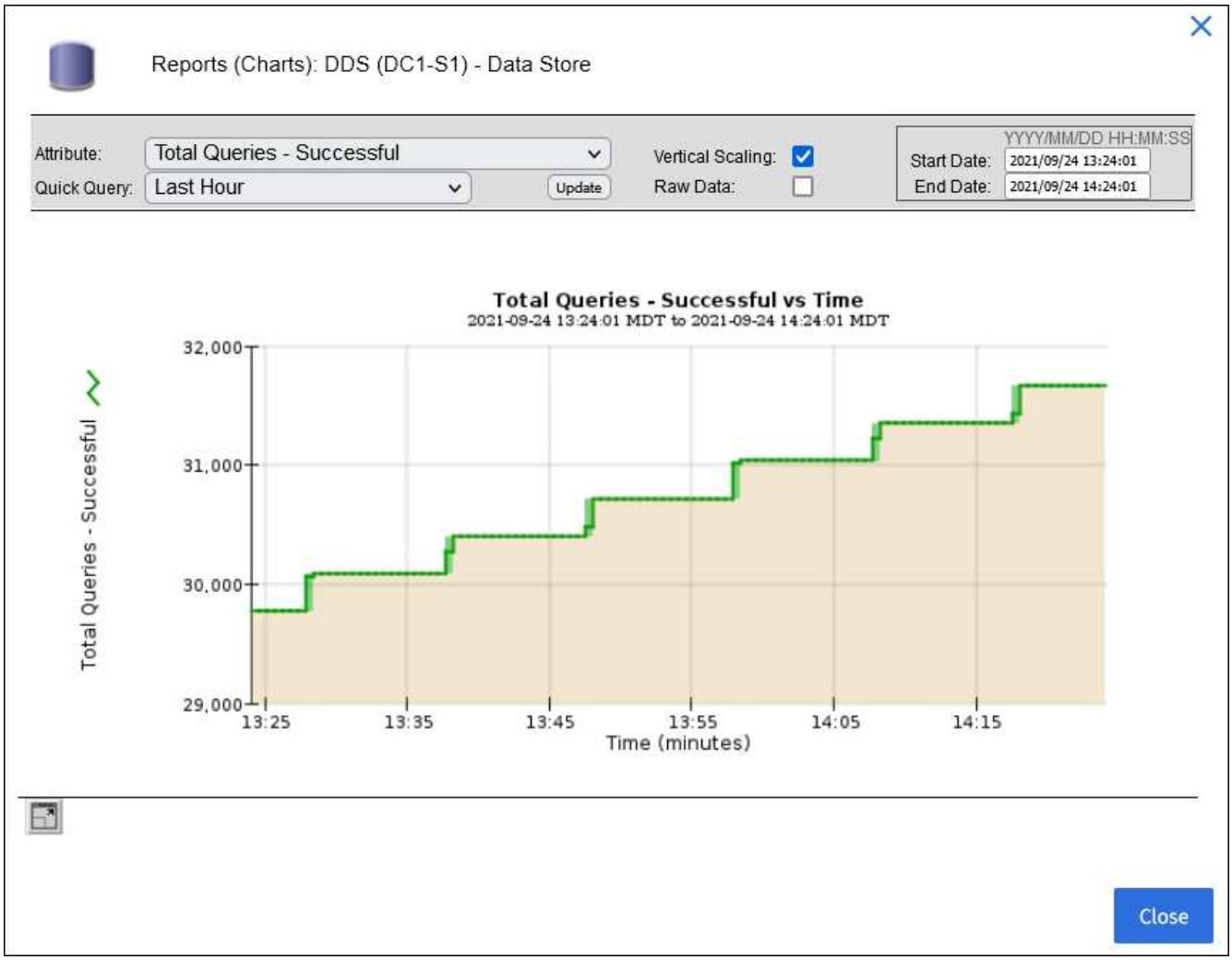
3. Vous pouvez également positionner votre curseur sur le graphique pour voir des valeurs plus détaillées pour un moment précis.

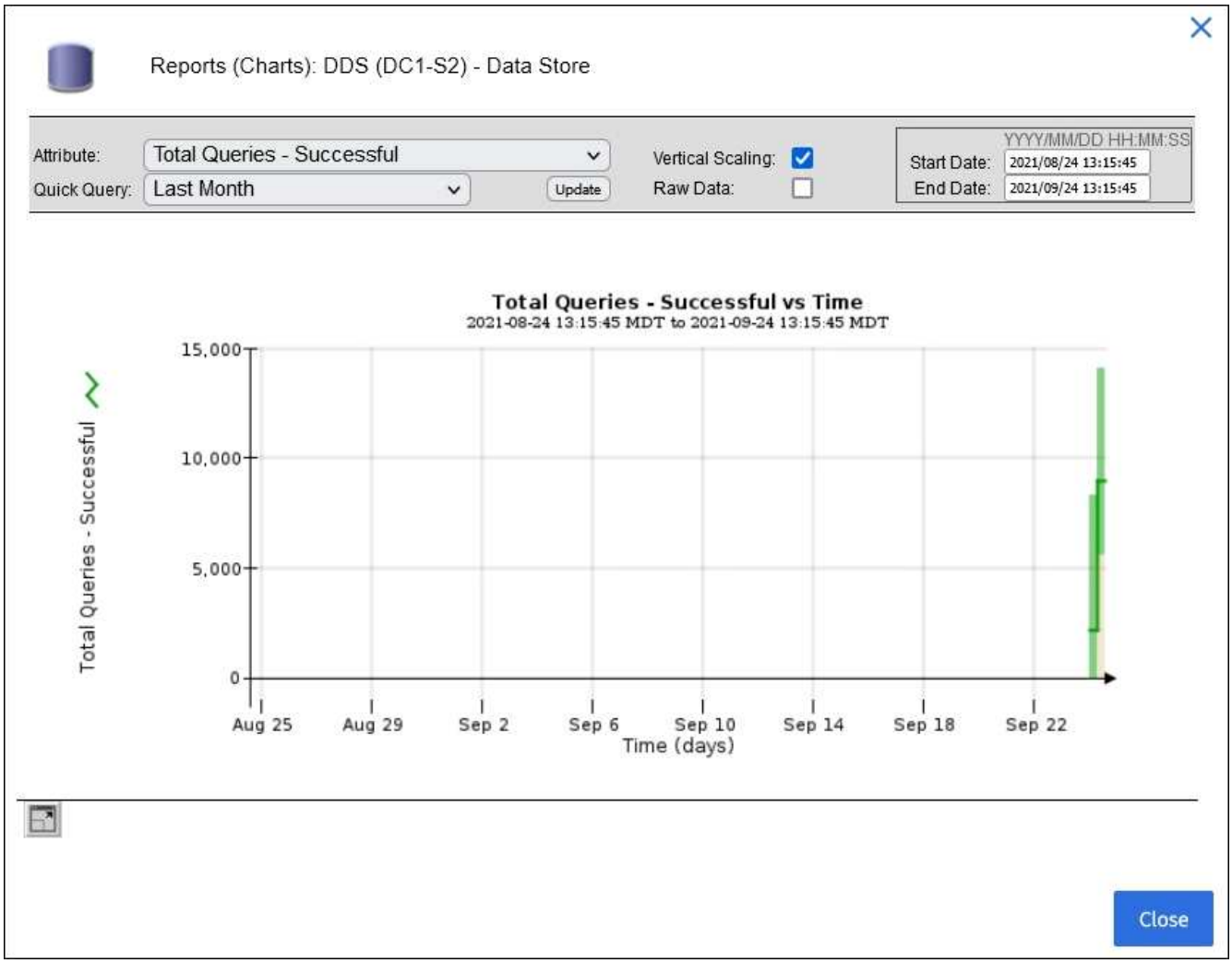


4. Selon les besoins, vous pouvez souvent afficher un graphique pour un attribut ou une mesure spécifique. Dans le tableau de la page Nœuds, sélectionnez l'icône du graphique à droite du nom de l'attribut.

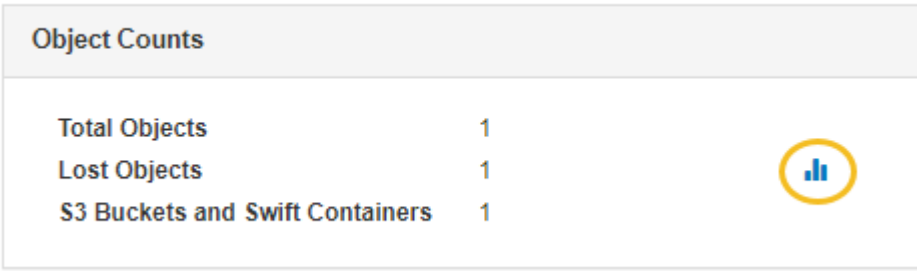
> Les graphiques ne sont pas disponibles pour toutes les métriques et tous les attributs.

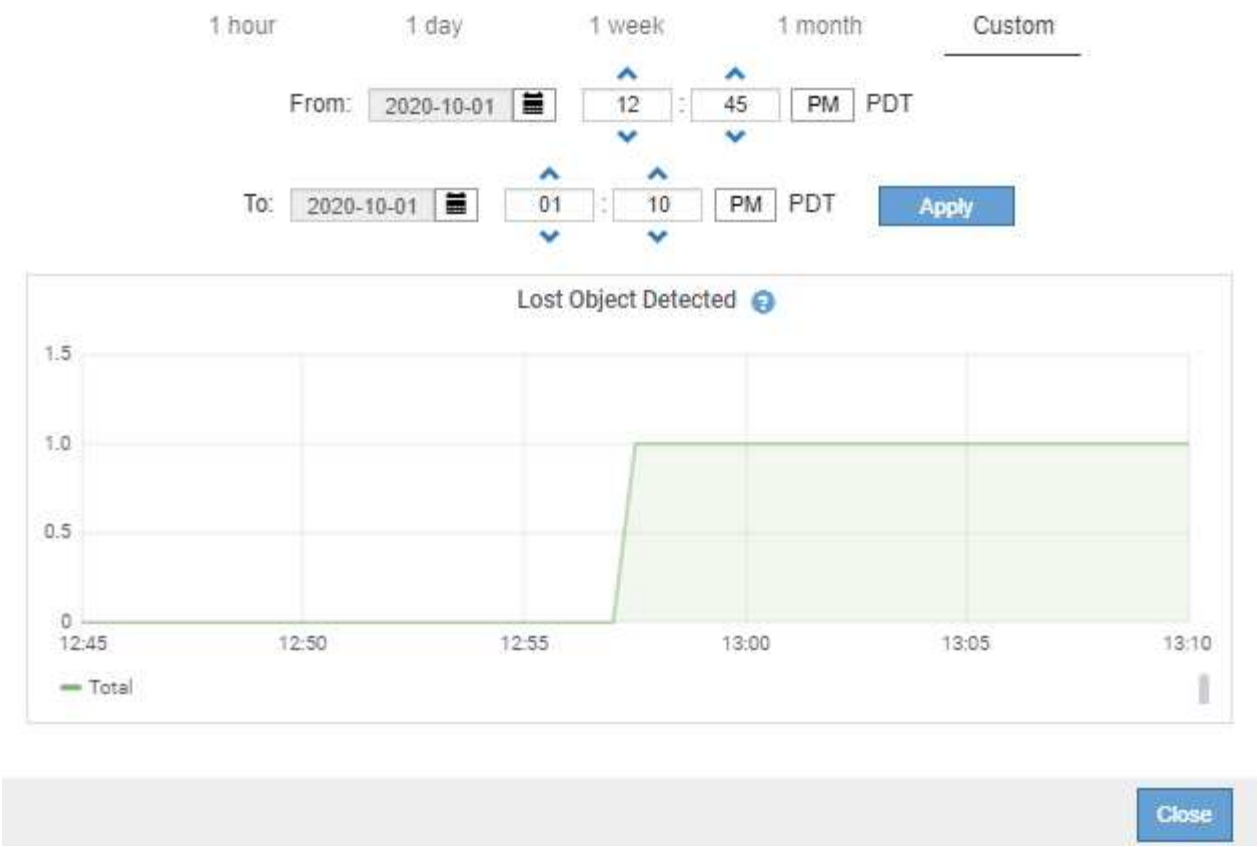
Exemple 1 : Dans l'onglet Objets d'un nœud de stockage, vous pouvez sélectionner l'icône de graphique pour voir le nombre total de requêtes de stockage de métadonnées réussies pour le nœud de stockage.


Reports (Charts): DDS (DC1-S1) - Data Store
Attribute:
Total Queries - Successful
Quick Query:
Last Hour
Update
Vertical Scaling:
Raw Data:
YYYY/MM/DD HH:MM:SS
Start Date:
2021/09/24 13:24:01
End Date:
2021/09/24 14:24:01
Total Queries - Successful vs Time
2021-09-24 13:24:01 MDT to 2021-09-24 14:24:01 MDT
Total Queries - Successful
32,000
31,000
30,000
29,000
13:25
13:35
13:45
13:55
14:05
14:15
Time (minutes)
Close

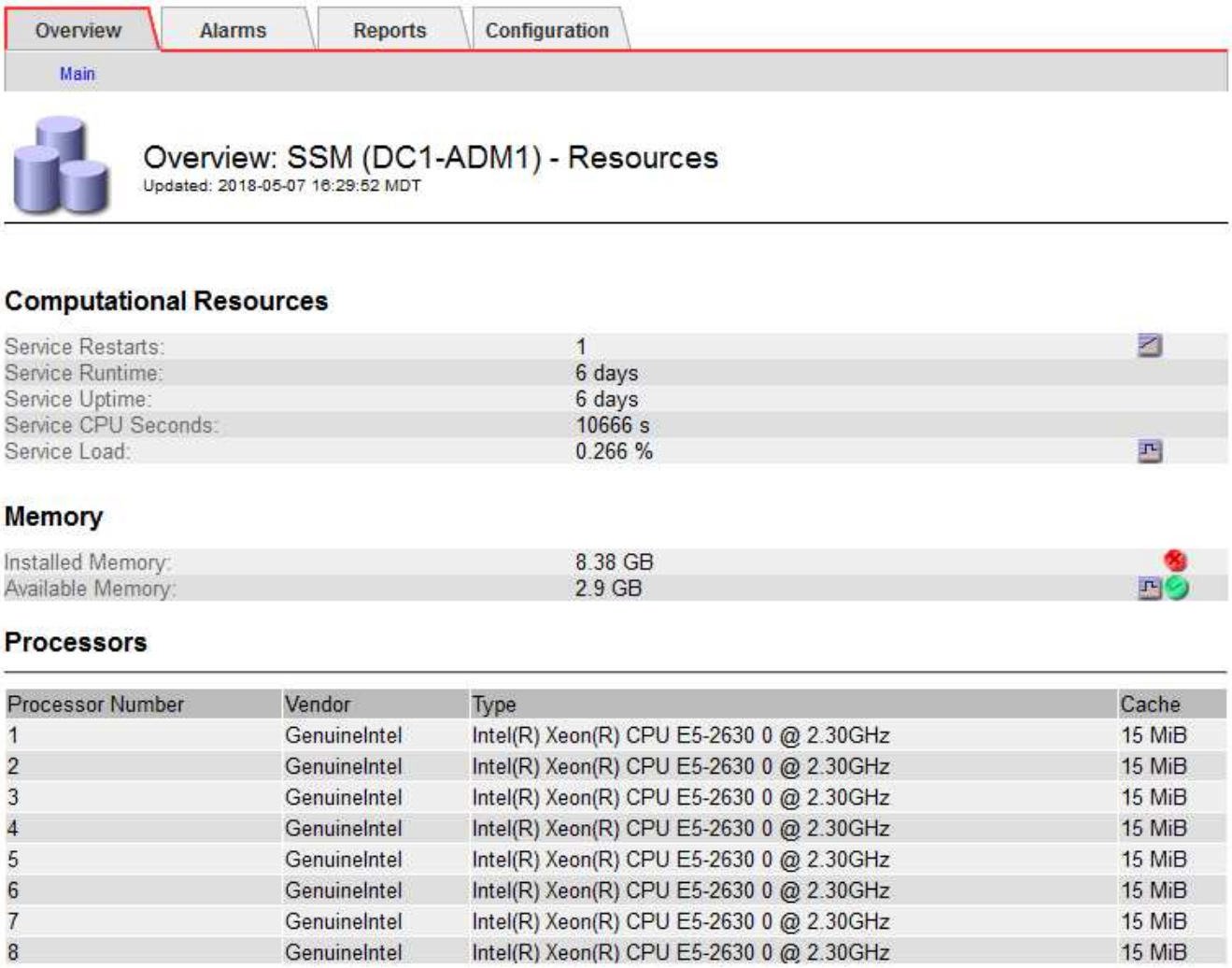


Exemple 2 : Dans l'onglet Objets d'un nœud de stockage, vous pouvez sélectionner l'icône de graphique pour voir le graphique Grafana du nombre d'objets perdus détectés au fil du temps.





5. Pour afficher les graphiques des attributs qui ne sont pas affichés sur la page Nœud, sélectionnez **SUPPORT** > **Outils** > **Topologie de grille**.
6. Sélectionnez ***nœud de grille*** > ***composant ou service*** > **Aperçu** > **Principal**.



7. Sélectionnez l'icône du graphique à côté de l'attribut.

   L'affichage passe automatiquement à la page **Rapports** > **Graphiques**. Le graphique affiche les données de l'attribut au cours de la dernière journée.

Générer des graphiques

Les graphiques affichent une représentation graphique des valeurs des données d'attribut. Vous pouvez générer un rapport sur un site de centre de données, un nœud de grille, un composant ou un service.

Avant de commencer

- Vous devez être connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Tu as"autorisations d'accès spécifiques" .

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **Topologie de grille**.
2. Sélectionnez ***nœud de grille*** > ***composant ou service*** > **Rapports** > **Graphiques**.
3. Sélectionnez l'attribut sur lequel générer le rapport dans la liste déroulante **Attribut**.
4. Pour forcer l'axe Y à démarrer à zéro, décochez la case **Mise à l'échelle verticale**.
5. Pour afficher les valeurs avec une précision totale, cochez la case **Données brutes** ou pour arrondir les

valeurs à un maximum de trois décimales (par exemple, pour les attributs indiqués sous forme de pourcentages), décochez la case **Données brutes**.

6. Sélectionnez la période sur laquelle porter le rapport dans la liste déroulante **Requête rapide**.

   Sélectionnez l'option Requête personnalisée pour sélectionner une plage horaire spécifique.

   Le graphique apparaît après quelques instants. Prévoyez quelques minutes pour la tabulation des plages de temps longues.

7. Si vous avez sélectionné Requête personnalisée, personnalisez la période du graphique en saisissant la **Date de début** et la **Date de fin**.

   Utiliser le format *YYYY/MM/DDHH:MM:SS* en heure locale. Des zéros non significatifs sont requis pour correspondre au format. Par exemple, 2017/4/6 7:30:00 échoue à la validation. Le format correct est : 2017/04/06 07:30:00.

8. Sélectionnez **Mettre à jour**.

   Un graphique est généré après quelques secondes. Prévoyez quelques minutes pour la tabulation des plages de temps longues. En fonction de la durée définie pour la requête, un rapport de texte brut ou un rapport de texte agrégé s'affiche.

Utiliser des rapports textuels

Les rapports textuels affichent une représentation textuelle des valeurs de données d'attribut qui ont été traitées par le service NMS. Il existe deux types de rapports générés en fonction de la période sur laquelle vous effectuez le rapport : les rapports de texte brut pour les périodes inférieures à une semaine et les rapports de texte agrégé pour les périodes supérieures à une semaine.

Rapports de texte brut

Un rapport de 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 d'échantillonnage : date et heure locales auxquelles une valeur d'attribut a été échantillonnée ou modifiée à la source.
- Valeur : valeur de l'attribut au moment de l'échantillonnage.

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 %

Rapports de texte agrégés

Un rapport de texte agrégé affiche des données sur une période plus longue (généralement une semaine) qu'un rapport de texte brut. Chaque entrée est le résultat de la synthèse de plusieurs valeurs d'attribut (un agrégat de valeurs d'attribut) par le service NMS au fil du temps dans 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 auxquelles le service NMS a agrégé (collecté) un ensemble de valeurs d'attribut modifiées.
- Valeur moyenne : la moyenne de la valeur de l'attribut sur la période agrégée.
- Valeur minimale : la valeur minimale sur la période agrégée.
- Valeur maximale : la valeur maximale sur la période 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 textuels

Les rapports textuels affichent une représentation textuelle des valeurs de données d'attribut qui ont été traitées par le service NMS. Vous pouvez générer un rapport sur un site de centre de données, un nœud de grille, un composant ou un service.

Avant de commencer

- Vous devez être connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Tu as"autorisations d'accès spécifiques" .

À propos de cette tâche

Pour les données d'attribut qui sont censées 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 basées sur des événements tels que des changements d'état ou de statut), 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 des périodes supérieures à une semaine.

Le texte gris indique que le service était administrativement hors service pendant la période d'échantillonnage. Le texte bleu indique que le service était dans un état inconnu.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **Topologie de grille**.
2. Sélectionnez ***nœud de grille*** > ***composant ou service*** > **Rapports** > **Texte**.
3. Sélectionnez l'attribut sur lequel générer le rapport 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 indiqués sous forme de pourcentages), décochez la case **Données brutes**.
6. Sélectionnez la période sur laquelle porter le rapport dans la liste déroulante **Requête rapide**.

   Sélectionnez l'option Requête personnalisée pour sélectionner une plage horaire spécifique.

Le rapport apparaît après quelques instants. Prévoyez quelques minutes pour la tabulation des plages de temps longues.

7. Si vous avez sélectionné Requête personnalisée, vous devez personnaliser la période sur laquelle porter le rapport en saisissant la **Date de début** et la **Date de fin**.

   Utiliser le format `YYYY/MM/DDHH:MM:SS` en heure locale. Des zéros non significatifs sont requis pour correspondre au format. Par exemple, 2017/4/6 7:30:00 échoue à la validation. Le format correct est : 2017/04/06 07:30:00.

8. Cliquez sur **Mettre à jour**.

   Un rapport texte est généré après quelques instants. Prévoyez quelques minutes pour la tabulation des plages de temps longues. En fonction de la durée définie pour la requête, un rapport de texte brut ou un rapport de texte agrégé s'affiche.

Exporter des rapports de texte

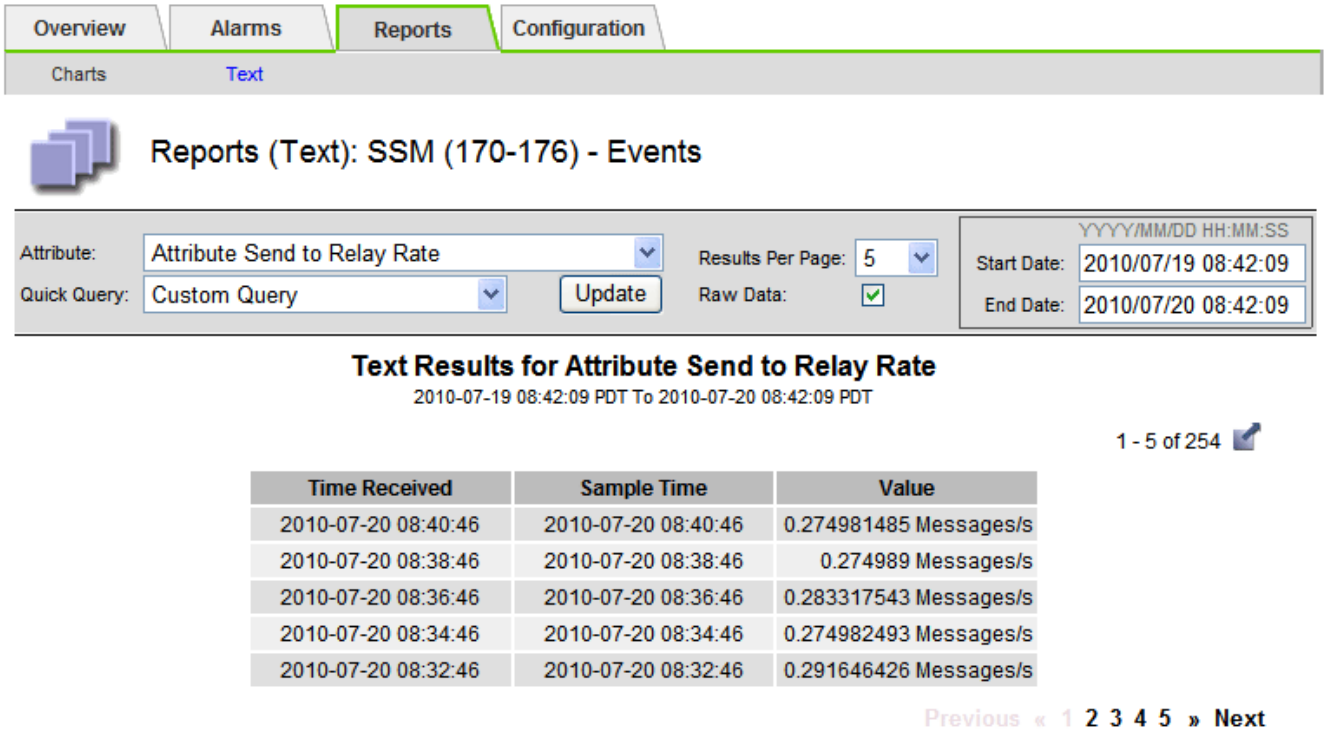
Les rapports de texte exportés ouvrent un nouvel onglet de navigateur, qui vous permet de sélectionner et de copier les données.

À propos de cette 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

1. Sélectionnez **SUPPORT** > **Outils** > **Topologie de grille**.
2. Créer un rapport texte.
3. Cliquez sur *Exporter* .



La fenêtre Rapport d'exportation de texte s'ouvre et affiche le rapport.

Grid ID: 000 000
OID: 2.16.124.113590.2.1.400019.1.1.1.16996732.200
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 Rapport de texte d'exportation.

   Ces données peuvent désormais être collées dans un document tiers tel qu'une feuille de calcul.

Surveiller les performances PUT et GET

Vous pouvez surveiller les performances de certaines opérations, telles que le stockage et la récupération d'objets, pour aider à identifier les modifications qui pourraient nécessiter une enquête plus approfondie.

À propos de cette tâche

Pour surveiller les performances PUT et GET, vous pouvez exécuter des commandes S3 directement depuis un poste de travail ou en utilisant l'application open source S3tester. L'utilisation de ces méthodes vous permet d'évaluer les performances indépendamment des facteurs externes à StorageGRID, tels que les problèmes avec une application cliente ou les problèmes avec un réseau externe.

Lorsque vous effectuez des tests d'opérations PUT et GET, utilisez les directives suivantes :

- Utilisez des tailles d'objet comparables à celles des objets que vous ingérez généralement dans votre grille.
- Effectuer des opérations sur des sites locaux et distants.

Messages dans le"journal d'audit" indique le temps total nécessaire pour exécuter certaines opérations. Par exemple, pour déterminer le temps de traitement total d'une requête S3 GET, vous pouvez consulter 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 satisfaire une demande, ainsi que le débit global que vous pouvez atteindre. Répétez régulièrement les mêmes tests et enregistrez les résultats, afin de pouvoir identifier les tendances qui pourraient nécessiter une enquête.

- Tu peux "télécharger S3tester depuis github" .

Surveiller les opérations de vérification des objets

Le système StorageGRID peut vérifier l'intégrité des données d'objet sur les nœuds de stockage, en recherchant les objets corrompus et manquants.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"Autorisation d'accès de maintenance ou root" .

À propos de cette tâche

Deux"processus de vérification" travailler ensemble pour garantir l'intégrité des données :

- **La vérification en arrière-plan** s'exécute automatiquement, vérifiant en permanence 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 de données d'objet répliquées et codées par effacement. Si des problèmes sont détectés, le système StorageGRID tente automatiquement de remplacer les données d'objet corrompues à partir de 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 de l'objet** peut être déclenchée par un utilisateur pour vérifier plus rapidement l'existence (mais pas l'exactitude) des données de l'objet.

  La vérification de l'existence de l'objet vérifie si toutes les copies répliquées attendues des objets et des fragments codés par effacement existent sur un nœud de stockage. La vérification de l'existence d'un objet fournit un moyen de vérifier l'intégrité des périphériques de stockage, en particulier si un problème matériel récent a pu affecter l'intégrité des données.

Vous devez examiner régulièrement les résultats des vérifications d'arrière-plan et des contrôles d'existence des objets. Enquêtez immédiatement sur tous les cas de données d'objet corrompues ou manquantes pour déterminer la cause première.

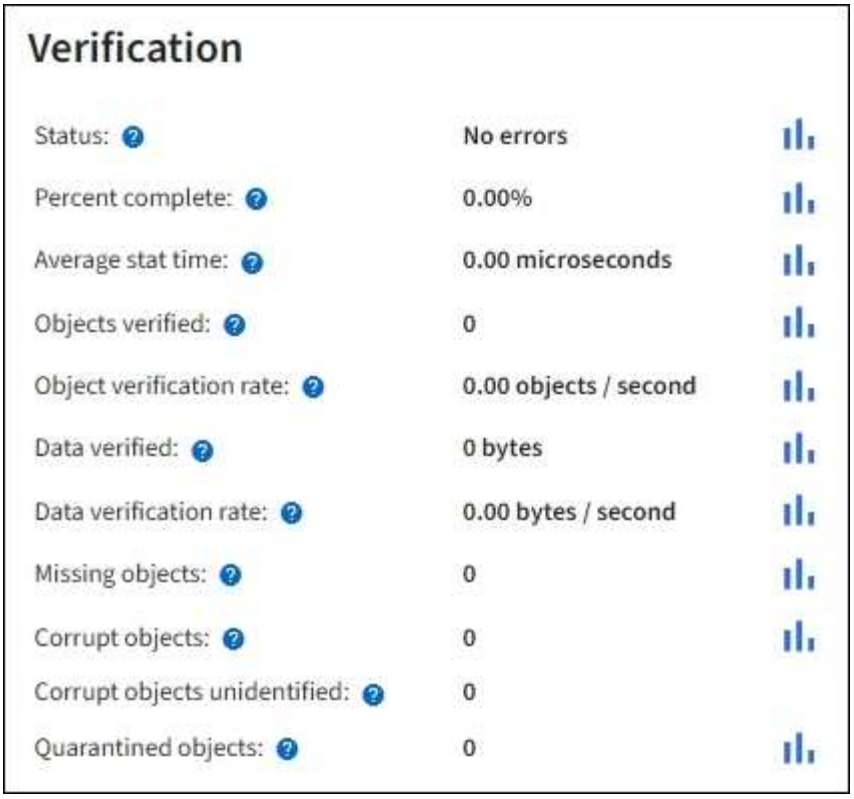
Étapes

1. Examiner les résultats des vérifications des antécédents :

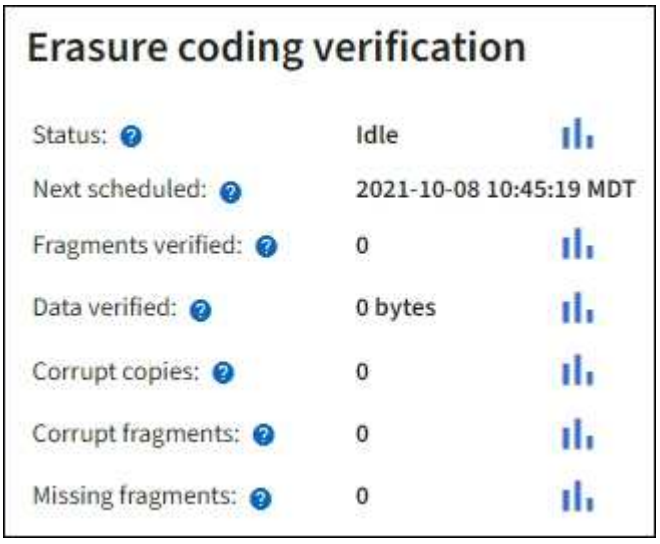
   a. Sélectionnez **NODES** > ***Storage Node*** > **Objects**.

   b. Vérifiez les résultats de la vérification :

      - Pour vérifier la vérification des données d'objet répliquées, examinez les attributs dans la section Vérification.

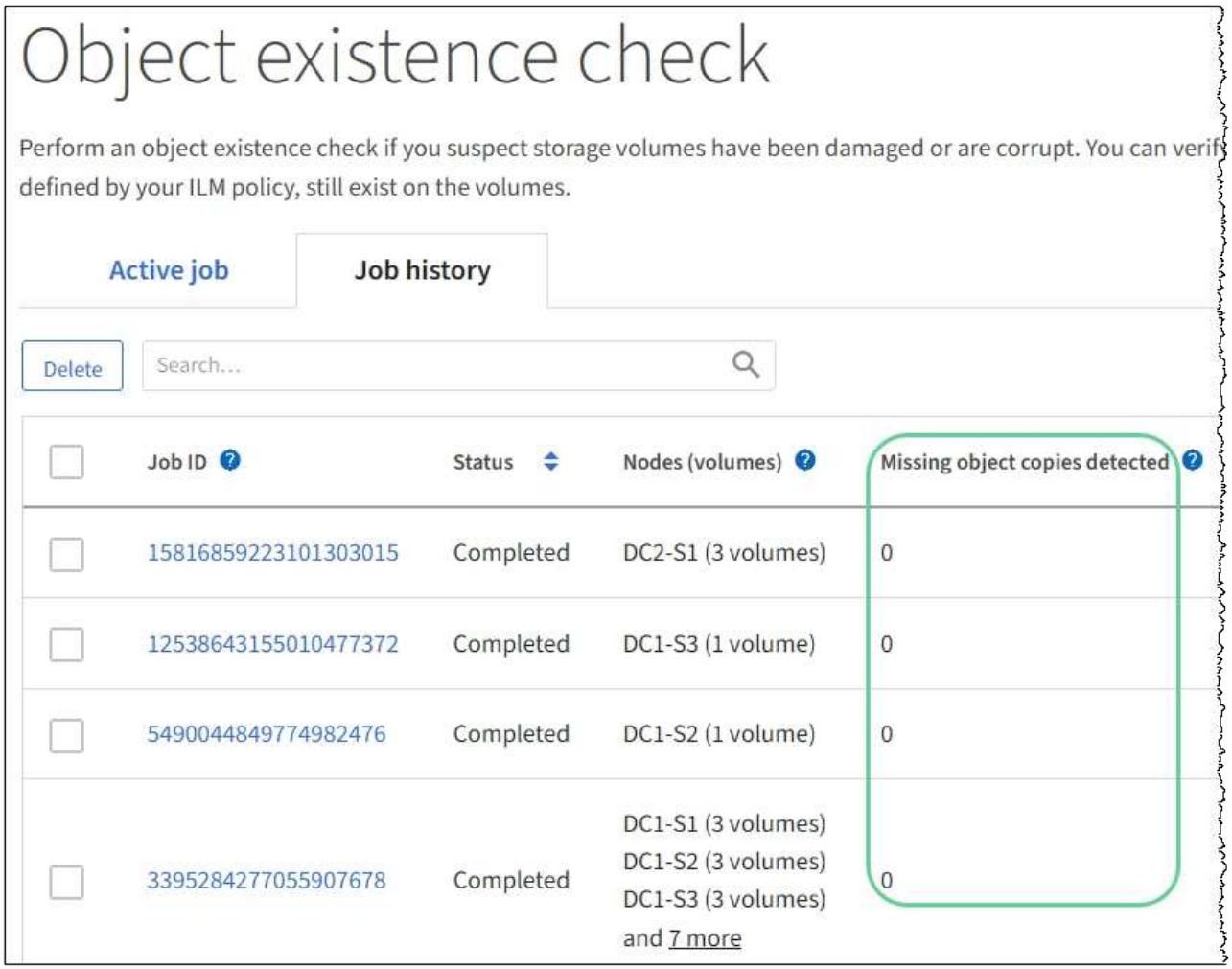


- Pour vérifier la vérification des fragments codés par effacement, sélectionnez ***Storage Node*** > **ILM** et examinez les attributs dans la section Vérification du codage par effacement.



Sélectionnez le point d'interrogation à côté du nom d'un attribut pour afficher un texte d'aide.

2. Examinez les résultats des tâches de vérification de l'existence des objets :
   a. Sélectionnez **MAINTENANCE** > **Vérification de l'existence de l'objet** > **Historique des tâches**.
   b. Analysez la colonne Copies d'objets manquantes détectées. Si des tâches ont entraîné la perte de 100 copies d'objets ou plus et que l'alerte **Objets perdus** a été déclenchée, contactez le support technique.



Surveiller les 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 enregistrés sur le serveur Syslog. Le message Dernier événement affiché dans le Gestionnaire de grille fournit plus d'informations sur l'événement le plus récent.

Les messages d'événements sont également répertoriés dans le `/var/local/log/bycast-err.log` fichier journal. Voir le"Référence des fichiers journaux" .

L'alarme SMTT (Total des événements) 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'enquête sur les événements afin que vous puissiez mieux comprendre pourquoi ces alarmes se sont produites. Si un événement s'est produit en raison d'un problème connu, il est possible de réinitialiser les compteurs d'événements en toute sécurité.

Étapes

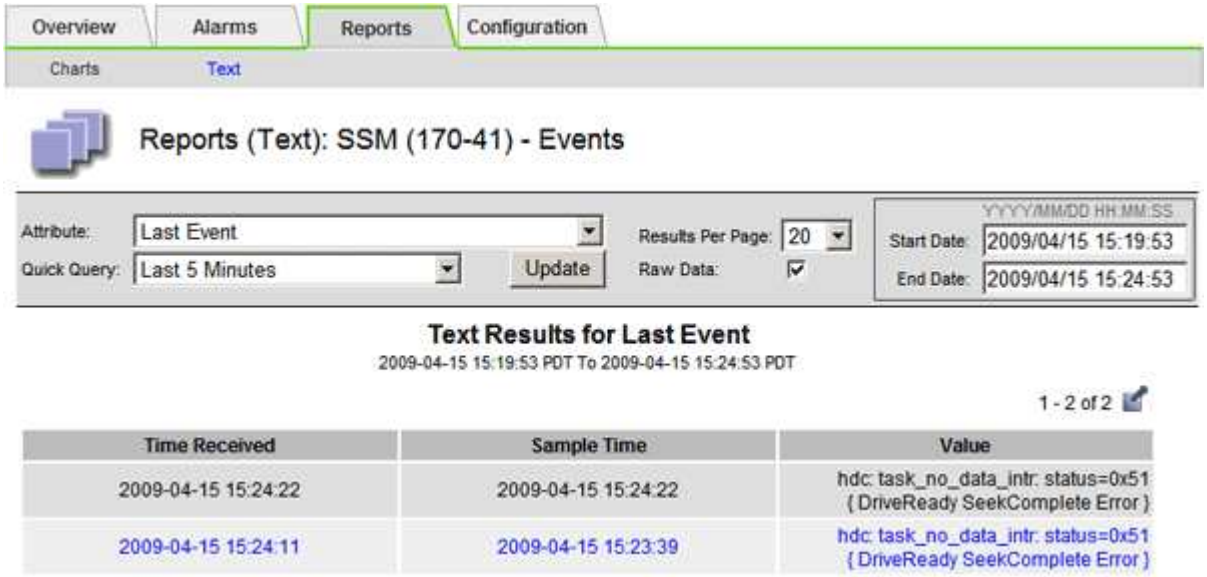
1. Passez en revue les événements système pour chaque nœud de grille :
   a. Sélectionnez **SUPPORT** > **Outils** > **Topologie de grille**.
   b. Sélectionnez ***site*** > ***nœud de grille*** > **SSM** > **Événements** > **Aperçu** > **Principal**.
2. Générez une liste de messages d'événements précédents pour aider à isoler les problèmes survenus dans

le passé :

a. Sélectionnez **SUPPORT** > **Outils** > **Topologie de grille**.
b. Sélectionnez ***site*** > ***nœud de grille*** > **SSM** > **Événements** > **Rapports**.
c. Sélectionnez **Texte**.

   L'attribut **Dernier événement** n'est pas affiché dans le"vue des graphiques" . Pour le voir :

d. Changez **Attribut** en **Dernier événement**.
e. Vous pouvez également sélectionner une période pour la **Requête rapide**.
f. Sélectionnez **Mettre à jour**.



Créer des événements syslog personnalisés

Les événements personnalisés vous permettent de suivre tous les événements utilisateur de niveau noyau, démon, erreur et critique enregistrés 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 pannes matérielles).

À propos de cette tâche

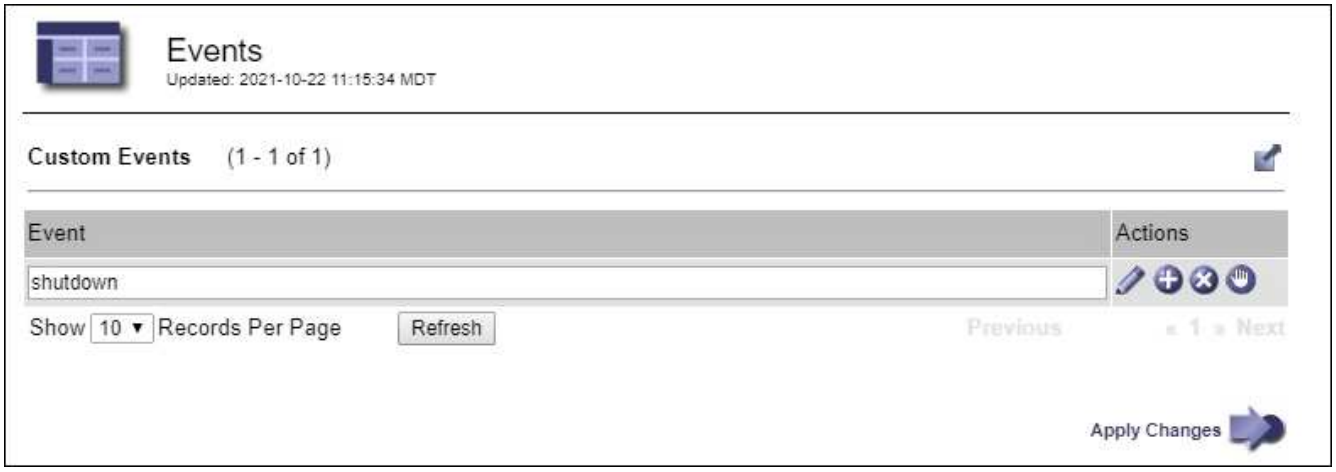
Envisagez de créer des événements personnalisés pour surveiller les problèmes récurrents. Les considérations suivantes s'appliquent aux événements personnalisés.

- Une fois qu'un événement personnalisé est créé, chaque occurrence de celui-ci est surveillée.
- Pour créer un événement personnalisé basé sur des mots-clés dans le `/var/local/log/messages` fichiers, les journaux dans ces fichiers doivent être :
  - Généré par le noyau
  - Généré par un démon ou un programme utilisateur au niveau d'erreur ou critique

Remarque : toutes les entrées du `/var/local/log/messages` les fichiers seront mis en correspondance à moins qu'ils ne satisfassent aux exigences énoncées ci-dessus.

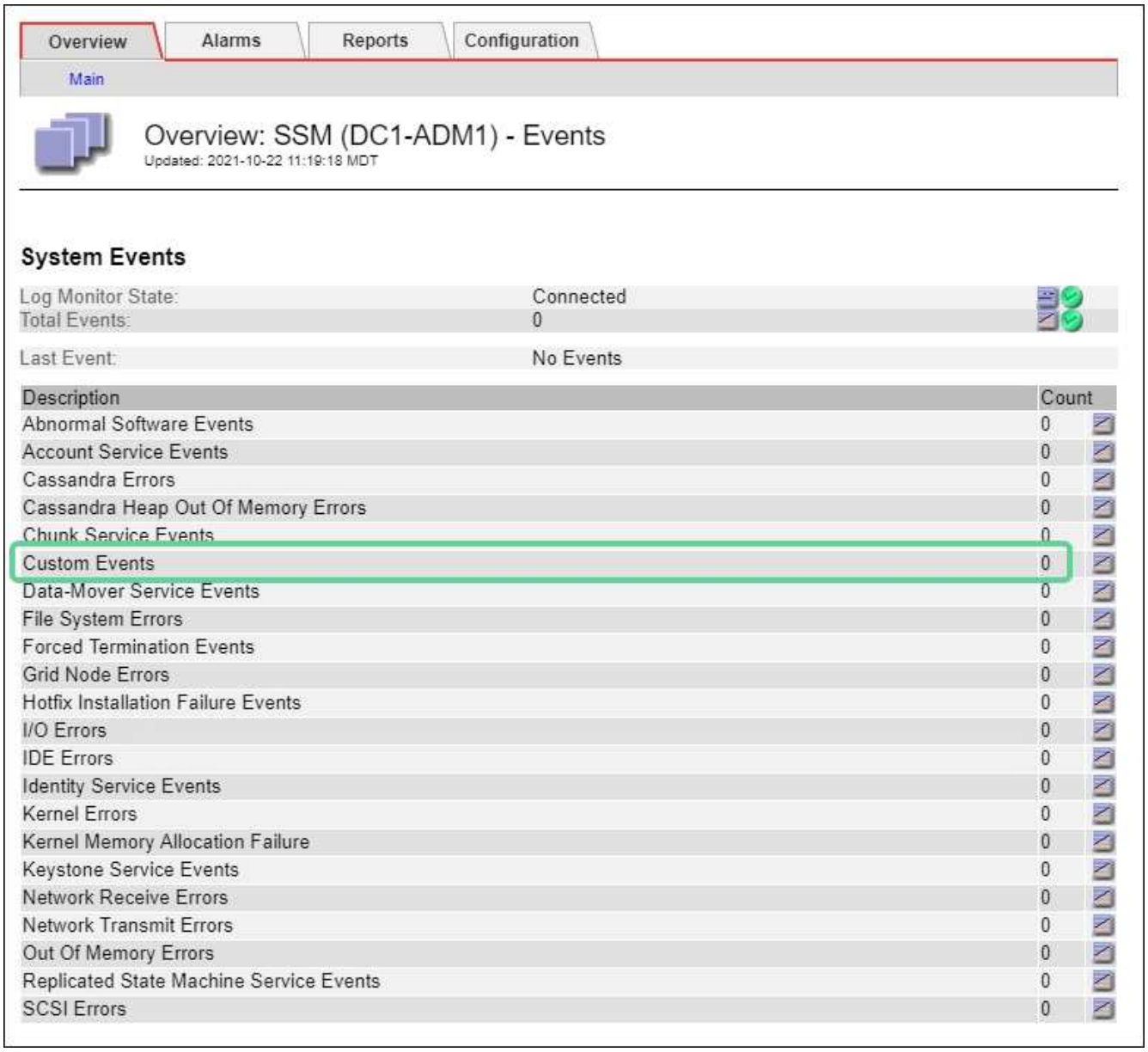
Étapes

1. Sélectionnez **SUPPORT** > **Alarmes (héritées)** > **Événements personnalisés**.
2. Cliquez sur *Modifier* (ou *Insérer* si ce n'est pas le premier événement).
3. Saisissez une chaîne d'événement personnalisée, par exemple, arrêt



4. Sélectionnez **Appliquer les modifications**.
5. Sélectionnez **SUPPORT** > **Outils** > **Topologie de grille**.
6. Sélectionnez ***nœud de grille*** > **SSM** > **Événements**.
7. Recherchez l'entrée pour les événements personnalisés dans la table Événements et surveillez la valeur de **Count**.

   Si le nombre augmente, un événement personnalisé que vous surveillez est déclenché sur ce nœud de grille.



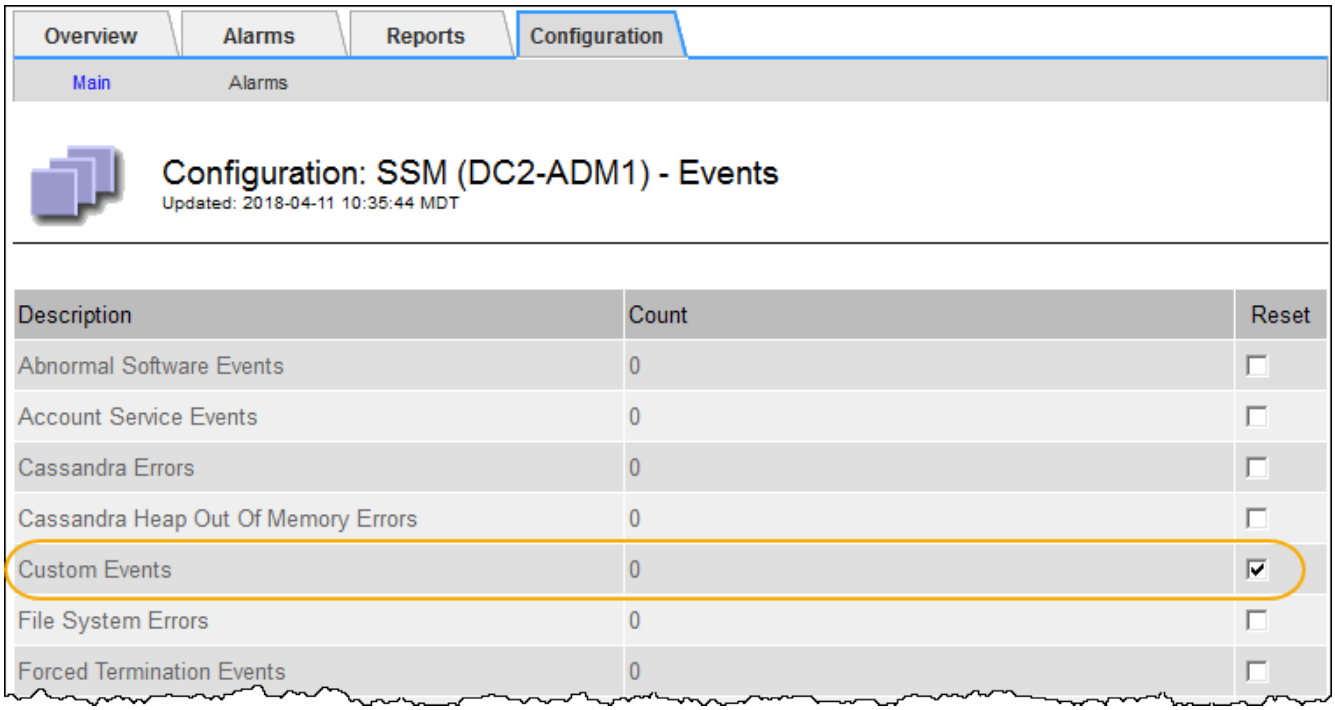
Réinitialiser le nombre d'événements personnalisés à zéro

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 provoque le déclenchement de l'alarme par l'événement suivant. En revanche, lorsque vous reconnaissez une alarme, celle-ci n'est redéclenchée que si le niveau de seuil suivant est atteint.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **Topologie de grille**.
2. Sélectionnez ***nœud de grille*** > **SSM** > **Événements** > **Configuration** > **Principal**.
3. Cochez la case **Réinitialiser** pour les événements personnalisés.



4. Sélectionnez **Appliquer les modifications**.

Examiner les messages d'audit

Les messages d'audit peuvent vous aider à mieux comprendre les opérations détaillées 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 du système sont liés au système d'audit lui-même, aux états des nœuds de grille, à l'activité des tâches à l'échelle du système et aux opérations de sauvegarde de service.
- Les messages d'audit du stockage d'objets sont liés au stockage et à la gestion des objets dans StorageGRID, y compris le stockage et les récupérations d'objets, les transferts de nœud de grille à nœud de grille et les vérifications.
- Les messages d'audit de lecture et d'écriture du client sont enregistrés lorsqu'une application client S3 effectue une demande de création, de modification ou de récupération d'un objet.
- Les messages d'audit de gestion enregistrent les demandes des utilisateurs adressées à 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 des informations d'audit par défaut, ou vous pouvez modifier la destination :

- StorageGRID utilise par défaut les destinations d'audit des nœuds locaux.
- Les entrées du journal d'audit de Grid Manager et de Tenant Manager peuvent être envoyées à un nœud

de stockage.

- En option, vous pouvez modifier la destination des journaux d'audit et envoyer les informations d'audit à un serveur syslog externe. Les journaux locaux des enregistrements d'audit continuent d'être générés et stockés lorsqu'un serveur syslog externe est configuré.
- "En savoir plus sur la configuration des messages d'audit et des 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, consultez"Examiner les journaux d'audit" .

Collecter les fichiers journaux et les données système

Vous pouvez utiliser Grid Manager 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" .
- Tu as"autorisations d'accès spécifiques" .
- Vous devez disposer de la phrase secrète de provisionnement.

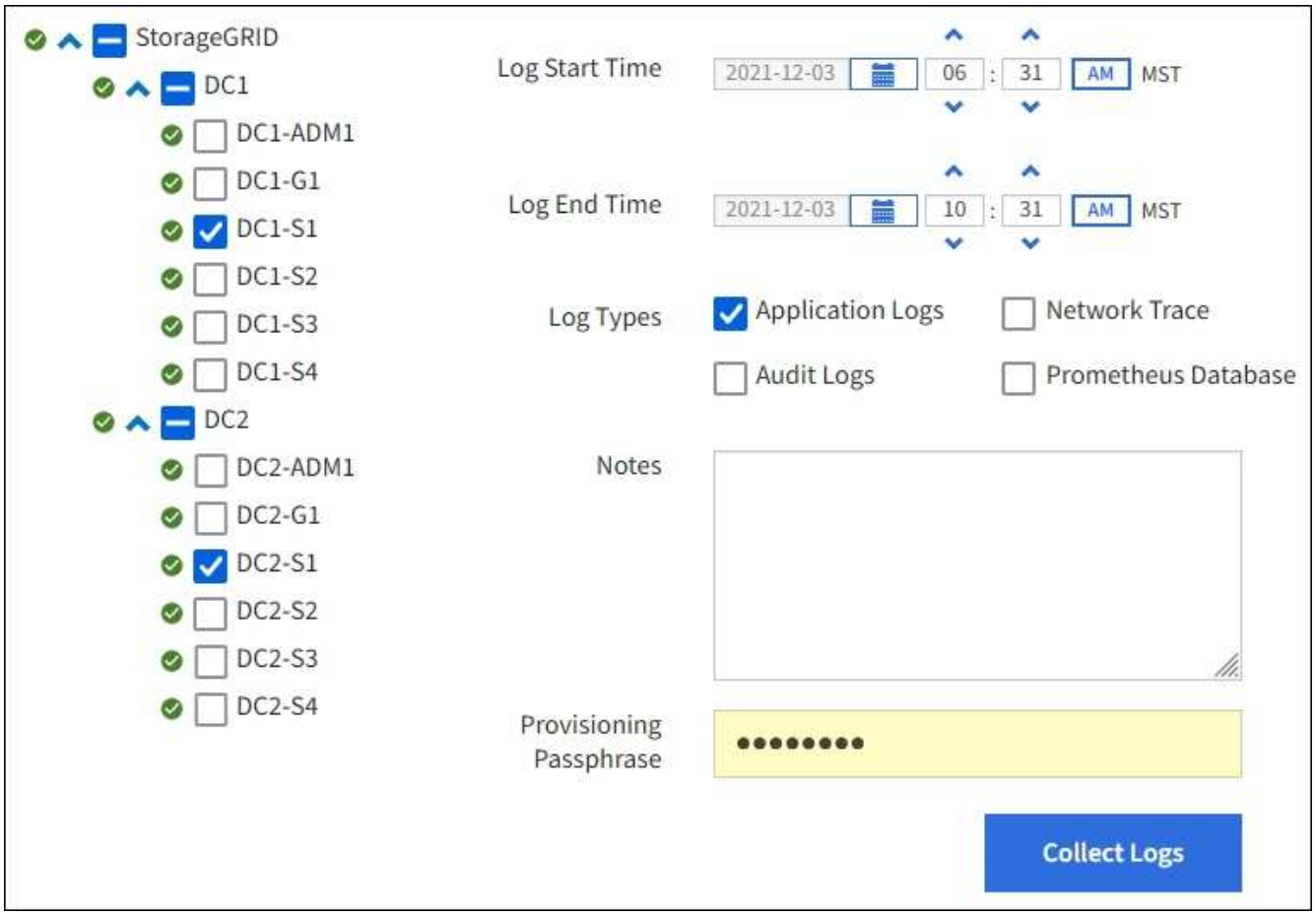
À propos de cette tâche

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.

En option, vous pouvez modifier la destination des journaux d'audit et envoyer les informations d'audit à un serveur syslog externe. Les journaux locaux des enregistrements d'audit continuent d'être générés et stockés lorsqu'un serveur syslog externe est configuré. Voir "Configurer 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.

   Selon vos besoins, vous pouvez collecter des fichiers journaux pour l'ensemble de la grille ou pour l'ensemble d'un site de centre de données.

3. Sélectionnez une **Heure de début** et une **Heure de fin** pour définir la plage horaire des données à inclure dans les fichiers journaux.

   Si vous sélectionnez une période très longue ou collectez les journaux de tous les nœuds d'une grande grille, l'archive des journaux peut devenir trop volumineuse pour être stockée sur un nœud ou trop volumineuse pour être collectée sur le nœud d'administration principal pour téléchargement. Si cela se produit, vous devez redémarrer la collecte des journaux avec un ensemble de données plus petit.

4. Sélectionnez les types de journaux que vous souhaitez collecter.
   - **Journaux d'application** : journaux spécifiques aux applications 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 du réseau.
   - **Base de données Prometheus** : métriques de séries chronologiques provenant des services sur tous les nœuds.
5. Vous pouvez également saisir des notes sur les fichiers journaux que vous collectez dans la zone de texte **Notes**.

Vous pouvez utiliser ces notes pour fournir au support technique des informations sur le problème qui vous a incité à collecter les fichiers journaux. Vos notes sont ajoutées à un fichier appelé `info.txt` , ainsi que d'autres informations sur la collecte de fichiers journaux. Le `info.txt` le fichier est enregistré dans le package d'archive du fichier journal.

6. Saisissez la phrase secrète de provisionnement de votre système StorageGRID dans la zone de texte **Phrase secrète 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 grille.

   Si vous recevez un message d'erreur concernant la taille du journal, essayez de collecter les journaux pendant une période plus courte ou pour moins de nœuds.

8. Sélectionnez **Télécharger** lorsque la collecte du fichier journal est terminée.

   Le fichier *.tar.gz* contient tous les fichiers journaux de tous les nœuds de grille où la collecte des journaux a réussi. À l'intérieur du fichier combiné *.tar.gz*, il y a une archive de fichier journal pour chaque nœud de grille.

Après avoir terminé

Vous pouvez retélécharger le package d'archive du fichier journal ultérieurement si vous en avez besoin.

En option, vous pouvez sélectionner **Supprimer** pour supprimer le package d'archive du fichier journal et libérer de l'espace disque. Le package d'archive de fichiers journaux actuel est automatiquement supprimé la prochaine fois que vous collectez des 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 package AutoSupport .

Avant de commencer

- Vous devez être connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous devez disposer de l'accès root ou de l'autorisation de configuration d'une autre grille.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > * AutoSupport*.
2. Dans l'onglet **Actions**, sélectionnez **Envoyer AutoSupport déclenchée par l'utilisateur**.

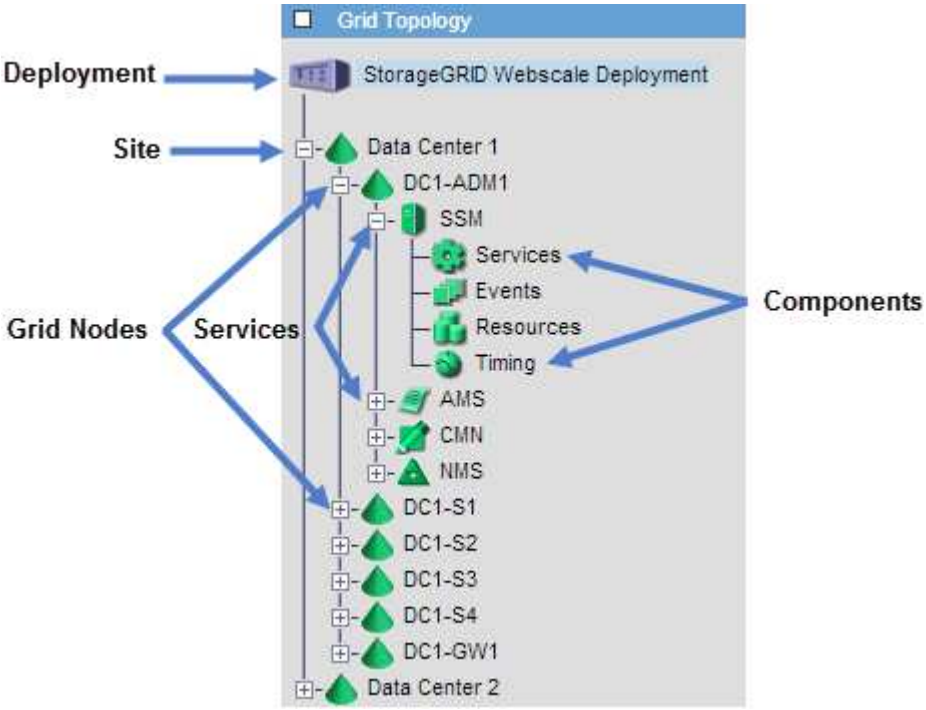
   StorageGRID tente d'envoyer un package AutoSupport au site de support NetApp . Si la tentative réussit, les valeurs **Résultat le plus récent** et **Dernière heure de réussite** dans l'onglet **Résultats** sont mises à jour. En cas de problème, la valeur **Résultat le plus récent** est mise à jour sur « Échec » et StorageGRID n'essaie pas d'envoyer à nouveau le package AutoSupport .

Après avoir envoyé un package AutoSupport déclenché par l'utilisateur, actualisez la page AutoSupport dans votre navigateur après 1 minute pour accéder aux résultats les plus récents.

Afficher l'arborescence de la topologie de la grille

L'arborescence de topologie de grille donne accès à des informations détaillées sur les éléments du système StorageGRID , notamment les sites, les nœuds de grille, les services et les composants. Dans la plupart des cas, vous n'avez besoin d'accéder à l'arborescence de la topologie de la grille que lorsque cela est indiqué dans la documentation ou lorsque vous travaillez avec le support technique.

Pour accéder à l'arborescence de topologie de grille, sélectionnez **SUPPORT** > **Outils** > **Topologie de grille**.



Pour développer ou réduire l'arborescence de la topologie de la grille, cliquez sur ⊞ ou ⊟ au niveau du site, du nœud ou du service. Pour développer ou réduire tous les éléments de l'ensemble du site ou de chaque nœud, maintenez la touche **<Ctrl>** enfoncée et cliquez.

Attributs StorageGRID

Les attributs signalent les valeurs et les statuts de nombreuses fonctions du système StorageGRID . Les 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 Grid Manager :

- **Page Nœuds** : de nombreuses valeurs affichées sur la page Nœuds sont des attributs StorageGRID . (Les métriques Prometheus sont également affichées sur les pages Nœuds.)
- **Arborescence de topologie de grille** : les valeurs d'attribut sont affichées dans l'arborescence de topologie de grille (**SUPPORT** > **Outils** > **Topologie de grille**).
- **Événements** : des événements système se produisent lorsque certains attributs enregistrent une condition

d’erreur ou de défaut pour un nœud, y compris des erreurs telles que des erreurs réseau.

Valeurs d’attribut

Les attributs sont rapportés dans la mesure du possible et sont approximativement corrects. Les mises à jour d’attributs peuvent être perdues dans certaines circonstances, comme le crash d’un service ou l’échec et la reconstruction d’un nœud de grille.

De plus, les délais de propagation peuvent ralentir la génération de rapports sur les attributs. Les valeurs mises à jour pour la plupart des attributs sont envoyées au système StorageGRID à intervalles fixes. Il peut s’écouler plusieurs minutes 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.

Examiner les mesures de support

Lors du dépannage d’un problème, vous pouvez travailler avec le support technique pour examiner les métriques et les graphiques détaillés de votre système StorageGRID .

Avant de commencer

- Vous devez être connecté au Grid Manager à l’aide d’un"navigateur Web pris en charge" .
- Tu as"autorisations d’accès spécifiques" .

À propos de cette tâche

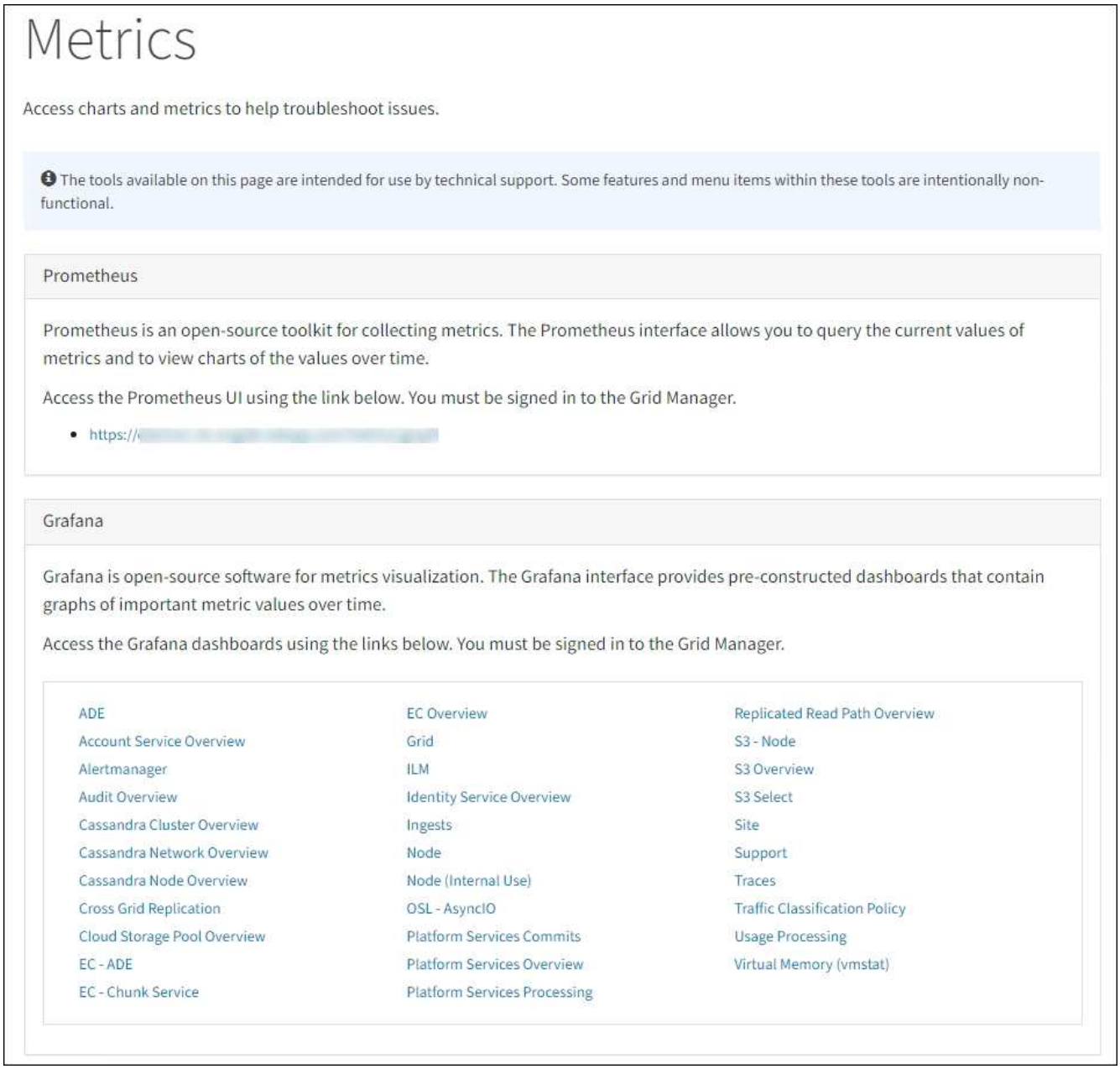
La page Métriques vous permet d’accéder aux interfaces utilisateur de Prometheus et Grafana. Prometheus est un logiciel open source de collecte de métriques. Grafana est un logiciel open source de visualisation de métriques.

> Les outils disponibles sur la page Métriques sont destinés à être utilisés par le support technique. Certaines fonctionnalités et éléments de menu de ces outils sont intentionnellement non fonctionnels et sont susceptibles d’être modifiés. Voir la liste des"métriques Prometheus couramment utilisées" .

Étapes

1. Comme indiqué par le support technique, sélectionnez **SUPPORT** > **Outils** > **Métriques**.

   Un exemple de la page Métriques est présenté ici :



2. Pour interroger les valeurs actuelles des métriques StorageGRID et afficher les graphiques des valeurs au fil du temps, cliquez sur le lien dans la section Prometheus.

   L'interface Prometheus apparaît. Vous pouvez utiliser cette interface pour exécuter des requêtes sur les métriques StorageGRID disponibles et pour représenter graphiquement les métriques StorageGRID au fil du temps.

   > Les métriques qui incluent *private* dans leurs noms sont destinées à un usage interne uniquement et sont susceptibles d'être modifiées entre les versions de StorageGRID sans préavis.

3. Pour accéder aux tableaux de bord pré-construits contenant des graphiques des métriques StorageGRID au fil du temps, cliquez sur les liens dans la section Grafana.

   L'interface Grafana pour le lien que vous avez sélectionné apparaît.

Exécuter les diagnostics

Lors du dépannage d'un problème, vous pouvez travailler avec le support technique pour exécuter des diagnostics sur votre système StorageGRID et examiner les résultats.

- "Examiner les mesures de support"
- "Métriques Prometheus couramment utilisées"

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Tu as"autorisations d'accès spécifiques" .

À propos de cette tâche

La page Diagnostics effectue un ensemble de vérifications de diagnostic sur l'état actuel de la grille. Chaque contrôle de diagnostic peut avoir l'un des trois statuts suivants :

-

Normal : Toutes les valeurs sont dans la plage normale.

- **Attention** : Une ou plusieurs valeurs sont en dehors de la plage normale.
- **Attention** : Une ou plusieurs valeurs sont significativement en dehors de la plage normale.

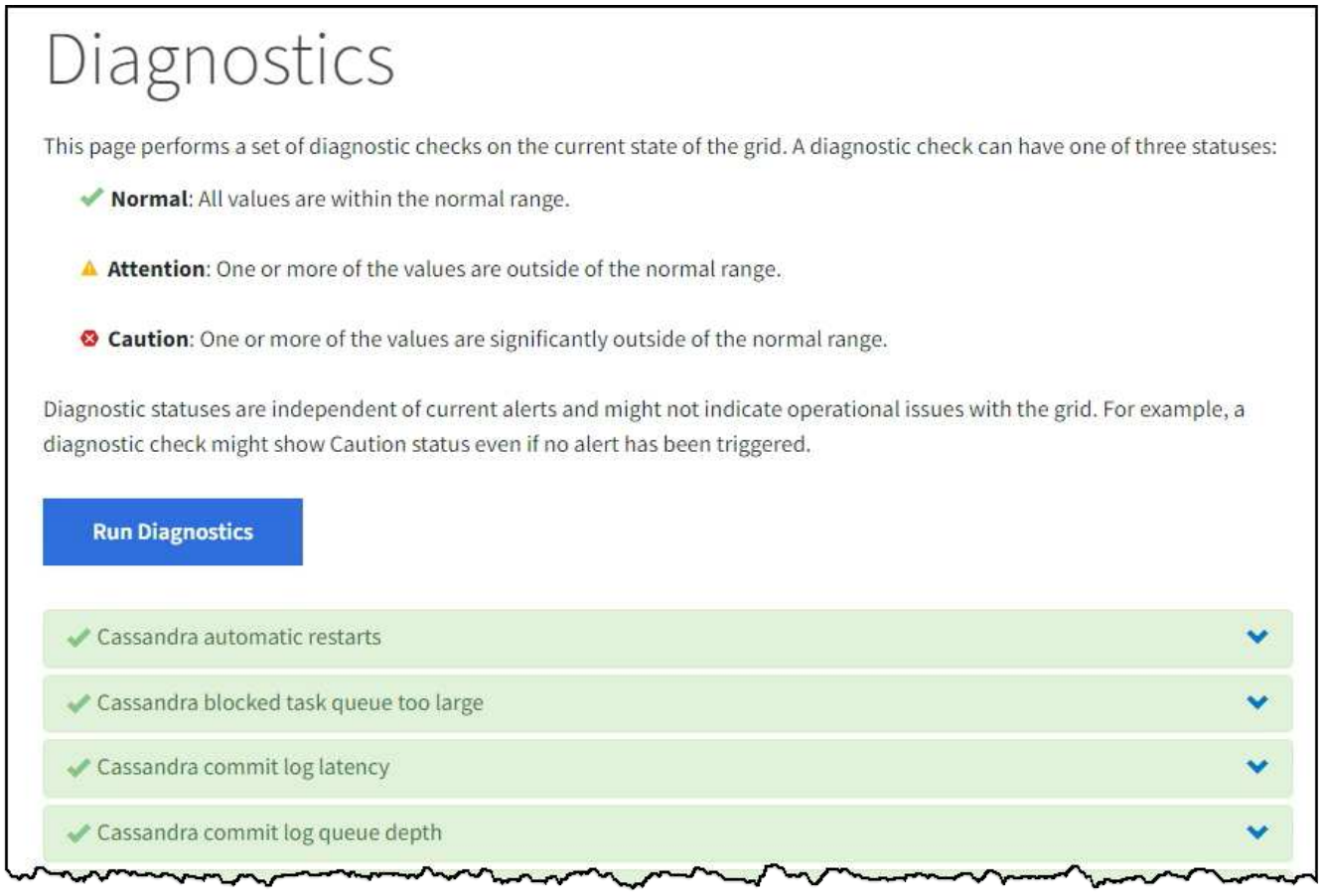
Les états de diagnostic sont indépendants des alertes actuelles et peuvent ne pas indiquer de problèmes opérationnels avec le réseau. Par exemple, un contrôle de diagnostic peut afficher le statut Attention même si aucune alerte n'a été déclenchée.

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 Normal). Au sein de chaque gravité, les résultats sont triés par ordre alphabétique.

   Dans cet exemple, tous les diagnostics ont un statut Normal.



2. Pour en savoir plus sur un diagnostic spécifique, cliquez n'importe où sur la ligne.

   Les détails sur le diagnostic et ses résultats actuels s'affichent. Les détails suivants sont répertoriés :

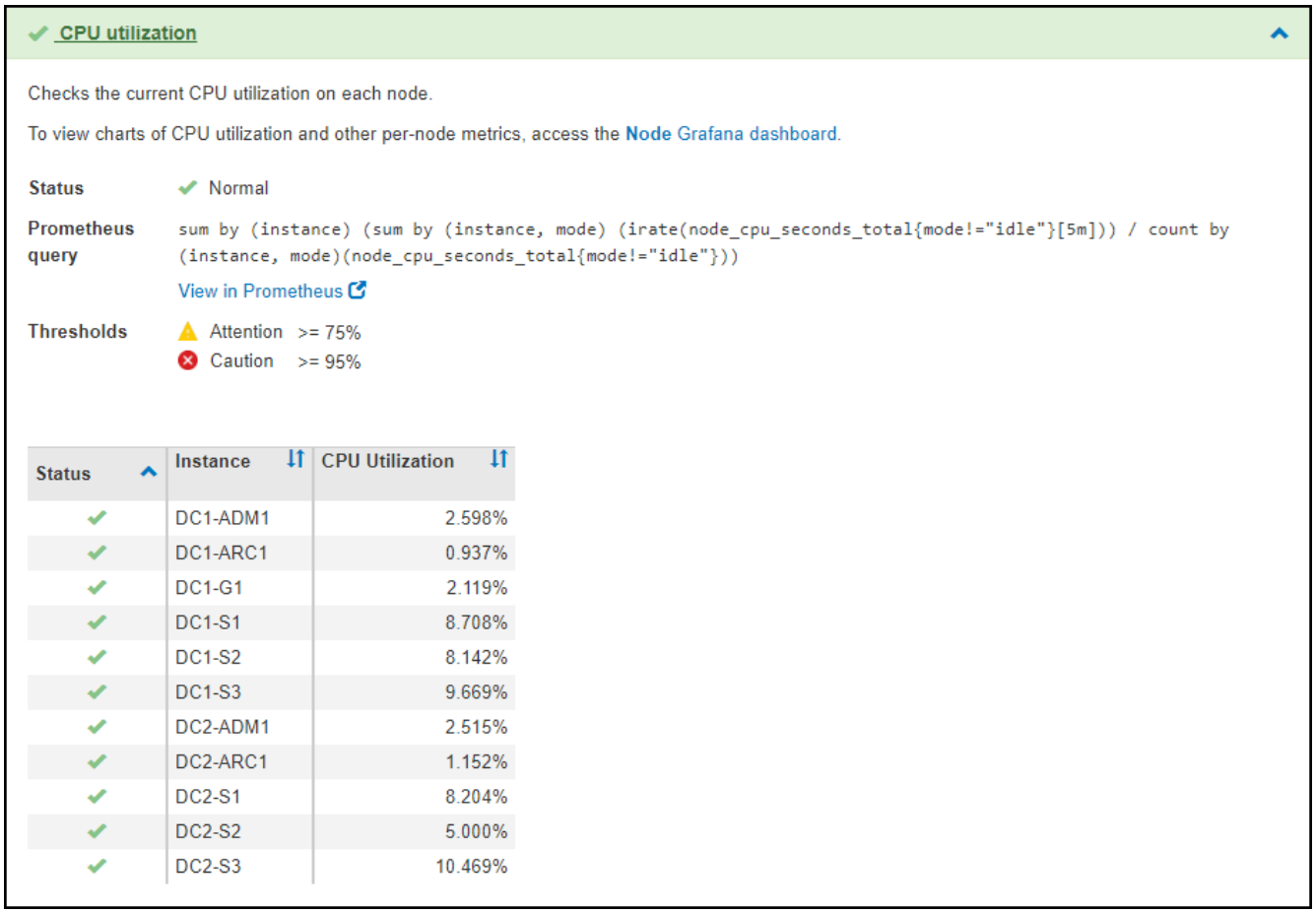
   - **Statut** : L'état actuel de ce diagnostic : Normal, Attention ou Attention.
   - **Requête Prometheus** : si elle est utilisée pour le diagnostic, l'expression Prometheus qui a été utilisée pour générer les valeurs d'état. (Une expression Prometheus n'est pas utilisée pour tous les

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** : un 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 affichée. Toutes les valeurs des nœuds sont inférieures aux seuils d'attention et de prudence, donc l'état global du diagnostic est Normal.



3. **Facultatif** : Pour voir les graphiques Grafana liés à ce diagnostic, cliquez sur le lien **Tableau de bord Grafana**.

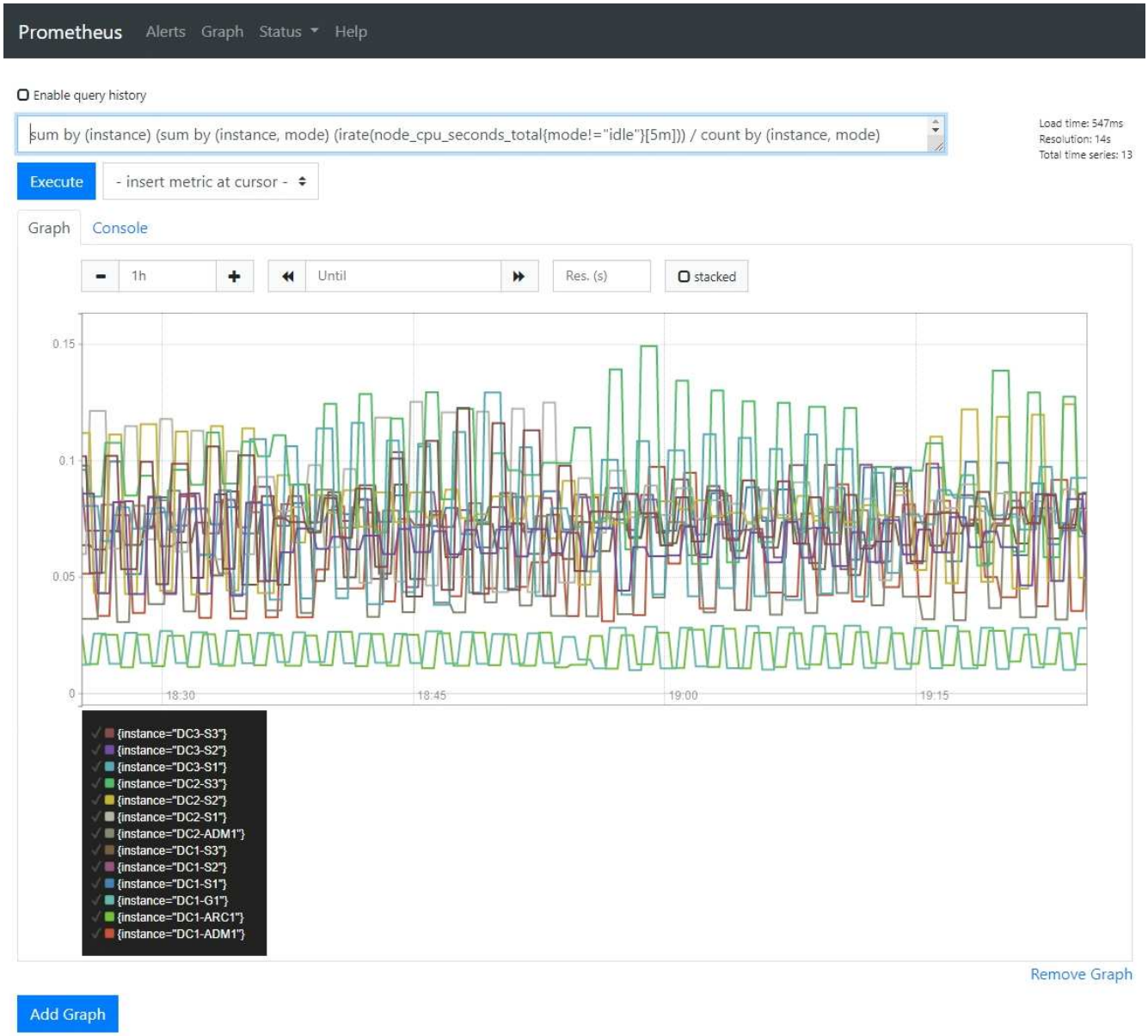
   Ce lien n'est pas affiché pour tous les diagnostics.

   Le tableau de bord Grafana associé apparaît. Dans cet exemple, le tableau de bord du nœud s'affiche, affichant l'utilisation du processeur au fil du temps pour ce nœud ainsi que d'autres graphiques Grafana pour le nœud.

   Vous pouvez également accéder aux tableaux de bord Grafana pré-construits à partir de la section Grafana de la page **SUPPORT** > **Outils** > **Métriques**.

4. **Facultatif** : Pour voir 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 apparaît.



Créer des applications de surveillance personnalisées

Vous pouvez créer des applications de surveillance et des tableaux de bord personnalisés à l'aide des mesures StorageGRID disponibles à partir de l'API Grid Management.

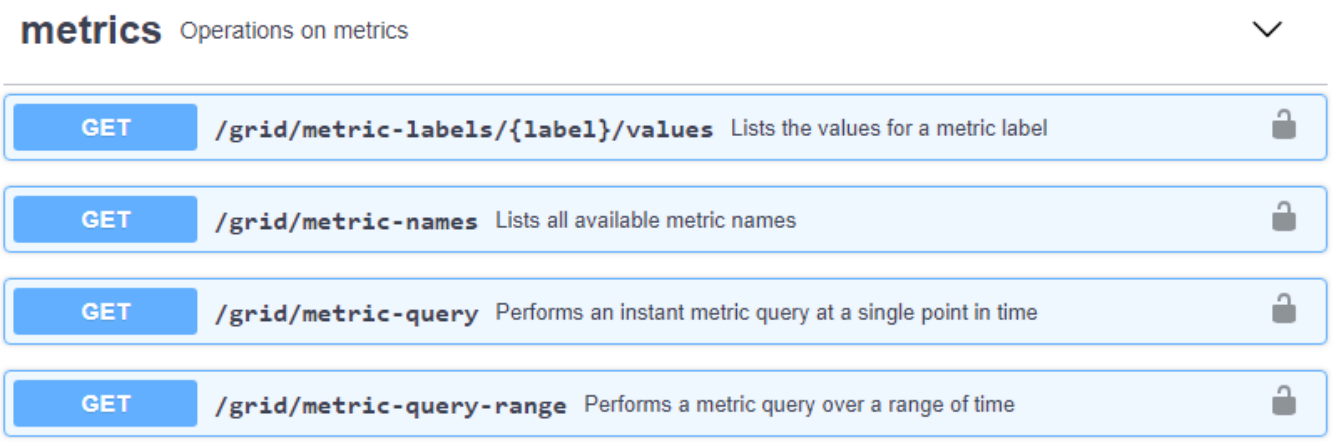
Si vous souhaitez surveiller des métriques qui ne sont pas affichées sur une page existante du Grid Manager, ou si vous souhaitez créer des tableaux de bord personnalisés pour StorageGRID, vous pouvez utiliser l'API Grid Management pour interroger les métriques StorageGRID .

Vous pouvez également accéder aux métriques Prometheus directement avec un outil de surveillance externe, tel que Grafana. L'utilisation d'un outil externe nécessite que vous téléchargiez ou génériez un certificat client administratif pour permettre à StorageGRID d'authentifier l'outil pour des raisons de sécurité. Voir le"instructions pour administrer StorageGRID" .

Pour afficher les opérations de l'API des métriques, y compris la liste complète des métriques disponibles, accédez au gestionnaire de grille. En haut de la page, sélectionnez l'icône d'aide et sélectionnez

Documentation API > métriques

.



Les détails sur la manière de mettre en œuvre une application de surveillance personnalisée dépassent le cadre de cette documentation.

Dépannage du système StorageGRID

Dépanner un système StorageGRID

Si vous rencontrez un problème lors de l'utilisation d'un système StorageGRID , reportez-vous aux conseils et instructions de cette section pour obtenir de l'aide pour déterminer et résoudre le problème.

Souvent, vous pouvez résoudre les problèmes par vous-même ; cependant, vous devrez peut-être faire appel au support technique pour résoudre certains problèmes.

Définir le problème

La première étape pour résoudre un problème est de le définir clairement.

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 clientes signalent que les objets ne peuvent pas être ingérés dans StorageGRID.
Quand le problème a-t-il commencé ?	L'ingestion d'objets a été refusée pour la première fois vers 14h50 le 8 janvier 2020.
Comment avez-vous remarqué le problème pour la première fois ?	Notifié par l'application client. J'ai également reçu des notifications d'alerte par e-mail.
Le problème survient-il systématiquement ou seulement parfois ?	Le problème persiste.

Question	Exemple de réponse
Si le problème se produit régulièrement, quelles sont les étapes qui le provoquent ?	Le problème se produit chaque fois qu'un client tente d'ingérer un objet.
Si le problème survient par intermittence, quand se produit-il ? Enregistrez les heures de chaque incident dont vous avez connaissance.	Le problème n'est pas intermittent.
Avez-vous déjà vu ce problème ? À quelle fréquence avez-vous eu ce problème dans le passé ?	C'est la première fois que je vois ce problème.

Évaluer le risque et l'impact sur le système

Après avoir défini le problème, évaluez son risque et son impact sur le système StorageGRID . Par exemple, la présence d'alertes critiques ne signifie pas nécessairement que le système ne fournit pas de services essentiels.

Ce tableau résume l'impact que l'exemple de problème a sur les opérations du système :

Question	Exemple de réponse
Le système StorageGRID peut-il ingérer du contenu ?	Non.
Les applications clientes peuvent-elles récupérer du contenu ?	Certains objets peuvent être récupérés et d'autres non.
Les données sont-elles en danger ?	Non.
La capacité à mener des affaires est-elle gravement affectée ?	Oui, car les applications clientes ne peuvent pas stocker d'objets dans le système StorageGRID et les données ne peuvent pas être récupérées de manière cohérente.

Collecter des données

Après avoir défini le problème et évalué son risque et son impact, collectez des données pour analyse. Le type de données qu'il est le plus utile de collecter dépend de la nature du problème.

Type de données à collecter	Pourquoi collecter ces données	Instructions
Créer une chronologie des changements récents	Les modifications apportées à votre système StorageGRID , à sa configuration ou à son environnement peuvent entraîner un nouveau comportement.	• Créer une chronologie des changements récents

Type de données à collecter	Pourquoi collecter ces données	Instructions
Avis sur les alertes	Les alertes peuvent vous aider à déterminer rapidement la cause première d'un problème en fournissant des indices importants sur les problèmes sous-jacents qui pourraient en être la cause. Consultez la liste des alertes actuelles pour voir si StorageGRID a identifié la cause première d'un problème pour vous. Consultez les alertes déclenchées dans le passé pour obtenir des informations supplémentaires.	• "Afficher les alertes actuelles et résolues"
Surveiller les événements	Les événements incluent toutes les erreurs système ou tous les événements de défaut pour un nœud, y compris les erreurs telles que les erreurs réseau. Surveillez les événements pour en savoir plus sur les problèmes ou pour aider au dépannage.	• "Surveiller les événements"
Identifier les tendances à l'aide de graphiques et de rapports textuels	Les tendances peuvent fournir des indices précieux sur le moment où les problèmes sont apparus pour la première fois et peuvent vous aider à comprendre à quelle vitesse les choses évoluent.	• "Utiliser des tableaux et des graphiques" • "Utiliser des rapports textuels"
Établir des lignes de base	Recueillir des informations sur les niveaux normaux de diverses valeurs opérationnelles. Ces valeurs de référence et les écarts par rapport à ces valeurs de référence peuvent fournir des indices précieux.	• Établir des lignes de base
Effectuer des tests d'ingestion et de récupération	Pour résoudre les problèmes de performances liés à l'ingestion et à la récupération, utilisez une station de travail pour stocker et récupérer des objets. Comparez les résultats avec ceux observés lors de l'utilisation de l'application cliente.	• "Surveiller les performances PUT et GET"
Examiner les messages d'audit	Consultez les messages d'audit pour suivre en détail les opérations StorageGRID . Les détails des messages d'audit peuvent être utiles pour résoudre de nombreux types de problèmes, y compris les problèmes de performances.	• "Examiner les messages d'audit"

Type de données à collecter	Pourquoi collecter ces données	Instructions
Vérifier l'emplacement des objets et l'intégrité du stockage	Si vous rencontrez des problèmes de stockage, vérifiez que les objets sont placés là où vous le souhaitez. Vérifiez l'intégrité des données d'objet sur un nœud de stockage.	• "Surveiller les opérations de vérification des objets" • "Confirmer les emplacements des données d'objet" • "Vérifier l'intégrité de l'objet"
Collecter des données pour le support technique	Le support technique peut vous demander de collecter des données ou d'examiner des informations spécifiques pour vous aider à résoudre les problèmes.	• "Collecter les fichiers journaux et les données système" • "Déclencher manuellement un package AutoSupport" • "Examiner les mesures de support"

Créer une chronologie des modifications récentes

Lorsqu'un problème survient, vous devez tenir compte de ce qui a changé récemment et du moment où ces changements se sont produits.

- Les modifications apportées à votre système StorageGRID , à sa configuration ou à son environnement peuvent entraîner un nouveau comportement.
- Une chronologie des changements peut vous aider à identifier les changements qui pourraient être responsables d'un problème et comment chaque changement pourrait avoir affecté son développement.

Créez un tableau des modifications récentes apportées à votre système qui comprend des informations sur le moment où chaque modification s'est produite et tous les détails pertinents sur la modification, tels que des informations sur ce qui se passait d'autre pendant que la modification était en cours :

L'heure du changement	Type de changement	Détails
Par exemple: • Quand avez-vous commencé la récupération du nœud ? • Quand la mise à niveau du logiciel a-t-elle été terminée ? • Avez-vous interrompu le processus ?	Ce qui s'est passé? Qu'est-ce que tu as fait?	Documentez tous les détails pertinents concernant le changement. Par exemple: • Détails des changements du réseau. • Quel correctif a été installé. • Comment les charges de travail des clients ont changé. Assurez-vous de noter si plusieurs changements se produisent en même temps. Par exemple, ce changement a-t-il été effectué alors 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 changé récemment ?
- La politique ILM a-t-elle été mise à jour ?
- La charge de travail du client a-t-elle changé ?
- L'application cliente ou son comportement a-t-il changé ?
- Avez-vous modifié les équilibreurs de charge ou ajouté ou supprimé un groupe de haute disponibilité de nœuds d'administration ou de nœuds de passerelle ?
- Des tâches ont-elles été commencées qui pourraient prendre beaucoup de temps à terminer ? Voici quelques exemples :
  - Récupération d'un nœud de stockage défaillant
  - Déclassement du nœud de stockage
- Des modifications ont-elles été apportées à l'authentification des utilisateurs, telles que l'ajout d'un locataire ou la modification de la configuration LDAP ?
- La migration des données est-elle en cours ?
- Les services de la plateforme ont-ils été récemment activés ou modifiés ?
- La conformité a-t-elle été activée récemment ?
- Des pools de stockage cloud ont-ils été ajoutés ou supprimés ?
- Des modifications ont-elles été apportées à la compression ou au cryptage du stockage ?
- Y a-t-il eu des changements dans l'infrastructure du réseau ? Par exemple, les VLAN, les routeurs ou les DNS.
- Des modifications ont-elles été apportées aux sources NTP ?
- Des modifications ont-elles été apportées aux interfaces Grid, Admin ou Client Network ?
- D'autres modifications ont-elles été apportées au système StorageGRID ou à son environnement ?

Établir des lignes de base

Vous pouvez établir des lignes de base pour votre système en enregistrant les niveaux normaux de diverses valeurs opérationnelles. À l'avenir, vous pourrez comparer les valeurs actuelles à ces lignes de base pour aider à détecter et à résoudre les valeurs anormales.

Propriété	Valeur	Comment obtenir
Consommation moyenne de stockage	Go consommés/jour Pourcentage consommé/jour	Accédez au gestionnaire de grille. Sur la page Nœuds, sélectionnez la grille entière ou un site et accédez à l'onglet Stockage. Sur le graphique Stockage utilisé - Données d'objet, recherchez une période où la ligne est assez stable. Positionnez votre curseur sur le graphique pour estimer la quantité de stockage consommée chaque jour Vous pouvez collecter ces informations pour l'ensemble du système ou pour un centre de données spécifique.
Consommation moyenne de métadonnées	Go consommés/jour Pourcentage consommé/jour	Accédez au gestionnaire de grille. Sur la page Nœuds, sélectionnez la grille entière ou un site et accédez à l'onglet Stockage. Sur le graphique Stockage utilisé - Métadonnées d'objet, recherchez une période où la ligne est assez stable. Positionnez votre curseur sur le graphique pour estimer la quantité de stockage de métadonnées consommée chaque jour Vous pouvez collecter ces informations pour l'ensemble du système ou pour un centre de données spécifique.
Taux d'opérations S3/Swift	Opérations/seconde	Dans le tableau de bord du gestionnaire de grille, sélectionnez **Performances** > **Opérations S3** ou **Performances** > **Opérations Swift**. Pour voir les taux et les nombres d'ingestion et de récupération pour un site ou un nœud spécifique, sélectionnez **NODES** > ***site ou Storage Node*** > **Objects**. Placez votre curseur sur le graphique Ingérer et récupérer pour S3.
Échec des opérations S3/Swift	Opérations	Sélectionnez **SUPPORT** > **Outils** > **Topologie de grille**. Dans l'onglet Présentation de la section Opérations API, affichez la valeur de Opérations S3 - Échec ou Opérations Swift - Échec.
Taux d'évaluation ILM	Objets/seconde	Depuis la page Nœuds, sélectionnez ***grid*** > **ILM**. Sur le graphique de la file d'attente ILM, recherchez une période où la ligne est assez stable. Placez votre curseur sur le graphique pour estimer une valeur de référence pour le **taux d'évaluation** de votre système.

Propriété	Valeur	Comment obtenir
Taux de balayage ILM	Objets/seconde	Sélectionnez **NODES** > ***grid*** > **ILM**. Sur le graphique de la file d'attente ILM, recherchez une période où la ligne est assez stable. Placez votre curseur sur le graphique pour estimer une valeur de référence pour le **taux d'analyse** pour votre système.
Objets mis en file d'attente à partir des opérations client	Objets/seconde	Sélectionnez **NODES** > ***grid*** > **ILM**. Sur le graphique de la file d'attente ILM, recherchez une période où la ligne est assez stable. Placez votre curseur sur le graphique pour estimer une valeur de référence pour **Objets mis en file d'attente (à partir des opérations client)** pour votre système.
Latence moyenne des requêtes	Millisecondes	Sélectionnez **NODES** > ***Storage Node*** > **Objects**. Dans la table Requêtes, affichez la valeur de la latence moyenne.

Analyser les données

Utilisez les informations que vous collectez pour déterminer la cause du problème et les solutions potentielles.

L'analyse dépend du problème, mais en général :

- Localisez les points de défaillance et les goulots d'étranglement à l'aide des alertes.
- Reconstruisez l'historique du problème à l'aide de l'historique des alertes et des graphiques.
- Utilisez des graphiques pour trouver des anomalies et comparer la situation problématique avec le fonctionnement normal.

Liste de contrôle des informations d'escalade

Si vous ne parvenez pas à résoudre le problème vous-même, contactez le support technique. Avant de contacter le support technique, rassemblez les informations répertoriées dans le tableau suivant pour faciliter la résolution du problème.

✔	Article	Remarques
	Énoncé du problème	Quels sont les symptômes du problème ? Quand le problème a-t-il commencé ? Cela se produit-il régulièrement ou par intermittence ? Si c'est par intermittence, à quelles heures cela s'est-il produit ? Définir le problème

✔	Article	Remarques
	Évaluation d'impact	Quelle est la gravité du problème ? Quel est l'impact sur l'application cliente ? • Le client s'est-il déjà connecté avec succès ? • Le client peut-il ingérer, récupérer et supprimer des données ?
	ID système StorageGRID	Sélectionnez **MAINTENANCE** > **Système** > **Licence**. L'ID système StorageGRID est affiché dans le cadre de la licence actuelle.
	Version du logiciel	En haut du gestionnaire de grille, sélectionnez l'icône d'aide et sélectionnez **À propos** pour voir la version de StorageGRID .
	Personnalisation	Résumez la configuration de votre système StorageGRID . Par exemple, énumérez les éléments suivants : • Le réseau utilise-t-il la compression du stockage, le cryptage du stockage ou la conformité ? • ILM crée-t-il des objets répliqués ou codés par effacement ? L'ILM assure-t-il la redondance du site ? Les règles ILM utilisent-elles les comportements d'ingestion équilibrés, stricts ou à double engagement ?
	Fichiers journaux et données système	Collectez les fichiers journaux et les données système de votre système. Sélectionnez **SUPPORT** > **Outils** > **Journaux**. Vous pouvez collecter des journaux pour l'ensemble de la grille ou pour des nœuds sélectionnés. Si vous collectez des journaux uniquement pour des nœuds sélectionnés, assurez-vous d'inclure au moins un nœud de stockage doté du service ADC. (Les trois premiers nœuds de stockage d'un site incluent le service ADC.) "Collecter les fichiers journaux et les données système"
	Informations de base	Collectez des informations de base concernant les opérations d'ingestion, les opérations de récupération et la consommation de stockage. Établir des lignes de base
	Chronologie des changements récents	Créez une chronologie qui résume tous les changements récents apportés au système ou à son environnement. Créer une chronologie des changements récents

✔	Article	Remarques
	Historique des efforts déployés pour diagnostiquer le problème	Si vous avez pris des mesures pour diagnostiquer ou résoudre le problème vous-même, assurez-vous d'enregistrer les étapes que vous avez suivies et le résultat.

Résoudre les problèmes d'objets et de stockage

Confirmer les emplacements des données d'objet

En fonction du problème, vous souhaiterez peut-être"confirmer où les données de l'objet sont stockées" . Par exemple, vous souhaiterez peut-être vérifier que la politique ILM fonctionne comme prévu et que les données d'objet sont stockées là où prévu.

Avant de commencer

- Vous devez avoir un identifiant d'objet, qui peut être l'un des suivants :
  - **UUID** : l'identifiant unique universel de l'objet. Entrez le UUID en majuscules.
  - **CBID** : l'identifiant unique de l'objet dans StorageGRID . Vous pouvez obtenir le CBID d'un objet à partir du journal d'audit. Entrez le CBID en majuscules.
  - **Seau S3 et clé d'objet** : Lorsqu'un objet est ingéré via le"Interface S3" , l'application cliente utilise une combinaison de clés de bucket et d'objet pour stocker et identifier l'objet.

Étapes

1. Sélectionnez **ILM** > **Recherche de métadonnées d'objet**.
2. Tapez l'identifiant de l'objet dans le champ **Identifiant**.

   Vous pouvez saisir un UUID, un CBID, une clé de bucket/objet S3 ou un nom de conteneur/objet Swift.

3. Si vous souhaitez rechercher une version spécifique de l'objet, saisissez l'ID de version (facultatif).

4. Sélectionnez **Rechercher**.

   Le"résultats de la recherche de métadonnées d'objet" apparaître. Cette page répertorie les types d'informations suivants :

   - 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 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 clé-valeur de métadonnées utilisateur personnalisées associées à l'objet.
- Pour les objets S3, toutes les paires clé-valeur de balise d'objet associées à l'objet.
- Pour les copies d'objets répliquées, l'emplacement de stockage actuel de chaque copie.
- Pour les copies d'objets codées par effacement, l'emplacement de stockage actuel de chaque fragment.
- Pour les copies d'objet dans un pool de stockage Cloud, l'emplacement de l'objet, y compris le nom du bucket externe et l'identifiant unique de l'objet.
- Pour les objets segmentés et les objets en plusieurs parties, une liste de segments d'objet comprenant les identifiants de segment et les tailles de données. Pour les objets comportant plus de 100 segments, seuls les 100 premiers segments sont affichés.
- Toutes les métadonnées d'objet au format de stockage interne non traité. Ces métadonnées brutes incluent des métadonnées système internes dont la persistance d'une version à l'autre n'est pas garantie.

L'exemple suivant montre 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": "0x8823DE7EC7C10416",
    "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
    "PPTH": "source",
    "META": {
        "BASE": {
            "PAWS": "2",
```


Pannes du magasin d’objets (volume de stockage)

Le stockage sous-jacent sur 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 du magasin d’objets pour chaque nœud de stockage. Les magasins d’objets sont affichés en bas de la page **NODES** > ***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

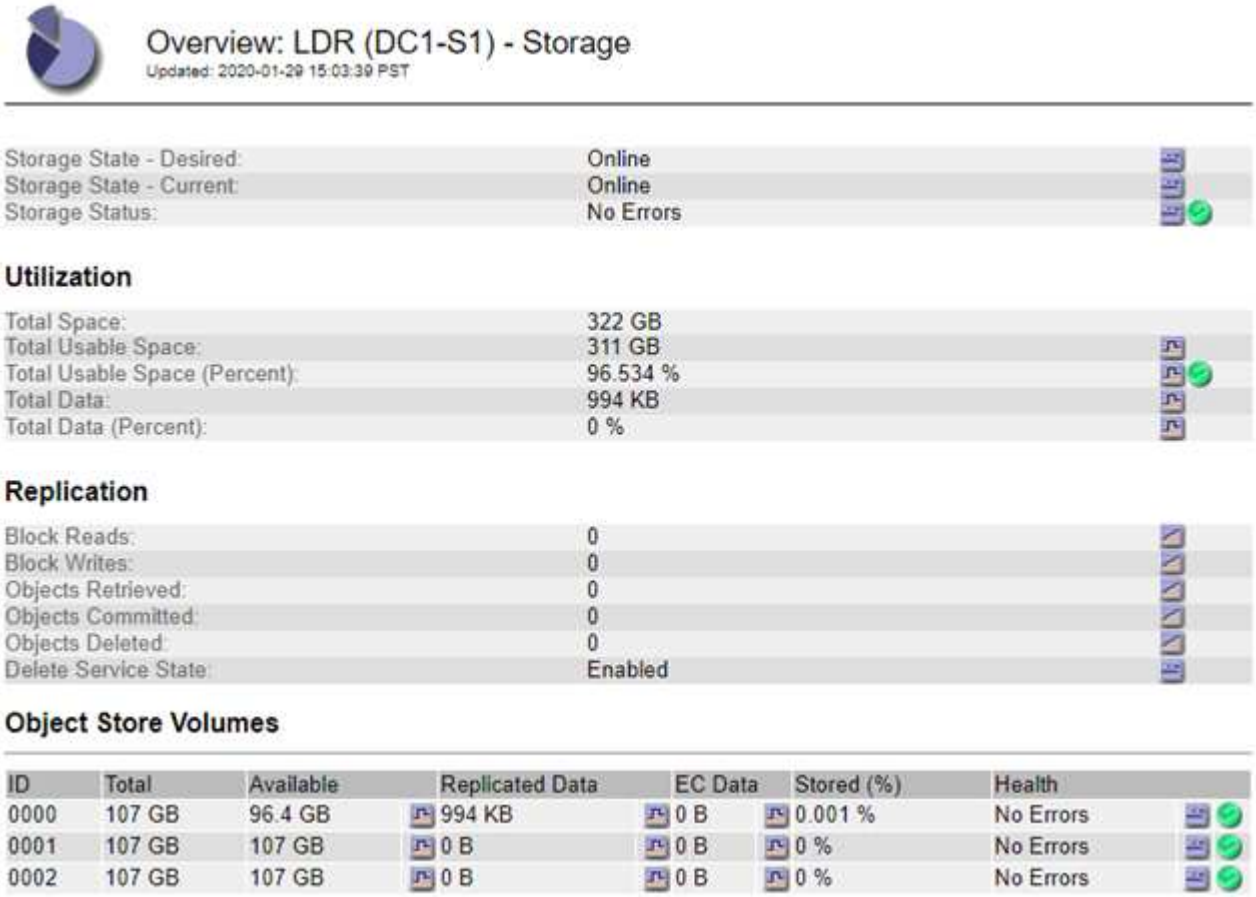
Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.73 GB	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	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 voir plus"détails sur chaque nœud de stockage" , suivez ces étapes :

1. Sélectionnez **SUPPORT** > **Outils** > **Topologie de grille**.
2. Sélectionnez ***site*** > ***Nœud de stockage*** > **LDR** > **Stockage** > **Aperçu** > **Principal**.



Selon la nature de la panne, les défauts d'un volume de stockage peuvent se refléter dans"alertes de volume de stockage" . Si un volume de stockage tombe en panne, vous devez réparer le volume de stockage défaillant pour restaurer le nœud de stockage à toutes ses fonctionnalités dès que possible. Si nécessaire, vous pouvez aller dans l'onglet **Configuration** et"placer le nœud de stockage dans un état de lecture seule" afin que le système StorageGRID puisse l'utiliser pour la récupération des données pendant que vous vous préparez à une récupération complète du serveur.

Vérifier l'intégrité de l'objet

Le système StorageGRID vérifie l'intégrité des données d'objet sur les nœuds de stockage, en recherchant les objets corrompus et manquants.

Il existe deux processus de vérification : la vérification en arrière-plan et la vérification de l'existence de l'objet (anciennement appelée vérification au premier plan). Ils travaillent ensemble pour garantir l'intégrité des données. La vérification en arrière-plan s'exécute automatiquement et vérifie en permanence l'exactitude des données de l'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) des 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 les copies corrompues des données d'objet et tente automatiquement de réparer tous les problèmes qu'il détecte.

La vérification en arrière-plan vérifie l'intégrité des objets répliqués et des objets codés par effacement, comme suit :

- **Objets répliqués** : si le processus de vérification en arrière-plan détecte un objet répliqué corrompu, la copie corrompue est supprimée de son emplacement et mise en quarantaine ailleurs sur le nœud de stockage. Ensuite, une nouvelle copie non corrompue est générée et placée pour satisfaire les politiques ILM actives. La nouvelle copie peut ne pas être placée sur le nœud de stockage qui a été utilisé pour la copie d'origine.

> Les données d'objet corrompues sont mises en quarantaine plutôt que supprimées du système, de sorte qu'elles restent accessibles. Pour plus d'informations sur l'accès aux données des objets mis en quarantaine, contactez le support technique.

- **Objets codés par effacement** : si le processus de vérification en arrière-plan détecte qu'un fragment d'un objet codé par effacement est corrompu, StorageGRID tente automatiquement de reconstruire le fragment manquant en place sur le même nœud de stockage, en utilisant les fragments de données et de parité restants. Si le fragment corrompu ne peut pas être reconstruit, une tentative est effectuée pour récupérer une autre copie de l'objet. Si la récupération réussit, une évaluation ILM est effectuée pour créer une copie de remplacement de l'objet codé par effacement.

  Le processus de vérification en arrière-plan vérifie les objets sur les nœuds de stockage uniquement. Il 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 rythme continu conçu pour ne pas interférer avec les activités ordinaires du système. La vérification des antécédents ne peut pas être arrêtée. Cependant, vous pouvez augmenter le taux de vérification en arrière-plan pour vérifier plus rapidement le contenu d'un nœud de stockage si vous suspectez 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'identification de l'objet), l'alerte **Objet corrompu non identifié détecté** est déclenchée.

Si la vérification en arrière-plan ne peut pas remplacer un objet corrompu car elle 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 inquiétudes concernant l'intégrité des données.

Avant de commencer

- Vous devez être connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Tu as"autorisations d'accès spécifiques" .

À propos de cette 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

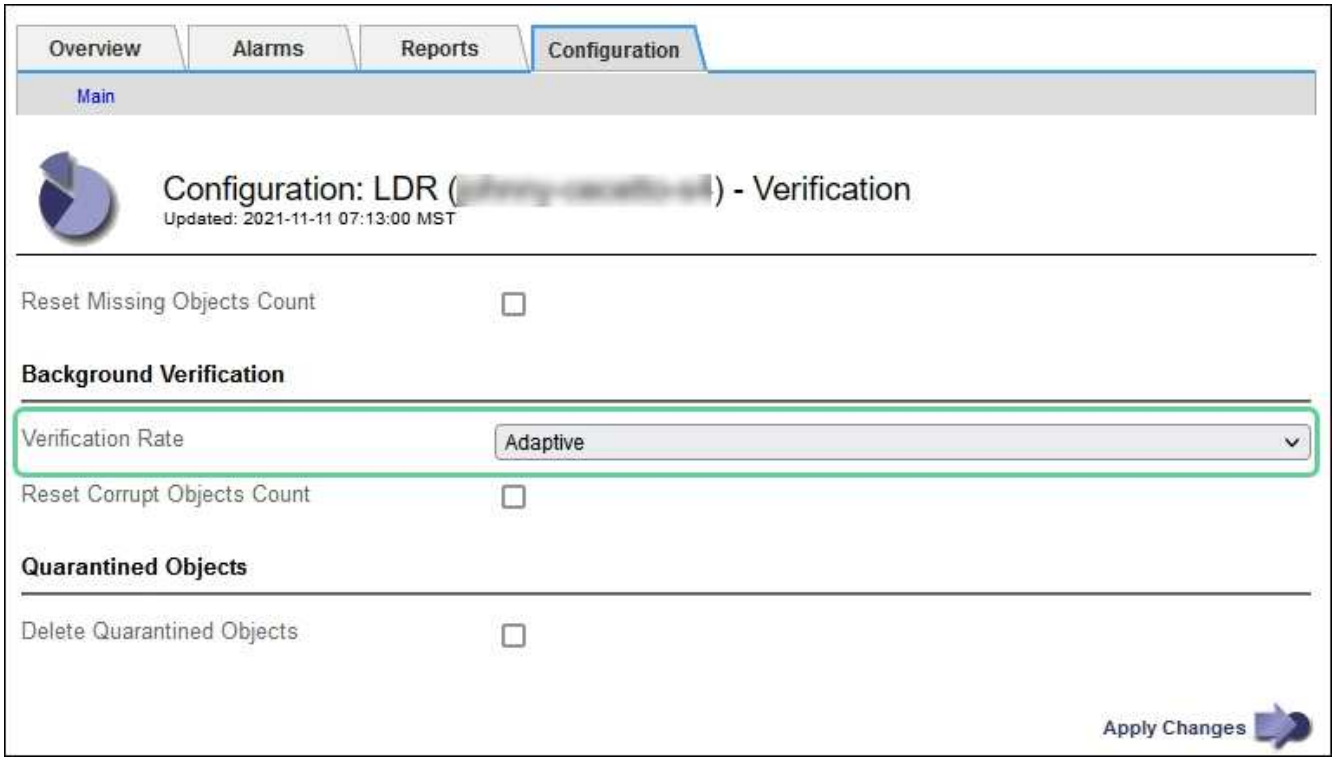
(selon la première valeur dépassée).

- Élevé : la vérification du stockage se déroule rapidement, à un rythme qui peut ralentir les activités ordinaires du système.

Utilisez le taux de vérification élevé uniquement lorsque vous suspectez qu'une panne matérielle ou logicielle a pu corrompre les données de l'objet. Une fois la vérification d'arrière-plan haute priorité terminée, le taux de vérification est automatiquement réinitialisé sur Adaptatif.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **Topologie de grille**.
2. Sélectionnez ***Nœud de stockage*** > **LDR** > **Vérification**.
3. Sélectionnez **Configuration** > **Principal**.
4. Accédez à **LDR** > **Vérification** > **Configuration** > **Principal**.
5. Sous Vérification en arrière-plan, sélectionnez **Taux de vérification** > **Élevé** ou **Taux de vérification** > **Adaptatif**.



6. Cliquez sur **Appliquer les modifications**.
7. Surveillez les résultats de la vérification en arrière-plan pour les objets répliqués.
   a. Accédez à **NODES** > ***Storage Node*** > **Objects**.
   b. Dans la section Vérification, surveillez les valeurs pour **Objets corrompus** et **Objets corrompus non identifiés**.

      Si la vérification en arrière-plan détecte des données d'objet répliquées corrompues, la mesure **Objets corrompus** est incrémentée et StorageGRID tente d'extraire l'identifiant d'objet des données, comme suit :

      - Si l'identifiant de l'objet peut être extrait, StorageGRID crée automatiquement une nouvelle copie des données de l'objet. La nouvelle copie peut être effectuée n'importe où dans le système

StorageGRID qui satisfait aux politiques 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 répliquées corrompues sont détectées, contactez le support technique pour déterminer la cause première de la corruption.

8. Surveillez les résultats de la vérification en arrière-plan pour les objets codés par 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 récupère en reconstruisant le fragment corrompu en place sur le même nœud de stockage.

   a. Sélectionnez **SUPPORT** > **Outils** > **Topologie de grille**.
   b. Sélectionnez ***Nœud de stockage*** > **LDR** > **Codage d'effacement**.
   c. Dans le tableau Résultats de vérification, surveillez l'attribut Fragments corrompus détectés (ECCD).

9. Une fois les objets corrompus restaurés automatiquement par le système StorageGRID , réinitialisez le nombre d'objets corrompus.
   a. Sélectionnez **SUPPORT** > **Outils** > **Topologie de grille**.
   b. Sélectionnez ***Nœud de stockage*** > **LDR** > **Vérification** > **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 souhaiter accéder aux objets mis en quarantaine pour aider à déboguer le problème sous-jacent ou pour tenter de récupérer des données.

    a. Sélectionnez **SUPPORT** > **Outils** > **Topologie de grille**.
    b. Sélectionnez ***Nœud de stockage*** > **LDR** > **Vérification** > **Configuration**.
    c. Sélectionnez **Supprimer les objets mis en quarantaine**.
    d. Sélectionnez **Appliquer les modifications**.

Qu'est-ce que la vérification de l'existence d'un objet ?

La vérification de l'existence d'un objet vérifie si toutes les copies répliquées attendues des objets et des fragments codés par effacement existent sur un nœud de stockage. La vérification de l'existence d'un objet ne vérifie pas les données de l'objet lui-même (la vérification en arrière-plan le fait) ; au lieu de cela, elle fournit un moyen de vérifier l'intégrité des périphériques de stockage, en particulier si un problème matériel récent a pu affecter l'intégrité des données.

Contrairement à la vérification en arrière-plan, qui se produit automatiquement, vous devez démarrer manuellement une tâche de vérification de l'existence d'un objet.

La vérification de l'existence des objets lit les métadonnées de chaque objet stocké dans StorageGRID et vérifie l'existence des copies d'objets répliquées et des fragments d'objets codés par effacement. Toute donnée manquante est traitée comme suit :

- **Copies répliquées** : si une copie des données d'objet répliquées est manquante, StorageGRID tente

automatiquement de remplacer la copie à partir d'une copie stockée ailleurs dans le système. Le nœud de stockage exécute une copie existante via une évaluation ILM, qui déterminera 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 satisfaire les politiques 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 en place sur le même nœud de stockage à l'aide des fragments restants. Si le fragment manquant ne peut pas être reconstruit (parce que trop de fragments ont été perdus), ILM tente de trouver une autre copie de l'objet, qu'il peut utiliser pour générer un nouveau fragment codé par effacement.

Exécuter la vérification de l'existence de l'objet

Vous créez et exécutez une tâche de vérification de l'existence d'un objet à la fois. Lorsque vous créez une tâche, vous sélectionnez les nœuds de stockage et les volumes que vous souhaitez vérifier. Vous sélectionnez également la consistance du travail.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"Autorisation d'accès de maintenance ou root" .
- Vous avez vérifié que les nœuds de stockage que vous souhaitez vérifier sont en ligne. Sélectionnez **NODES** pour afficher le tableau des nœuds. Assurez-vous qu'aucune icône d'alerte n'apparaît à côté du nom du nœud pour les nœuds que vous souhaitez vérifier.
- Vous avez vérifié que les procédures suivantes ne sont **pas** en cours d'exécution sur les nœuds que vous souhaitez vérifier :
  - Extension du réseau pour ajouter un nœud de stockage
  - Mise hors service du nœud de stockage
  - Récupération d'un volume de stockage défaillant
  - Récupération d'un nœud de stockage avec un lecteur système défaillant
  - Rééquilibrage de la CE
  - Clonage de nœud d'appareil

La vérification de l'existence de l'objet ne fournit pas d'informations utiles pendant que ces procédures sont en cours.

À propos de cette 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 de l'existence de l'objet**.
2. Sélectionnez **Créer un travail**. L'assistant Créer une tâche de vérification de l'existence d'un objet s'affiche.
3. Sélectionnez les nœuds contenant les volumes que vous souhaitez vérifier. Pour sélectionner tous les nœuds en ligne, cochez la case **Nom du nœud** dans l'en-tête de la colonne.

   Vous pouvez rechercher par nom de nœud ou par site.

Vous ne pouvez pas sélectionner des nœuds qui ne sont pas connectés au réseau.

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 de volume de stockage ou du nom du nœud.

   Pour sélectionner tous les volumes pour chaque nœud sélectionné, cochez la case **Volume de stockage** dans l'en-tête de colonne.

6. Sélectionnez **Continuer**.
7. Sélectionnez la consistance pour le travail.

   La cohérence détermine le nombre de copies de métadonnées d'objet utilisées pour la vérification de l'existence de l'objet.

   - **Site fort** : Deux copies de métadonnées sur un seul site.
   - **Strong-global** : Deux copies de métadonnées sur chaque site.
   - **Tous** (par défaut) : les trois copies de métadonnées sur chaque site.

     Pour plus d'informations sur la cohérence, consultez les descriptions dans l'assistant.

8. Sélectionnez **Continuer**.
9. Vérifiez et révisez vos sélections. Vous pouvez sélectionner **Précédent** pour accéder à une étape précédente de l'assistant afin de mettre à jour vos sélections.

   Une tâche de vérification de l'existence d'un objet est générée et s'exécute jusqu'à ce que l'un des événements suivants se produise :

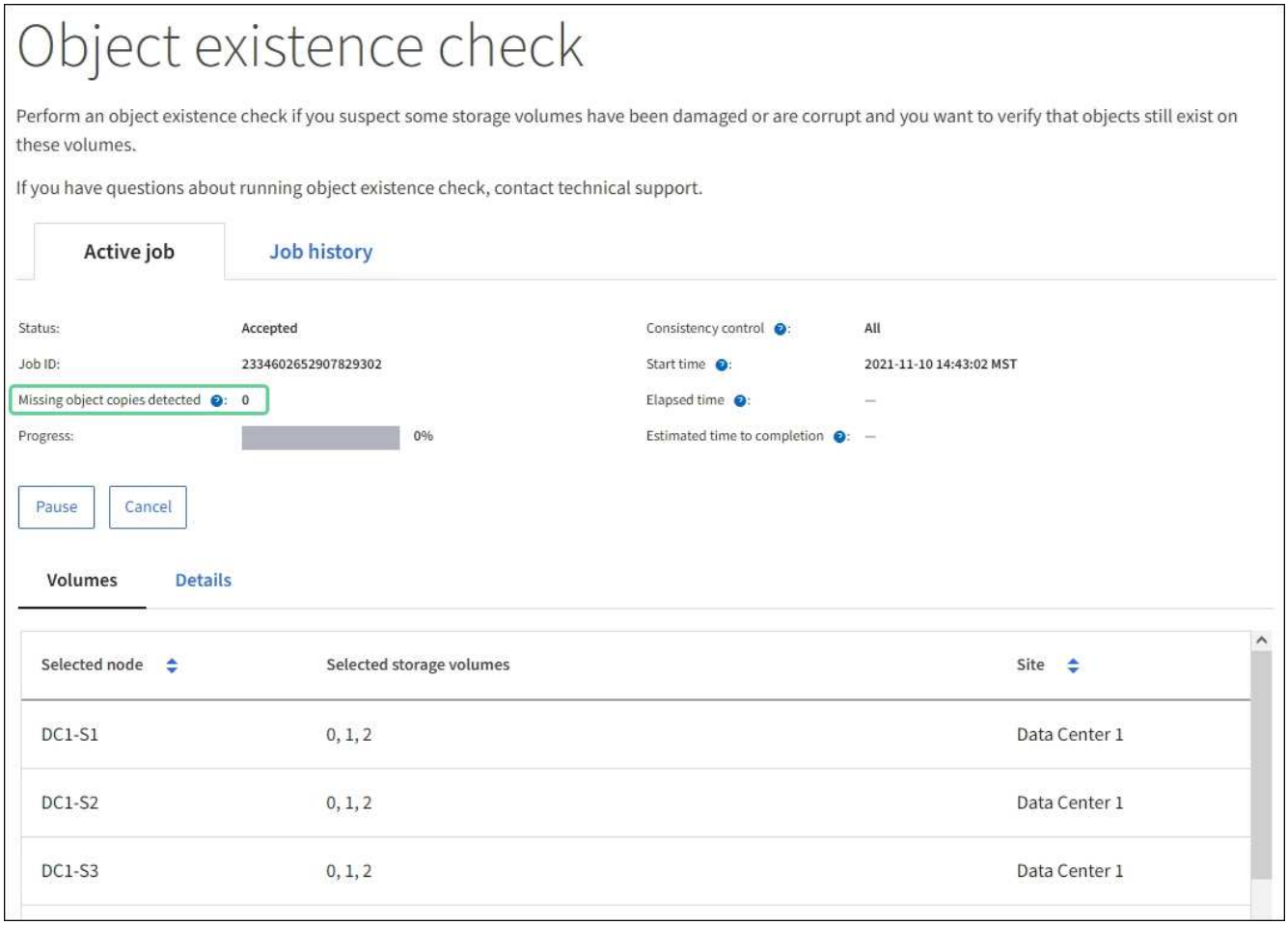
   - Le travail est terminé.
   - Vous mettez en pause ou annulez le travail. Vous pouvez reprendre un travail que vous avez suspendu, mais vous ne pouvez pas reprendre un travail que vous avez annulé.
   - Le travail stagne. L'alerte **La vérification de l'existence de l'objet est bloquée** est déclenchée. Suivez les actions correctives spécifiées pour l'alerte.
   - Le travail échoue. L'alerte **La vérification de l'existence de l'objet a échoué** est déclenchée. Suivez les actions correctives spécifiées pour l'alerte.
   - Un message « Service indisponible » ou « Erreur interne du serveur » s'affiche. Après une minute, actualisez la page pour continuer à surveiller le travail.

   > Si nécessaire, vous pouvez quitter la page de vérification de l'existence de l'objet et y revenir pour continuer à surveiller le travail.

10. Pendant l'exécution du travail, affichez l'onglet **Tâche active** et notez la valeur de Copies d'objets manquantes détectées.

    Cette valeur représente le nombre total de copies manquantes d'objets répliqués et d'objets codés par effacement avec un ou plusieurs fragments manquants.

    Si le nombre de copies d'objets manquants détectées est supérieur à 100, il peut y avoir un problème avec le stockage du nœud de stockage.



11. Une fois le travail terminé, effectuez les actions supplémentaires requises :
    - Si le nombre de copies d'objets manquantes détectées est nul, aucun problème n'a été détecté. Aucune action n'est requise.
    - Si le nombre de copies d'objets manquantes détectées est supérieur à zéro et que l'alerte **Objets perdus** n'a pas été déclenchée, alors toutes les copies manquantes ont été réparées par le système. Vérifiez que tous les problèmes matériels ont été corrigés pour éviter de futurs dommages aux copies d'objets.
    - Si le nombre de copies d'objets manquantes détectées est supérieur à zéro et que l'alerte **Objets perdus** a été déclenchée, l'intégrité des données peut être affectée. Contactez le support technique.
    - Vous pouvez enquêter sur les copies d'objets perdues en utilisant grep pour extraire les messages d'audit LLST : `grep LLST audit_file_name` .

      Cette procédure est similaire à celle pour"enquête sur les objets perdus" , bien que pour les copies d'objets, vous recherchez `LLST` au lieu de `OLST` .

12. Si vous avez sélectionné la cohérence Strong-Site ou Strong-Global pour le travail, attendez environ trois semaines pour la cohérence des métadonnées, puis réexécutez 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 la tâche, la réexécution de la tâche peut effacer les copies d'objets manquantes signalées par erreur ou entraîner la vérification de copies d'objets supplémentaires si elles ont été manquées.

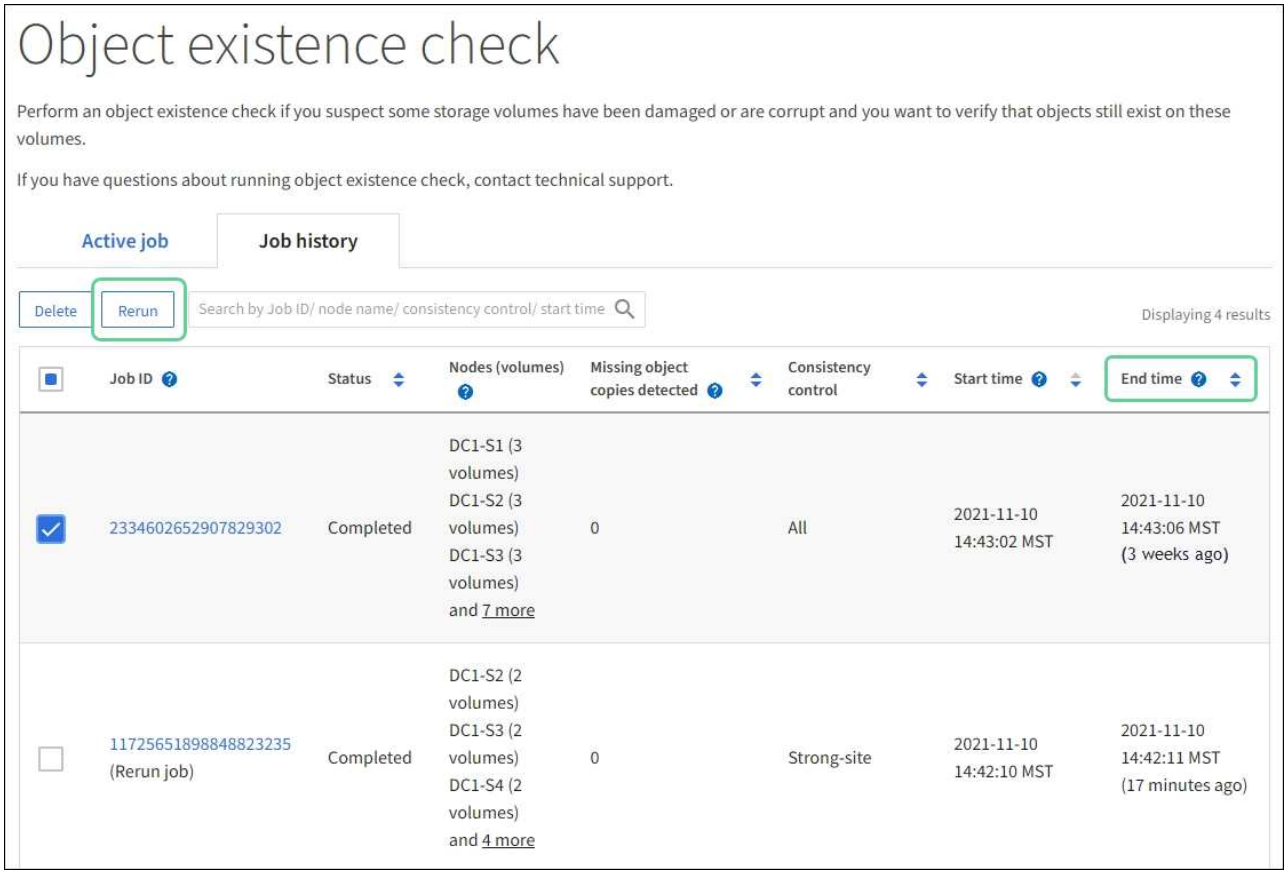
    a. Sélectionnez **MAINTENANCE** > **Vérification de l'existence de l'objet** > **Historique des tâches**.

b. Déterminer les tâches prêtes à être réexécutées :

   i. Consultez la colonne **Heure de fin** pour déterminer quelles tâches ont été exécutées il y a plus de trois semaines.

   ii. Pour ces tâches, scannez la colonne de contrôle de cohérence pour strong-site ou strong-global.

c. Cochez la case correspondant à chaque tâche que vous souhaitez réexécuter, puis sélectionnez **Réexécuter**.



d. Dans l'assistant de réexécution des tâches, vérifiez les nœuds et les volumes sélectionnés ainsi que la cohérence.

e. Lorsque vous êtes prêt à réexécuter les tâches, sélectionnez **Réexécuter**.

L'onglet Travail actif apparaît. Tous les travaux que vous avez sélectionnés sont réexécutés comme un seul travail avec une cohérence de site forte. Un champ **Tâches associées** dans la section Détails répertorie les identifiants de tâche pour les tâches d'origine.

Après avoir terminé

Si vous avez encore des inquiétudes concernant l'intégrité des données, accédez à **SUPPORT** > **Outils** > **Topologie de grille** > ***site*** > ***Nœud de stockage*** > **LDR** > **Vérification** > **Configuration** > **Principal** 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 tous les problèmes qu'elle détecte. Trouver et réparer les problèmes potentiels le plus rapidement possible réduit le risque de perte de données.

Dépannage de l'alerte S3 PUT : taille de l'objet trop grande

L'alerte de taille d'objet S3 PUT trop grande est déclenchée si un locataire tente une opération PutObject non multipartite qui dépasse la limite de taille S3 de 5 Gio.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Tu as"autorisations d'accès spécifiques" .

Déterminez quels locataires utilisent des objets supérieurs à 5 Gio, afin de pouvoir les avertir.

Étapes

1. Accédez à **CONFIGURATION** > **Surveillance** > **Serveur d'audit et syslog**.
2. Si les écritures du client sont normales, accédez au journal d'audit :

   a. Entrer `ssh admin@primary_Admin_Node_IP`

   b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

   c. Entrez la commande suivante pour passer en root : `su -`

   d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

   Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#` .

   e. Accédez au répertoire dans lequel se trouvent les journaux d'audit.

   Le répertoire du journal d'audit et les nœuds applicables dépendent de vos paramètres de destination d'audit.

Option	Destination
Nœuds locaux (par défaut)	`/var/local/log/localaudit.log`
Nœuds d'administration/nœuds locaux	• Nœuds d'administration (principaux et non principaux) : `/var/local/audit/export/audit.log` • Tous les nœuds : Le `/var/local/log/localaudit.log` le fichier est généralement vide ou manquant dans ce mode.
Serveur syslog externe	`/var/local/log/localaudit.log`

   En fonction des paramètres de destination de votre audit, saisissez : `cd /var/local/log` ou `/var/local/audit/export/`

   Pour en savoir plus, consultez"Sélectionner les destinations des informations d'audit" .

   f. Identifiez les locataires qui utilisent des objets supérieurs à 5 Gio.

      i. Entrer `zgrep SPUT * | egrep "CSIZ\(UI64\):([5-9]|[1-9][0-9]+)[0-9]{9}"`

      ii. Pour chaque message d'audit dans les résultats, regardez `S3AI` champ pour déterminer l'ID du compte locataire. Utilisez les autres champs du message pour déterminer quelle adresse IP a été utilisée par le client, le bucket et l'objet :

Code	Description
SAIP	IP source
S3AI	ID du locataire
S3BK	Seau
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):"933908492661540043 43"][SACC(CS
TR):"bhavna"][S3AK(CSTR):"06OX85M40Q90Y280B7YT"][SUSR(CSTR):"urn:sgws:id
entity::933908492661540043 43:root"][SBAI(CSTR):"933908492661540043 43"][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 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 pour le nœud de stockage dans l'alerte. Précisez 15 minutes avant et après l'alerte.

   b. Extrayez le fichier et accédez à `bycast.log` :

      ```
      /GID<grid_id>_<time_stamp>/<site_node>/<time_stamp>/grid/bycast.log
      ```

   c. Rechercher dans le journal pour `method=PUT` et identifier 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. Informez les locataires que la taille maximale de PutObject est de 5 Gio et qu'ils doivent utiliser des téléchargements en plusieurs parties pour les objets supérieurs à 5 Gio.

5. Ignorez l’alerte pendant une semaine si l’application a été modifiée.

Résoudre les problèmes de données d’objets perdues ou manquantes

Résoudre les problèmes de données d’objets perdues ou manquantes

Les objets peuvent être récupérés pour plusieurs raisons, notamment les demandes de lecture à partir d’une application cliente, les vérifications en arrière-plan des données d’objet répliquées, les réévaluations ILM et la restauration des données d’objet lors de la récupération d’un nœud de stockage.

Le système StorageGRID utilise les informations de localisation dans les métadonnées d’un objet pour déterminer à partir de quel emplacement récupérer l’objet. Si aucune copie de l’objet n’est trouvée à l’emplacement prévu, le système tente de récupérer une autre copie de l’objet ailleurs dans le système, en supposant que la politique ILM contient une règle permettant de créer deux ou plusieurs copies de l’objet.

Si cette récupération réussit, le système StorageGRID remplace la copie manquante de l’objet. Dans le cas contraire, 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 à code d’effacement, si une copie ne peut pas être récupérée à partir de l’emplacement prévu, l’attribut Copies corrompues détectées (ECOR) est incrémenté de un avant qu’une tentative de récupération d’une copie à partir d’un autre emplacement ne soit effectuée. 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 toujours exister dans un nœud de stockage hors ligne ou actuellement indisponible. Voir "Enquêter sur les objets perdus" .

Dans le cas où les données de l’objet sans copies sont perdues, il n’existe aucune solution de récupération. Cependant, vous devez réinitialiser le compteur d’objets perdus pour éviter que les objets perdus connus ne masquent les nouveaux objets perdus. Voir "Réinitialiser le nombre d’objets perdus et manquants" .

Enquêter sur les objets perdus

Lorsque l’alerte **Objets perdus** est déclenchée, vous devez enquêter immédiatement. Collectez des informations sur les objets concernés et contactez le support technique.

Avant de commencer

- Vous devez être connecté au Grid Manager à l’aide d’un"navigateur Web pris en charge" .
- Tu as"autorisations d’accès spécifiques" .
- Vous devez avoir le `Passwords.txt` déposer.

À propos de cette tâche

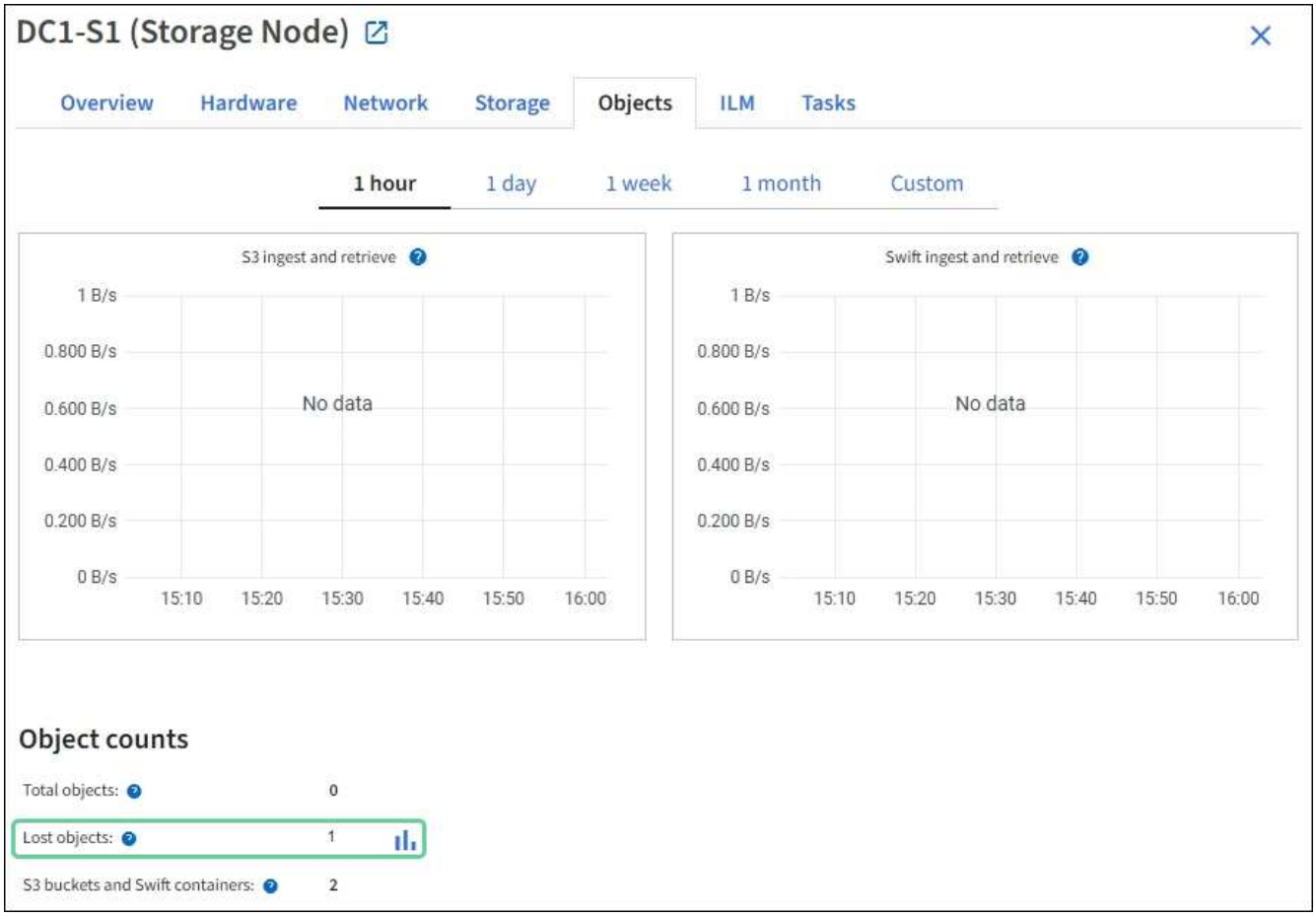
L’alerte **Objets perdus** indique que StorageGRID estime qu’il n’existe aucune copie d’un objet dans la grille. Les données ont peut-être été définitivement perdues.

Enquêtez immédiatement sur les alertes d’objets perdus. Vous devrez peut-être prendre des mesures pour éviter toute perte de données supplémentaire. Dans certains cas, vous pourrez peut-être restaurer un objet perdu si vous agissez rapidement.

Étapes

1. Sélectionnez **NODES**.
2. Sélectionnez ***Nœud de stockage*** > **Objets**.
3. Consultez le nombre d'objets perdus affiché dans le tableau Nombre d'objets.

   Ce nombre indique le nombre total d'objets que ce nœud de grille détecte comme manquants dans l'ensemble du système StorageGRID . La valeur est la somme des compteurs d'objets perdus du composant de magasin de données dans les services LDR et DDS.



4. À partir d'un nœud d'administration,"accéder 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 de grille :
      i. Entrez la commande suivante : `ssh admin@grid_node_IP`
      ii. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
      iii. Entrez la commande suivante pour passer en root : `su -`
      iv. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer. 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.

      Le répertoire du journal d'audit et les nœuds applicables dépendent de vos paramètres de destination d'audit.

Option	Destination
Nœuds locaux (par défaut)	`/var/local/log/localaudit.log`
Nœuds d'administration/nœuds locaux	• Nœuds d'administration (principaux et non principaux) : `/var/local/audit/export/audit.log` • Tous les nœuds : Le `/var/local/log/localaudit.log` le fichier est généralement vide ou manquant dans ce mode.
Serveur syslog externe	`/var/local/log/localaudit.log`

En fonction des paramètres de destination de votre audit, saisissez : `cd /var/local/log` ou `/var/local/audit/export/`

Pour en savoir plus, consultez"Sélectionner les destinations des informations d'audit" .

c. Utilisez grep pour extraire les messages d'audit d'objet perdu (OLST). Entrer: `grep OLST audit_file_name`

d. Notez la valeur UUID incluse dans le message.

```
Admin: # grep OLST 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):OLST][ANID(UI32):12448208][A
MID(FC32):ILMX][ATID(UI64):7729403978647354233]]
```

5. Recherchez les métadonnées de l'objet perdu en utilisant l'UUID :

a. Sélectionnez **ILM** > **Recherche de métadonnées d'objet**.

b. Saisissez l'UUID et sélectionnez **Rechercher**.

c. Vérifiez les emplacements dans les métadonnées et prenez les mesures appropriées :

Métadonnées	Conclusion
Objet <object_identifier> non trouvé	Si l'objet n'est pas trouvé, le message « ERROR":" » est renvoyé. Si l'objet n'est pas trouvé, vous pouvez réinitialiser le nombre d'**Objets perdus** pour effacer l'alerte. L'absence d'un objet indique que l'objet a été intentionnellement supprimé.

Métadonnées	Conclusion
Emplacements > 0	Si des emplacements sont répertoriés dans la sortie, l'alerte **Objets perdus** peut être un faux positif. Confirmer que les objets existent. Utilisez l'ID de nœud et le chemin de fichier répertoriés dans la sortie pour confirmer que le fichier objet se trouve à l'emplacement répertorié. (La procédure pour"recherche d'objets potentiellement perdus" explique comment utiliser l'ID de nœud pour trouver le nœud de stockage correct.) Si les objets existent, vous pouvez réinitialiser le nombre d'**Objets perdus** pour effacer l'alerte.
Emplacements = 0	S'il n'y a aucun emplacement répertorié dans la sortie, l'objet est potentiellement manquant. Vous pouvez essayer de"rechercher et restaurer l'objet" vous-même, ou vous pouvez contacter le support technique. Le support technique peut vous demander de déterminer si une procédure de récupération de stockage est en cours. Voir les informations sur"restauration des données d'objet à l'aide de Grid Manager" et"restauration des données d'objet sur un volume de stockage" .

Rechercher et restaurer des objets potentiellement perdus

Il peut être possible de trouver et de restaurer des objets qui ont déclenché une alerte **Objet perdu** et une alarme Objets perdus (LOST) héritée et que vous avez identifiés comme potentiellement perdus.

Avant de commencer

- Vous avez l'UUID de tout objet perdu, tel qu'identifié dans"Enquêter sur les objets perdus" .
- Vous avez le `Passwords.txt` déposer.

À propos de cette tâche

Vous pouvez suivre cette procédure pour rechercher des copies répliquées de l'objet perdu ailleurs dans la grille. Dans la plupart des cas, l'objet perdu ne sera pas retrouvé. Cependant, dans certains cas, vous pourrez peut-être retrouver et restaurer un objet répliqué perdu si vous agissez rapidement.

Contactez le support technique pour obtenir de l'aide sur cette procédure.

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 de grille :

      i. Entrez la commande suivante : `ssh admin@grid_node_IP`

ii. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

iii. Entrez la commande suivante pour passer en root : `su -`

iv. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer. Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#` .

b. Accédez au répertoire où se trouvent les journaux d'audit.

Le répertoire du journal d'audit et les nœuds applicables dépendent de vos paramètres de destination d'audit.

Option	Destination
Nœuds locaux (par défaut)	`/var/local/log/localaudit.log`
Nœuds d'administration/nœuds locaux	• Nœuds d'administration (principaux et non principaux) : `/var/local/audit/export/audit.log` • Tous les nœuds : Le `/var/local/log/localaudit.log` le fichier est généralement vide ou manquant dans ce mode.
Serveur syslog externe	`/var/local/log/localaudit.log`

En fonction des paramètres de destination de votre audit, saisissez : `cd /var/local/log` ou `/var/local/audit/export/`

Pour en savoir plus, consultez"Sélectionner les destinations des informations d'audit" .

c. Utilisez grep pour extraire le"messages d'audit associés à l'objet potentiellement perdu" et les envoyer vers 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 >
/var/local/tmp/messages_about_lost_object.txt
```

d. Utilisez grep pour extraire les messages d'audit d'emplacement perdu (LLST) de ce fichier de sortie. Entrer: `grep LLST output_file_name`

Par exemple:

```
Admin: # grep LLST /var/local/tmp/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):15815351
34379225]
[ATYP(FC32):LLST][ANID(UI32):12448208][AMID(FC32):CLSM][ATID(UI64):70
868710831907434 09]]
```

e. Recherchez le champ PCLD et le champ NOID dans le message LLST.

Si elle est présente, la valeur de PCLD est le chemin complet sur le disque vers la copie de l'objet répliqué manquant. La valeur de NOID est l'ID du nœud du LDR où une copie de l'objet peut être trouvée.

Si vous trouvez l'emplacement d'un 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 pour le service LDR se trouve dans la table Informations sur le nœud. Passez en revue les informations de 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 de grille :

i. Entrez la commande suivante : `ssh admin@grid_node_IP`

ii. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

iii. Entrez la commande suivante pour passer en root : `su -`

iv. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#` .

b. Déterminez si le chemin d'accès au fichier de l'objet existe.

Pour le chemin d'accès au fichier de l'objet, utilisez la valeur de PCLD du message d'audit LLST.

Par exemple, saisissez :

```
ls '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
```

Placez toujours le chemin du fichier objet entre guillemets simples dans les commandes pour échapper aux caractères spéciaux.

- Si le chemin de l'objet n'est pas trouvé, l'objet est perdu et ne peut pas être restauré à l'aide de cette procédure. Contactez le support technique.
- Si le chemin de l'objet est trouvé, passez à l'étape suivante. Vous pouvez tenter de restaurer l'objet

trouvé dans StorageGRID.

3. Si le chemin de l'objet a été trouvé, essayez de restaurer l'objet dans 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. Connectez-vous à Telnet sur 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, saisissez :

      ```
      Object_Found '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
      ```

      Délivrance du `Object_Found` la commande notifie la grille de l'emplacement de l'objet. Il déclenche également les politiques ILM actives, qui effectuent des copies supplémentaires comme spécifié dans chaque politique.

      > Si le nœud de stockage sur lequel vous avez trouvé l'objet est hors ligne, vous pouvez copier l'objet sur n'importe quel nœud de stockage en ligne. Placez l'objet dans n'importe quel répertoire /var/local/rangedb du nœud de stockage en ligne. Ensuite, émettez le `Object_Found` commande utilisant ce chemin de fichier vers l'objet.

      - Si l'objet ne peut pas être restauré, le `Object_Found` la commande échoue. Contactez le support technique.
      - Si l'objet a été restauré avec succès sur 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 avec succès sur StorageGRID, vérifiez que les nouveaux emplacements ont été créés :
   a. Sign in au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
   b. Sélectionnez **ILM** > **Recherche de métadonnées d'objet**.
   c. Saisissez l'UUID et sélectionnez **Rechercher**.
   d. Vérifiez les métadonnées et les nouveaux emplacements.
5. À partir d'un nœud d'administration, recherchez dans les journaux d'audit le message d'audit ORLM pour cet objet afin de confirmer que la gestion du cycle de vie des informations (ILM) a placé des copies comme

requis.

a. Connectez-vous au nœud de grille :

   i. Entrez la commande suivante : `ssh admin@grid_node_IP`

   ii. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

   iii. Entrez la commande suivante pour passer en root : `su -`

   iv. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer. 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. Se référer àsous-étape 1. b .

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 >
/var/local/tmp/messages_about_restored_object.txt
```

d. Utilisez grep pour extraire les messages d'audit des règles d'objet respectées (ORLM) de ce fichier de sortie. Entrer: `grep ORLM output_file_name`

   Par exemple:

```
Admin: # grep ORLM /var/local/tmp/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 LOCS dans le message d'audit.

   Si elle est présente, la valeur de CLDI dans LOCS est l'ID du nœud et l'ID du volume où une copie d'objet a été créée. Ce message indique que l'ILM a été appliqué et que deux copies d'objet ont été créées à deux emplacements dans la grille.

6. "Réinitialiser 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 à zéro.

Avant de commencer

- Vous devez être connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Tu as"autorisations d'accès spécifiques" .

À propos de cette tâche

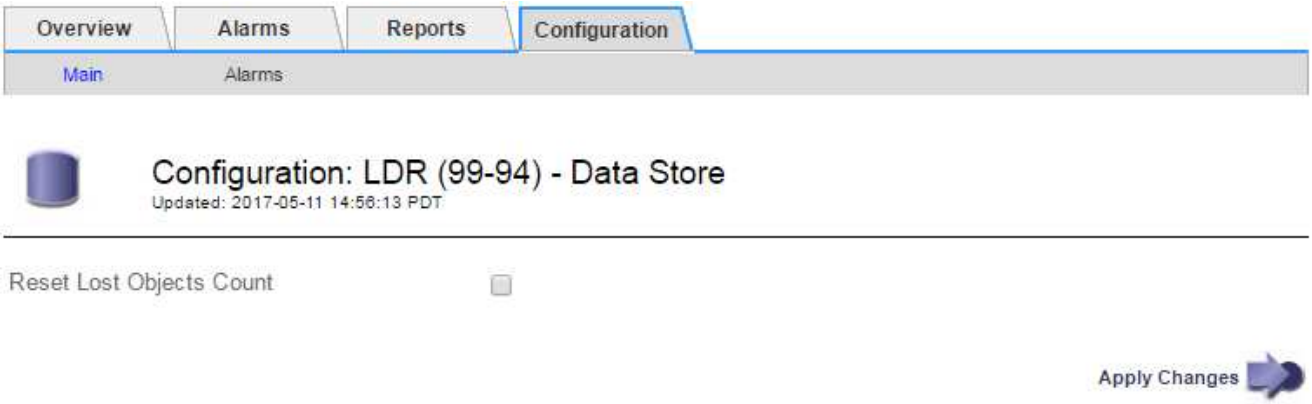
Vous pouvez réinitialiser le compteur d'objets perdus à partir de l'une des pages suivantes :

- **SUPPORT** > **Outils** > **Topologie de grille** > ***Site*** > ***Nœud de stockage*** > **LDR** > **Magasin de données** > **Présentation** > **Principal**
- **SUPPORT** > **Outils** > **Topologie de grille** > ***Site*** > ***Nœud de stockage*** > **DDS** > **Magasin de données** > **Présentation** > **Principal**

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*** > ***Nœud de stockage*** > **LDR** > **Magasin de données** > **Configuration** pour le nœud de stockage qui a l'alerte **Objets perdus** ou l'alarme PERDU.
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** ainsi que l'alarme PERDU s'effacent, ce qui peut prendre quelques minutes.

5. Vous pouvez également réinitialiser d'autres valeurs d'attributs associés qui pourraient avoir été incrémentées au cours du processus d'identification de l'objet perdu.

   a. Sélectionnez ***Site*** > ***Nœud de stockage*** > **LDR** > **Codage d'effacement** > **Configuration**.

   b. Sélectionnez **Réinitialiser le nombre d'échecs de lecture** et **Réinitialiser le nombre de copies corrompues détectées**.

   c. Cliquez sur **Appliquer les modifications**.

d. Sélectionnez ***Site*** > ***Nœud de stockage*** > **LDR** > **Vérification** > **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 nécessaires, vous pouvez sélectionner **Supprimer les objets mis en quarantaine**.

   Les 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 possible de supprimer en toute sécurité les objets mis en quarantaine. Cependant, si l'alerte **Objets perdus** ou l'alarme PERDU est déclenchée, le support technique peut souhaiter 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**.

Dépannage de l'alerte de faible stockage de données d'objet

L'alerte **Faible stockage de données d'objet** surveille la quantité d'espace disponible pour stocker les données d'objet sur chaque nœud de stockage.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Tu as"autorisations d'accès spécifiques" .

À propos de cette tâche

L'alerte **Faible stockage de données d'objet** est déclenchée lorsque la quantité totale de données d'objet répliquées et codées par effacement sur un nœud de stockage répond à l'une des conditions configurées dans la règle d'alerte.

Par défaut, une alerte majeure est déclenchée lorsque cette condition est évaluée comme vraie :

```
(storagegrid_storage_utilization_data_bytes/
(storagegrid_storage_utilization_data_bytes +
storagegrid_storage_utilization_usable_space_bytes)) >=0.90
```

Dans cet état :

- `storagegrid_storage_utilization_data_bytes`est une estimation de la taille totale des données d'objet répliquées et codées par effacement pour un nœud de stockage.
- `storagegrid_storage_utilization_usable_space_bytes`est la quantité totale d'espace de stockage d'objets restant pour un nœud de stockage.

Si une alerte majeure ou mineure de **Faible stockage de données d'objet** est déclenchée, vous devez effectuer une procédure d'extension dès que possible.

Étapes

1. Sélectionnez **ALERTES** > **Actuel**.

La page Alertes apparaît.

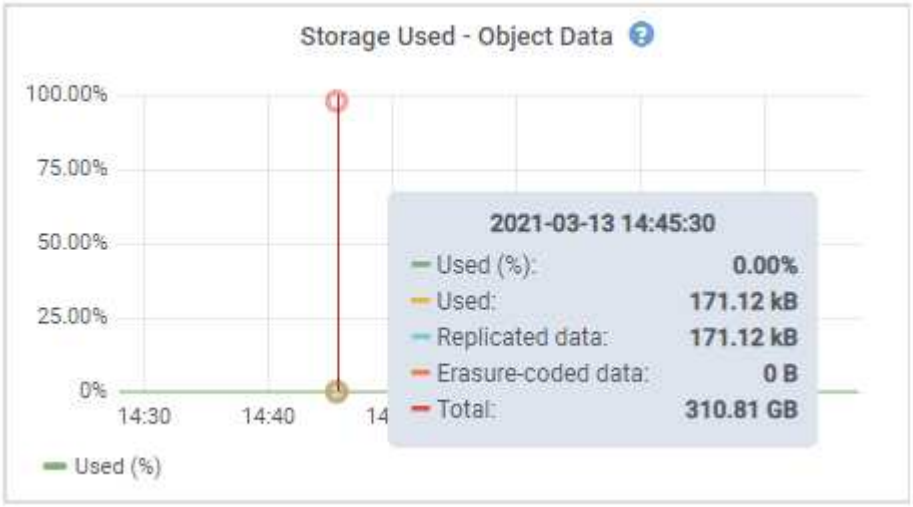
2. Dans le tableau des alertes, développez le groupe d'alertes **Faible stockage de données d'objet**, si nécessaire, et sélectionnez l'alerte que vous souhaitez afficher.

   Sélectionnez l'alerte, pas l'en-tête d'un groupe d'alertes.

3. Vérifiez les détails dans la boîte de dialogue et notez les points suivants :
   - Le temps déclenché
   - Le nom du site et du nœud
   - Les valeurs actuelles des métriques pour cette alerte
4. Sélectionnez **NODES** > ***Storage Node ou Site*** > **Storage**.
5. Placez votre curseur sur le graphique Stockage utilisé - Données de l'objet.

   Les valeurs suivantes sont affichées :

   - **Utilisé (%)** : Le pourcentage de l'espace total utilisable qui a été utilisé pour les données de l'objet.
   - **Utilisé** : la quantité d'espace total utilisable qui a été utilisée pour les données de l'objet.
   - **Données répliquées** : une estimation de la quantité de données d'objet répliquées sur ce nœud, ce site ou cette grille.
   - **Données codées par effacement** : une estimation de la quantité de données d'objet codées par effacement sur ce nœud, ce site ou cette grille.
   - **Total**: La quantité totale d'espace utilisable sur ce nœud, ce site ou cette grille. La valeur utilisée est la `storagegrid_storage_utilization_data_bytes` métrique.



6. Sélectionnez les contrôles de temps au-dessus du graphique pour afficher l'utilisation du stockage sur différentes périodes.

   L'analyse de l'utilisation du stockage au fil du temps peut vous aider à comprendre la quantité de stockage utilisée avant et après le déclenchement de l'alerte et peut vous aider à estimer le temps nécessaire pour que l'espace restant du nœud soit plein.

7. Dès que possible,"ajouter de la capacité de stockage" à votre réseau.

   Vous pouvez ajouter des volumes de stockage (LUN) aux nœuds de stockage existants ou ajouter de

nouveaux nœuds de stockage.

Pour plus d'informations, consultez la section "Gérer des nœuds de stockage complets" .

Dépannage des alertes de remplacement du 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 **Remplacement du 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" les paramètres globaux étaient les mêmes valeurs 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, les 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 maximale et ne pourrait pas accepter de nouvelles données si des filigranes optimisés étaient appliqués. StorageGRID ne modifiera pas les paramètres de filigrane dans ce cas.
- Vous avez précédemment défini l'un des filigranes du volume de stockage sur une valeur personnalisée. StorageGRID ne remplacera pas les paramètres de filigrane personnalisés par des valeurs optimisées. Cependant, StorageGRID peut déclencher l'alerte **Remplacement du filigrane en lecture seule faible** si votre valeur personnalisée pour le filigrane en lecture seule logicielle du volume de stockage est trop petite.

Comprendre l'alerte

Si vous utilisez des valeurs personnalisées pour les filigranes de volume de stockage, l'alerte **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 du volume de stockage est inférieure à la valeur optimisée minimale pour ce nœud de stockage. Si vous continuez à utiliser le paramètre personnalisé, le nœud de stockage risque de manquer cruellement d'espace avant de pouvoir passer en toute sécurité à l'état de lecture seule. Certains volumes de stockage peuvent devenir inaccessibles (démontés automatiquement) lorsque le nœud atteint sa capacité.

Par exemple, supposons que vous ayez précédemment défini le filigrane de lecture seule logicielle 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 de stockage A :

Volume 0	12 Go
Volume 1	12 Go
Volume 2	11 Go

Volume 3	15 Go

L'alerte **Remplacement du filigrane en lecture seule faible** est déclenchée pour le nœud de stockage A, car votre filigrane personnalisé (5 Go) est inférieur à la valeur optimisée minimale pour tous les volumes de ce nœud (11 Go). Si vous continuez à utiliser le paramètre personnalisé, le nœud risque de manquer cruellement d'espace avant de pouvoir passer en toute sécurité à l'état de lecture seule.

Résoudre l'alerte

Suivez ces étapes si une ou plusieurs alertes de **remplacement du filigrane en lecture seule faible** 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 supérieur.
- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"Autorisation d'accès root" .

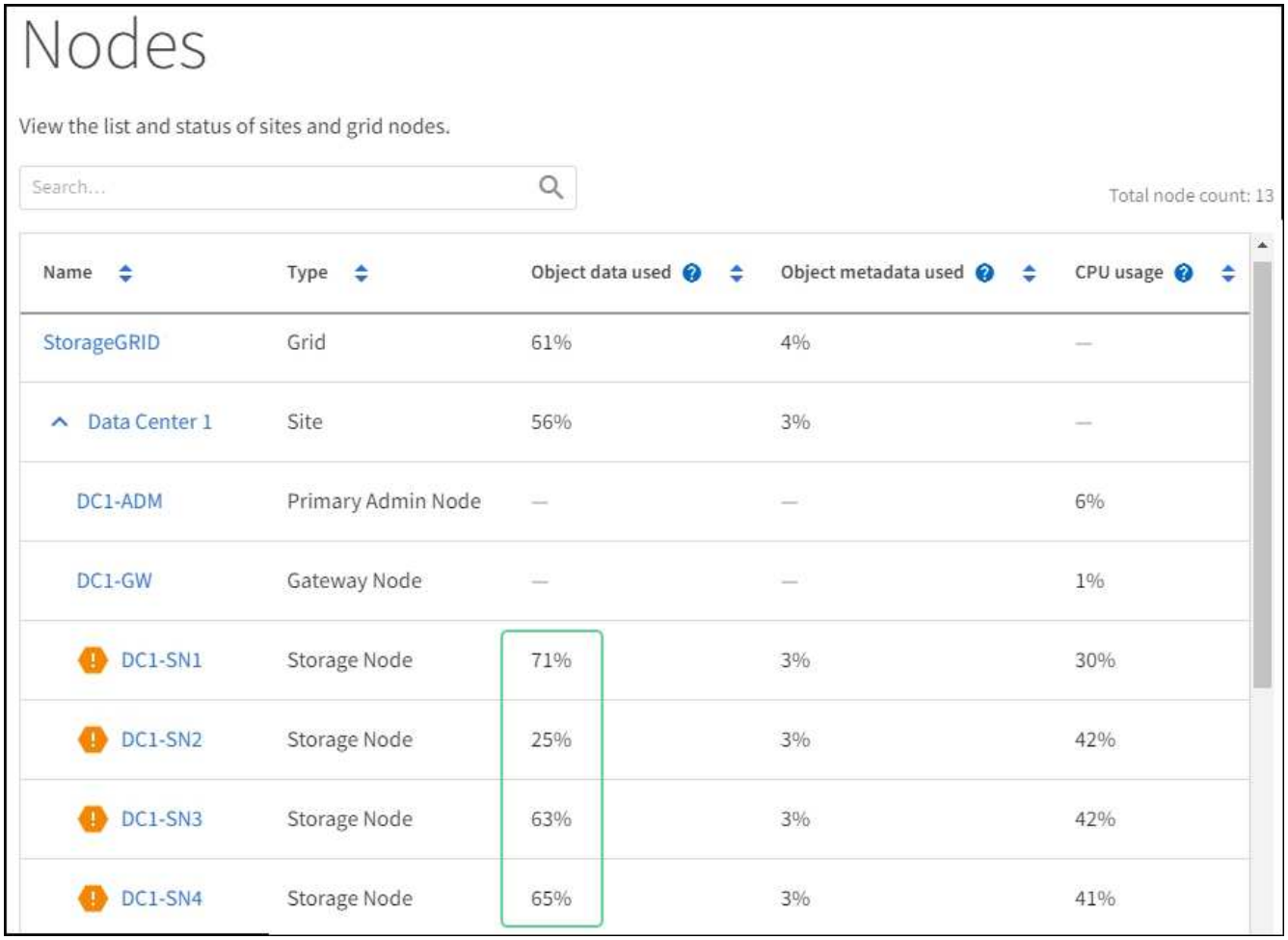
À propos de cette tâche

Vous pouvez résoudre l'alerte **Remplacement du filigrane en lecture seule faible** en mettant à jour les paramètres de filigrane personnalisés avec les nouveaux remplacements de filigrane. Toutefois, si un ou plusieurs nœuds de stockage sont presque pleins ou si vous avez des exigences ILM particulières, vous devez d'abord afficher 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 **NODES**.
2. Pour chaque site de la grille, développez la liste des nœuds.
3. Consultez les valeurs de pourcentage affichées dans la colonne **Données d'objet utilisées** pour chaque nœud de stockage sur chaque site.



4. Suivez l'étape appropriée :

   a. Si aucun des nœuds de stockage n'est presque plein (par exemple, toutes les valeurs **Données d'objet utilisées** sont inférieures à 80 %), vous pouvez commencer à utiliser les paramètres de remplacement. Aller àUtiliser des filigranes optimisés .

   b. Si les règles ILM utilisent un comportement d'ingestion strict ou si des pools de stockage spécifiques sont presque pleins, effectuez les étapes décrites dansAfficher les filigranes de stockage optimisés etDéterminez si vous pouvez utiliser des filigranes optimisés .

Afficher les filigranes de stockage optimisés

StorageGRID utilise deux mesures Prometheus pour afficher les valeurs optimisées qu'il a calculées pour le filigrane en lecture seule du volume de stockage. Vous pouvez afficher les valeurs optimisées minimales et maximales pour chaque nœud de stockage de votre grille.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **Métriques**.
2. Dans la section Prometheus, sélectionnez le lien pour accéder à l'interface utilisateur de Prometheus.
3. Pour voir le filigrane en lecture seule minimal recommandé, entrez la métrique Prometheus suivante et sélectionnez **Exécuter** :

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

   La dernière colonne affiche la valeur optimisée minimale du filigrane en lecture seule souple pour tous les

volumes de stockage sur chaque nœud de stockage. Si cette valeur est supérieure au paramètre personnalisé pour le filigrane en lecture seule logicielle du volume de stockage, l'alerte **Remplacement du filigrane en lecture seule faible** est déclenchée pour le nœud de stockage.

4. Pour voir le filigrane en lecture seule maximal recommandé, entrez la métrique Prometheus suivante et sélectionnez **Exécuter** :

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

   La dernière colonne affiche la valeur optimisée maximale du filigrane en lecture seule pour tous les volumes de stockage sur chaque nœud de stockage.

5. Notez la valeur optimisée maximale pour chaque nœud de stockage.

Déterminez si vous pouvez utiliser des filigranes optimisés

Étapes

1. Sélectionnez **NODES**.
2. Répétez ces étapes pour chaque nœud de stockage en ligne :
   a. Sélectionnez ***Nœud de stockage*** > **Stockage**.
   b. Faites défiler jusqu'au tableau Magasins d'objets.
   c. Comparez la valeur **Disponible** pour chaque magasin d'objets (volume) au filigrane optimisé maximal que vous avez noté 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 optimisé maximal pour ce nœud, accédez àUtiliser des filigranes optimisés pour commencer à utiliser les filigranes optimisés.

   Sinon, étendez la grille dès que possible. Soit"ajouter des volumes de stockage" à un nœud existant ou"ajouter de nouveaux nœuds de stockage" . Ensuite, allez àUtiliser 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 **Remplacement du filigrane en lecture seule faible**.

> ⓘ Les mêmes valeurs de filigrane personnalisées sont appliquées à chaque volume de stockage sur chaque nœud de stockage. L'utilisation de valeurs inférieures à celles recommandées pour les filigranes de volume de stockage peut entraîner l'inaccessibilité de certains volumes de stockage (démontage automatique) 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 de volume de stockage optimisés 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.

Résoudre les problèmes de métadonnées

Si des problèmes de métadonnées surviennent, 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 de métadonnées est déclenchée.

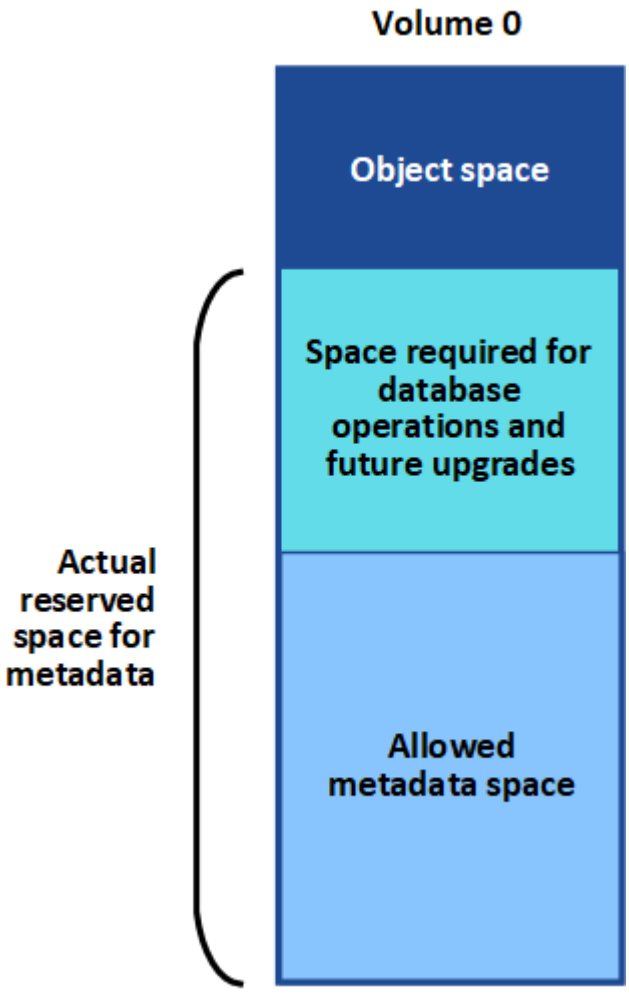
Avant de commencer

Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .

À propos de cette tâche

Suivez les actions recommandées pour chaque alerte liée aux métadonnées déclenchée. Si l'alerte **Faible stockage de métadonnées** est déclenchée, vous devez ajouter de nouveaux nœuds de stockage.

StorageGRID réserve une certaine quantité d'espace sur le volume 0 de chaque nœud de stockage pour les métadonnées d'objet. Cet espace, appelé *espace réservé réel*, est subdivisé en espace autorisé pour les métadonnées d'objet (l'espace de métadonnées autorisé) et l'espace requis pour les opérations essentielles de la base de données, telles que le compactage et la réparation. L'espace de métadonnées autorisé régit la capacité globale de l'objet.



Si les métadonnées de l'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 produiront.

Tu peux"surveiller la capacité des métadonnées des objets pour chaque nœud de stockage" pour vous aider à anticiper les erreurs et à les corriger avant qu'elles ne surviennent.

StorageGRID utilise la métrique Prometheus suivante pour mesurer le degré de remplissage de l'espace de métadonnées autorisé :

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utiliza
tion_metadata_allowed_bytes
```

Lorsque cette expression Prometheus atteint certains seuils, l'alerte **Faible stockage de métadonnées** est déclenchée.

- **Mineur** : les métadonnées de l'objet utilisent 70 % ou plus de l'espace de métadonnées autorisé. Vous devez ajouter de nouveaux nœuds de stockage dès que possible.
- **Majeur** : les métadonnées de l'objet utilisent 90 % ou plus de l'espace de métadonnées autorisé. Vous devez ajouter de nouveaux nœuds de stockage immédiatement.

> Lorsque les métadonnées d'objet utilisent 90 % ou plus de l'espace de métadonnées autorisé, un avertissement apparaît sur le tableau de bord. Si cet avertissement apparaît, vous devez ajouter immédiatement de nouveaux nœuds de stockage. Vous ne devez jamais autoriser les métadonnées d'objet à utiliser plus de 100 % de l'espace autorisé.

- **Critique** : les métadonnées de l'objet utilisent 100 % ou plus 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 de nouveaux objets et ajouter immédiatement de nouveaux nœuds de stockage.

> Si la taille du volume 0 est inférieure à l'option de stockage d'espace réservé aux métadonnées (par exemple, dans un environnement hors production), le calcul de l'alerte **Faible stockage de métadonnées** peut être inexact.

Étapes

1. Sélectionnez **ALERTES** > **Actuel**.
2. Dans le tableau des alertes, développez le groupe d'alertes **Faible stockage de métadonnées**, si nécessaire, et sélectionnez l'alerte spécifique que vous souhaitez afficher.
3. Consultez les détails dans la boîte de dialogue d'alerte.
4. Si une alerte majeure ou critique de **stockage de métadonnées faible** a été déclenchée, effectuez une extension pour ajouter immédiatement des nœuds de stockage.

> Étant donné que StorageGRID conserve des copies complètes de toutes les métadonnées d'objet sur chaque site, la capacité des métadonnées de l'ensemble de la grille est limitée par la capacité des métadonnées du plus petit site. Si vous devez ajouter une capacité de métadonnées à un site, vous devez également"développer d'autres sites" par le même nombre de nœuds de stockage.

Une fois l'extension effectuée, StorageGRID redistribue les métadonnées d'objet existantes aux nouveaux nœuds, ce qui augmente la capacité globale des métadonnées de la grille. Aucune action de l'utilisateur n'est requise. L'alerte **Faible stockage de métadonnées** est effacée.

Résoudre les erreurs de certificat

Si vous constatez un problème de sécurité ou de certificat lorsque vous essayez 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.

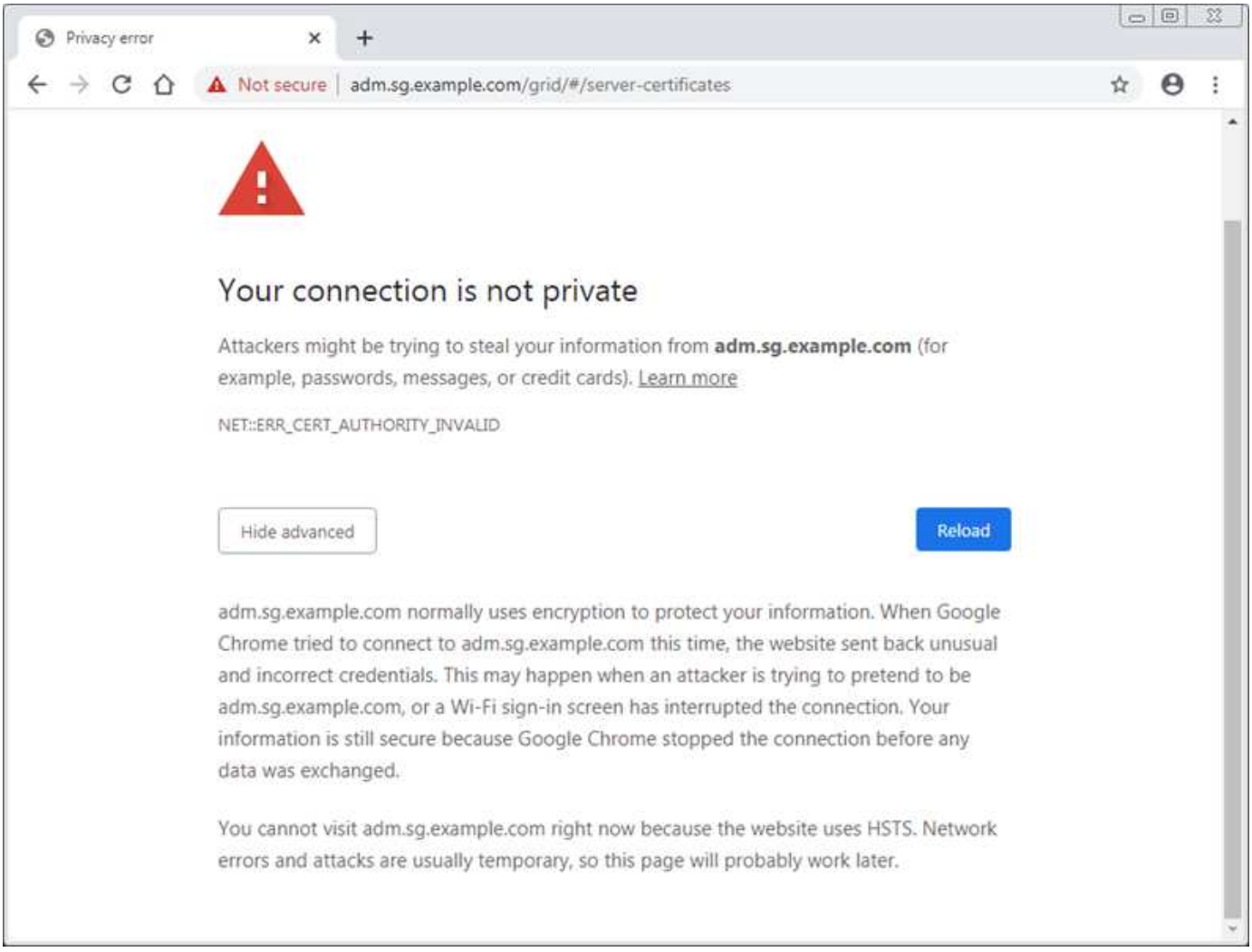
À propos de cette tâche

Les erreurs de certificat peuvent entraîner des problèmes lorsque vous essayez de vous connecter à StorageGRID à l'aide de Grid Manager, de l'API Grid Management, de Tenant Manager ou de l'API Tenant Management. Des erreurs de certificat peuvent également se produire lorsque vous essayez de vous connecter à un client S3 ou à un outil de surveillance externe.

Si vous accédez au Grid Manager ou au Tenant Manager 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'une des situations suivantes se produit :

- Votre certificat d'interface de gestion personnalisée expire.
- Vous revenez d'un certificat d'interface de gestion personnalisé au 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 perturbées 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 clients pour l'intégration Prometheus externe, des erreurs de certificat peuvent être provoquées par le certificat de l'interface de gestion StorageGRID ou par des certificats clients. L'alerte **Expiration des certificats clients configurés sur la page Certificats** est déclenchée lorsqu'un certificat client est sur le point d'expirer.

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 de 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 expirera bientôt, téléchargez ou générez un nouveau certificat.
   - Pour un certificat de serveur, consultez les étapes pour"configuration d'un certificat de serveur personnalisé pour le Grid Manager et le Tenant Manager" .
   - Pour un certificat client, consultez les étapes pour"configuration d'un certificat client" .
3. Pour les erreurs de certificat de serveur, essayez l'une ou les deux options suivantes :
   - Assurez-vous que le nom alternatif du sujet (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 essayez de vous connecter à StorageGRID à l'aide d'un nom de domaine :
     i. Saisissez l'adresse IP du nœud d'administration au lieu du nom de domaine pour contourner l'erreur de connexion et accéder au gestionnaire de grille.
     ii. Depuis le Gestionnaire de grille, sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats** puis"sélectionnez l'onglet de certificat approprié" pour installer un nouveau certificat personnalisé ou continuer avec le certificat par défaut.
     iii. Dans les instructions d'administration de StorageGRID, consultez les étapes pour"configuration d'un certificat de serveur personnalisé pour le Grid Manager et le Tenant Manager" .

Résoudre les problèmes liés au nœud d'administration et à l'interface utilisateur

Vous pouvez effectuer plusieurs tâches pour aider à 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 un"réseautage" ou "matériel" problème, un problème avec"Services du nœud d'administration" , ou un"problème avec la base de données Cassandra" sur les nœuds de stockage connectés.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le `Passwords.txt` déposer.
- Tu as"autorisations d'accès spécifiques" .

À propos de cette tâche

Utilisez 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 de vous connecter à nouveau.

   Si l'erreur n'est pas résolue automatiquement, passez à l'étape suivante.

2. Si votre système StorageGRID possède 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 indisponible.
   - Si vous parvenez à vous connecter, vous pouvez utiliser les options **Tableau de bord**, **NODES**, **Alerts** et **SUPPORT** pour vous aider à déterminer la cause de l'erreur.
   - Si vous n'avez qu'un seul nœud d'administration ou si vous ne parvenez toujours pas à 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" .

   Vous devrez peut-être désactiver et réactiver temporairement SSO pour un seul nœud d'administration afin de résoudre les problèmes.

   > 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 utilisateur fédéré ne fonctionne pas, essayez de vous connecter au gestionnaire de grille 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'identité**.
     iii. Cliquez sur **Tester la connexion** pour valider vos paramètres de connexion au serveur LDAP.
     iv. Si le test échoue, résolvez toutes les erreurs 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 Secure Shell (ssh) pour vous connecter au nœud d'administration :
   a. Entrez la commande suivante : `ssh admin@Admin_Node_IP`

b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

c. Entrez la commande suivante pour passer en root : `su -`

d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

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 mgmt api sont tous en cours d'exécution.

La sortie est mise à jour immédiatement 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. Confirmez que le service nginx-gw est en cours d'exécution `# service nginx-gw status`

9. Utilisez Lumberjack pour collecter des journaux : `# /usr/local/sbin/lumberjack.rb`

Si l'échec d'authentification s'est produit dans le passé, vous pouvez utiliser les options de script Lumberjack --start et --end pour spécifier la plage horaire appropriée. Utilisez lumberjack -h pour plus de détails sur ces options.

La sortie vers le terminal indique où l'archive du 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 ne parvenez pas à identifier de problèmes avec le nœud d'administration, exécutez l'une des commandes suivantes pour déterminer les adresses IP des trois nœuds de stockage qui exécutent le service ADC sur votre site. En règle générale, il s'agit des trois premiers nœuds de stockage installés sur le site.

```
# cat /etc/hosts
```

```
# gpt-list-services adc
```

Les nœuds d'administration utilisent le service ADC pendant le processus d'authentification.

12. Depuis le 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 les services idnt, acct, nginx et cassandra sont tous en cours d'exécution.

14. Répéter les étapesUtilisez le bûcheron pour collecter des bûches etRéviser les journaux 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 d'interface utilisateur

L'interface utilisateur du Grid Manager ou du Tenant Manager 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. Videz le cache de votre navigateur Web.

   La suppression du cache supprime les ressources obsolètes utilisées par la version précédente du logiciel StorageGRID et permet à l'interface utilisateur de fonctionner à nouveau correctement. Pour obtenir des

instructions, consultez la documentation de votre navigateur Web.

Résoudre les problèmes de réseau, de matériel et de plate-forme

Il existe plusieurs tâches que vous pouvez effectuer pour vous aider à déterminer la source des problèmes liés au réseau, au matériel et à la plate-forme StorageGRID .

Erreur « 422 : Entité non traitable »

L'erreur 422 : Entité non traitable peut se produire pour différentes raisons. Vérifiez le message d'erreur pour déterminer la cause de votre problème.

Si vous voyez l'un des messages d'erreur répertoriés, prenez l'action recommandée.

Message d'erreur	Cause profonde et action corrective

`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`
	Ce message peut s'afficher si vous sélectionnez l'option **Ne pas utiliser TLS** pour Transport Layer Security (TLS) lors de la configuration de la fédération d'identité à l'aide de Windows Active Directory (AD).
	
	L'utilisation de l'option **Ne pas utiliser TLS** n'est pas prise en charge pour une utilisation avec des serveurs AD qui appliquent la signature LDAP. Vous devez sélectionner l'option **Utiliser STARTTLS** ou l'option **Utiliser LDAPS** pour TLS.

Message d'erreur	Cause profonde et action corrective

`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)`
	Ce message s'affiche si vous essayez d'utiliser un chiffrement non pris en charge pour établir une connexion TLS (Transport Layer Security) depuis StorageGRID vers un système externe utilisé pour identifier la fédération ou les pools de stockage cloud.
	
	Vérifiez les chiffrements proposés par le système externe. Le système doit utiliser l'un des"chiffrements pris en charge par StorageGRID" pour les connexions TLS sortantes, comme indiqué dans les instructions d'administration de StorageGRID.

Alerte de non-concordance MTU du réseau de grille

L'alerte **Incompatibilité MTU du réseau de grille** est déclenchée lorsque le paramètre d'unité de transmission maximale (MTU) pour l'interface du réseau de grille (eth0) diffère considérablement entre les nœuds de la grille.

À propos de cette tâche

Les différences dans les paramètres MTU peuvent indiquer que certains réseaux eth0, mais pas tous, sont configurés pour les trames jumbo. Une non-concordance de taille MTU supérieure à 1 000 peut entraîner des problèmes de performances réseau.

Étapes

1. Répertoriez les paramètres MTU pour eth0 sur tous les nœuds.
   - Utilisez la requête fournie dans le gestionnaire de grille.
   - Accéder à *`primary Admin Node IP address`*`/metrics/graph` et entrez la requête suivante : `node_network_mtu_bytes{device="eth0"}`
2. "Modifier les paramètres MTU"si nécessaire pour garantir qu'ils sont les mêmes pour l'interface du 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 basés sur 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 avoir la valeur MTU souhaitée, puis utiliser le `change-ip.py` script pour changer la valeur MTU du réseau dans le conteneur.

Utilisez les arguments suivants pour modifier le MTU sur les nœuds basés sur Linux ou VMware.

Arguments positionnels	Description
`mtu`	Le MTU à définir. Doit être compris entre 1280 et 9216.
`network`	Les réseaux auxquels appliquer le MTU. Inclure un ou plusieurs des types de réseaux suivants : • grille • administrateur • client

+

Arguments optionnels	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 réception de trame de réseau de nœuds

Les alertes **Erreur de réception de trame de réseau de nœuds** peuvent être provoquées par des problèmes de connectivité entre StorageGRID et votre matériel réseau. Cette alerte disparaît d'elle-même une fois le problème sous-jacent résolu.

À propos de cette tâche

Les alertes **Erreur de réception de trame de réseau de nœud** peuvent être provoquées par les problèmes suivants avec le matériel réseau qui se connecte à StorageGRID:

- La correction d'erreur directe (FEC) est requise et n'est pas utilisée
- Incompatibilité entre le port du commutateur et le MTU de la carte réseau
- Taux d'erreur de lien élevés
- Dépassement de mémoire tampon en anneau de la carte réseau

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 :

Incompatibilité FEC

Ces étapes s'appliquent uniquement aux alertes **Erreur de trame de réception du réseau de nœuds** causées par une incompatibilité FEC sur les appliances StorageGRID .

a. Vérifiez l'état FEC du port dans le commutateur connecté à votre appliance StorageGRID .
b. Vérifiez l'intégrité physique des câbles reliant l'appareil au commutateur.
c. Si vous souhaitez modifier les paramètres FEC pour tenter de résoudre l'alerte, assurez-vous d'abord que l'appliance est configurée pour le mode **Auto** sur la page Configuration de liaison du programme d'installation de l'appliance StorageGRID (consultez les instructions de votre appliance :
   - "SG6160"
   - "SGF6112"
   - "SG6000"
   - "SG5800"
   - "SG5700"
   - "SG110 et SG1100"
   - "SG100 et SG1000"
d. Modifiez les paramètres FEC sur les ports du commutateur. Les ports de l'appliance StorageGRID ajusteront leurs paramètres FEC pour correspondre, si possible.

   Vous ne pouvez pas configurer les paramètres FEC sur les appliances StorageGRID . Au lieu de cela, les appareils tentent de découvrir et de refléter les paramètres FEC sur les ports de commutateur auxquels ils sont connectés. Si les liaisons sont forcées à des vitesses de réseau de 25 GbE ou 100 GbE, le commutateur et la carte réseau risquent de ne pas parvenir à négocier un paramètre FEC commun. Sans paramètre FEC commun, le réseau reviendra au mode « sans FEC ». Lorsque FEC n'est pas activé, les connexions sont plus sensibles aux erreurs causées par le bruit électrique.

   Les appliances StorageGRID prennent en charge Firecode (FC) et Reed Solomon (RS) FEC, ainsi que l'absence de FEC.

Incompatibilité entre le port du commutateur et le MTU de la carte réseau

Si l'alerte est provoquée par une incompatibilité entre le port de commutateur et le MTU de la carte réseau, vérifiez que la taille du MTU configurée sur le nœud est la même que le paramètre MTU du port de commutateur.

La taille MTU configurée sur le nœud peut être inférieure au paramètre sur le port de commutateur auquel le nœud est connecté. Si un nœud StorageGRID reçoit une trame Ethernet supérieure à son MTU, ce qui est possible avec cette configuration, l'alerte **Erreur de trame de réception du réseau du nœud** peut être signalée. Si vous pensez que c'est ce qui se passe, modifiez le MTU du port du commutateur pour qu'il corresponde au MTU de l'interface réseau StorageGRID ou modifiez le MTU de l'interface réseau StorageGRID pour qu'il corresponde au port du commutateur, en fonction de vos objectifs ou exigences en matière de MTU de bout en bout.

Pour des performances réseau optimales, tous les nœuds doivent être configurés avec des valeurs MTU similaires sur leurs interfaces Grid Network. L'alerte **Incompatibilité MTU du réseau de grille** est déclenchée s'il existe une différence significative dans les paramètres MTU du réseau de grille sur des nœuds individuels. Les valeurs MTU ne doivent pas nécessairement être les mêmes pour tous les types de réseaux. Voir Dépannage de l'alerte de non-concordance MTU du réseau de grille pour plus d'informations.

Voir aussi "Modifier le paramètre MTU" .

Taux d'erreur de lien élevés

a. Activez FEC, si ce n'est pas déjà fait.
b. Vérifiez que votre câblage réseau est de bonne qualité et qu'il n'est pas endommagé ou mal connecté.
c. Si les câbles ne semblent pas être le problème, contactez le support technique.

Vous remarquerez peut-être des taux d'erreur élevés dans un environnement avec un bruit électrique élevé.

Dépassement de mémoire tampon en anneau de la carte réseau

Si l'erreur est un dépassement de mémoire tampon en anneau de la carte réseau, contactez le support technique.

La mémoire tampon en anneau peut être saturée lorsque le système StorageGRID est surchargé et incapable de traiter les événements réseau en temps opportun.

3. Surveillez le problème et contactez le support technique si l'alerte ne se résout pas.

Erreurs de synchronisation horaire

Vous pourriez rencontrer des problèmes de synchronisation horaire dans votre grille.

Si vous rencontrez des problèmes de synchronisation horaire, 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 .

Quand"spécification de la source NTP externe" pour 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 de haute précision, tels que StorageGRID.

Linux : problèmes de connectivité réseau

Vous pourriez rencontrer des problèmes de connectivité réseau pour les nœuds StorageGRID hébergés sur des hôtes Linux.

Clonage d'adresse MAC

Dans certains cas, les problèmes de réseau peuvent être résolus en utilisant le clonage d'adresse MAC. Si vous utilisez des hôtes virtuels, définissez la valeur de la clé de clonage d'adresse MAC pour chacun de vos réseaux sur « true » dans votre fichier de configuration de nœud. Ce paramètre oblige l'adresse MAC du conteneur StorageGRID à utiliser l'adresse MAC de l'hôte. Pour créer des fichiers de configuration de nœud, consultez les instructions pour"Red Hat Enterprise Linux" ou"Ubuntu ou Debian" .

> ⓘ Créez des interfaces réseau virtuelles distinctes à utiliser par 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 promiscuité n'a pas été activé sur l'hyperviseur.

Pour plus d'informations sur l'activation du clonage MAC, consultez les instructions de"Red Hat Enterprise Linux" ou"Ubuntu ou Debian" .

Mode promiscuité

Si vous ne souhaitez pas utiliser le clonage d'adresse MAC et préférez autoriser toutes les interfaces à recevoir et à transmettre des données pour des 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 **Accepter** pour le mode promiscuité, les modifications d'adresse MAC et les transmissions falsifiées. Les valeurs définies sur le commutateur virtuel peuvent être remplacées par les valeurs au niveau du groupe de ports. Assurez-vous donc que les paramètres sont les mêmes aux deux endroits.

Pour plus d'informations sur l'utilisation du mode Promiscuous, consultez les instructions de"Red Hat Enterprise Linux" ou"Ubuntu ou Debian" .

Linux : l'état du nœud est « orphelin »

Un nœud Linux dans un état orphelin indique généralement que le service StorageGrid ou le démon du nœud StorageGRID contrôlant le conteneur du nœud est mort de manière inattendue.

À propos de cette tâche

Si un nœud Linux signale qu'il est dans un état orphelin, vous devez :

- Vérifiez les journaux pour les erreurs et les messages.
- Essayez de redémarrer le nœud.
- Si nécessaire, utilisez les commandes du moteur de conteneur pour arrêter le conteneur de nœud existant.
- Redémarrez le nœud.

Étapes

1. Vérifiez les journaux du démon de service et du nœud orphelin pour détecter d'éventuelles erreurs évidentes ou des messages concernant une sortie inattendue.
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 contrôle du nœud de grille de stockage. Par exemple : `sudo docker stop --time secondscontainer-name`

   Pour `seconds` , entrez le nombre de secondes pendant lesquelles vous souhaitez attendre 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. Redémarrer le nœud : `storagegrid node start node-name`

   ```
   storagegrid node start DC1-S1-172-16-1-172
   ```

Linux : Dépannage de la prise en charge d'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.

À propos de cette tâche

Pour voir 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** à côté de **Adresses IP** dans l'onglet Présentation.

Si l'adresse IPv6 n'est pas affichée et que le nœud est installé sur un hôte Linux, suivez ces étapes 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 devrait 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 `sysctl` paramètres. Ensuite, changez la valeur à 0 avant de continuer.

3. Entrez le conteneur de nœud 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 devrait être 1.

```
net.ipv6.conf.all.disable_ipv6 = 1
```

Si le résultat n'est pas 1, cette procédure ne s'applique pas. Contactez le support 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 qui peuvent être liés à l'utilisation d'un serveur syslog externe et répertorie les actions correctives.

Ces erreurs sont affichées par l'assistant de configuration du serveur syslog externe si vous rencontrez des problèmes lors de l'envoi de messages de test pour valider que le serveur syslog externe est correctement configuré.

Les problèmes lors de l'exécution peuvent être signalés par le"Erreur de transfert du serveur syslog externe" alerte. Si vous recevez cette alerte, suivez les instructions de l'alerte pour renvoyer les messages de test afin d'obtenir des messages d'erreur détaillés.

Pour plus d'informations sur l'envoi d'informations d'audit à un serveur syslog externe, consultez :

- "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
Ne peut pas résoudre le nom d'hôte	Le nom de domaine complet que vous avez saisi pour le serveur syslog n'a pas pu être résolu en une adresse IP. 1. Vérifiez le nom d'hôte que vous avez entré. Si vous avez saisi une adresse IP, assurez-vous qu'il s'agit d'une adresse IP valide en notation WXYZ (« décimale à points »). 2. Vérifiez que les serveurs DNS sont correctement configurés. 3. Confirmez que chaque nœud peut accéder aux adresses IP du serveur DNS.
Connexion rejetée	Une connexion TCP ou TLS au serveur syslog a été refusée. Il se peut qu'aucun service n'écoute sur le port TCP ou TLS pour l'hôte, ou qu'un pare-feu bloque l'accès. 1. Vérifiez que vous avez entré le nom de domaine complet ou l'adresse IP, le port et le protocole corrects pour le serveur Syslog. 2. Confirmez que l'hôte du service Syslog exécute un démon Syslog qui écoute sur le port spécifié. 3. Confirmez qu'un pare-feu ne bloque pas l'accès aux connexions TCP/TLS des nœuds à l'IP et au port du serveur syslog.

Message d’erreur	Description et actions recommandées
Réseau inaccessible	Le serveur syslog n’est pas sur un sous-réseau directement connecté. Un routeur a renvoyé un message d’échec ICMP pour indiquer qu’il ne pouvait pas transmettre les messages de test des nœuds répertoriés au serveur Syslog. 1. Vérifiez que vous avez entré le nom de domaine complet ou l’adresse IP correct pour le serveur syslog. 2. Pour chaque nœud répertorié, vérifiez la liste des sous-réseaux du réseau de grille, les listes de sous-réseaux des réseaux d’administration et les passerelles du réseau client. Confirmez qu’ils sont configurés pour acheminer le trafic vers le serveur Syslog via l’interface réseau et la passerelle attendues (Grille, Admin ou Client).
Hôte inaccessible	Le serveur syslog se trouve sur un sous-réseau directement connecté (sous-réseau utilisé par les nœuds répertoriés pour leurs adresses IP de grille, d’administration ou de 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. 1. Vérifiez que vous avez entré le nom de domaine complet ou l’adresse IP correct pour le serveur syslog. 2. Vérifiez que l’hôte exécutant le service syslog est opérationnel.
La connexion a expiré	Une tentative de connexion TCP/TLS a été effectuée, mais aucune réponse n’a été reçue du serveur syslog pendant une longue période. Il peut y avoir une mauvaise configuration du routage ou un pare-feu peut abandonner le trafic sans envoyer de réponse (une configuration courante). 1. Vérifiez que vous avez entré le nom de domaine complet ou l’adresse IP correct pour le serveur syslog. 2. Pour chaque nœud répertorié, vérifiez la liste des sous-réseaux du réseau de grille, les listes de sous-réseaux des réseaux d’administration et les passerelles du réseau client. Confirmez qu’ils sont configurés pour acheminer le trafic vers le serveur Syslog à l’aide de l’interface réseau et de la passerelle (Grille, Admin ou Client) sur lesquelles vous prévoyez que le serveur Syslog sera atteint. 3. Confirmez 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.

Message d'erreur	Description et actions recommandées
Connexion fermée par le partenaire	Une connexion TCP au serveur syslog a été établie avec succès mais a été fermée ultérieurement. Les raisons peuvent être les suivantes : • Le serveur syslog a peut-être été redémarré ou redémarré. • Le nœud et le serveur syslog peuvent avoir des paramètres TCP/TLS différents. • Un pare-feu intermédiaire peut fermer les connexions TCP inactives. • Un serveur non-syslog écoutant sur le port du serveur syslog a peut-être fermé la connexion. Pour résoudre ce problème : 1. Vérifiez que vous avez entré le nom de domaine complet ou l'adresse IP, le port et le protocole corrects pour le serveur Syslog. 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. 3. Vérifiez qu'un pare-feu intermédiaire n'est pas configuré pour fermer les connexions TCP inactives.
Erreur de certificat TLS	Le certificat de serveur reçu du serveur syslog n'était pas compatible avec le groupe de certificats CA et le certificat client que vous avez fournis. 1. Confirmez que le groupe de certificats CA et le certificat client (le cas échéant) sont compatibles avec le certificat du serveur sur le serveur Syslog. 2. Confirmez que les identités dans le certificat du serveur du serveur syslog incluent les valeurs IP ou FQDN attendues.
Transfert suspendu	Les enregistrements Syslog ne sont plus transmis au serveur Syslog et StorageGRID n'est pas en mesure de détecter la raison. Consultez les journaux de débogage fournis avec cette erreur pour tenter de déterminer la cause première.
Session TLS terminée	Le serveur Syslog a mis fin à la session TLS et StorageGRID n'est pas en mesure de détecter la raison. 1. Consultez les journaux de débogage fournis avec cette erreur pour tenter de déterminer la cause première. 2. Vérifiez que vous avez entré le nom de domaine complet ou l'adresse IP, le port et le protocole corrects pour le serveur Syslog. 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. 4. Confirmez que le groupe de certificats CA et le certificat client (le cas échéant) sont compatibles avec le certificat du serveur du serveur Syslog. 5. Confirmez que les identités dans le certificat du serveur du serveur syslog incluent les valeurs IP ou FQDN attendues.

Message d’erreur	Description et actions recommandées
La requête de résultats a échoué	Le nœud d’administration utilisé pour la configuration et les tests du serveur Syslog ne peut pas demander les résultats des tests aux nœuds répertoriés. Un ou plusieurs nœuds peuvent être en panne. 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. 2. Redémarrez le service miscd sur les nœuds répertoriés.

Examiner les journaux d’audit

Messages d’audit et journaux

Ces instructions contiennent des informations sur la structure et le contenu des messages d’audit et des journaux d’audit StorageGRID . Vous pouvez utiliser ces informations pour lire et analyser la piste d’audit de l’activité du système.

Ces instructions sont destinées aux administrateurs chargés de produire des rapports d’activité et d’utilisation du système qui nécessitent l’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, consultez"Configurer les messages d’audit et les destinations des journaux" .

Auditer le flux et la rétention des messages

Tous les services StorageGRID génèrent des messages d’audit pendant le fonctionnement normal du système. Vous devez comprendre comment ces messages d’audit circulent à travers le système StorageGRID vers le `audit.log` déposer.

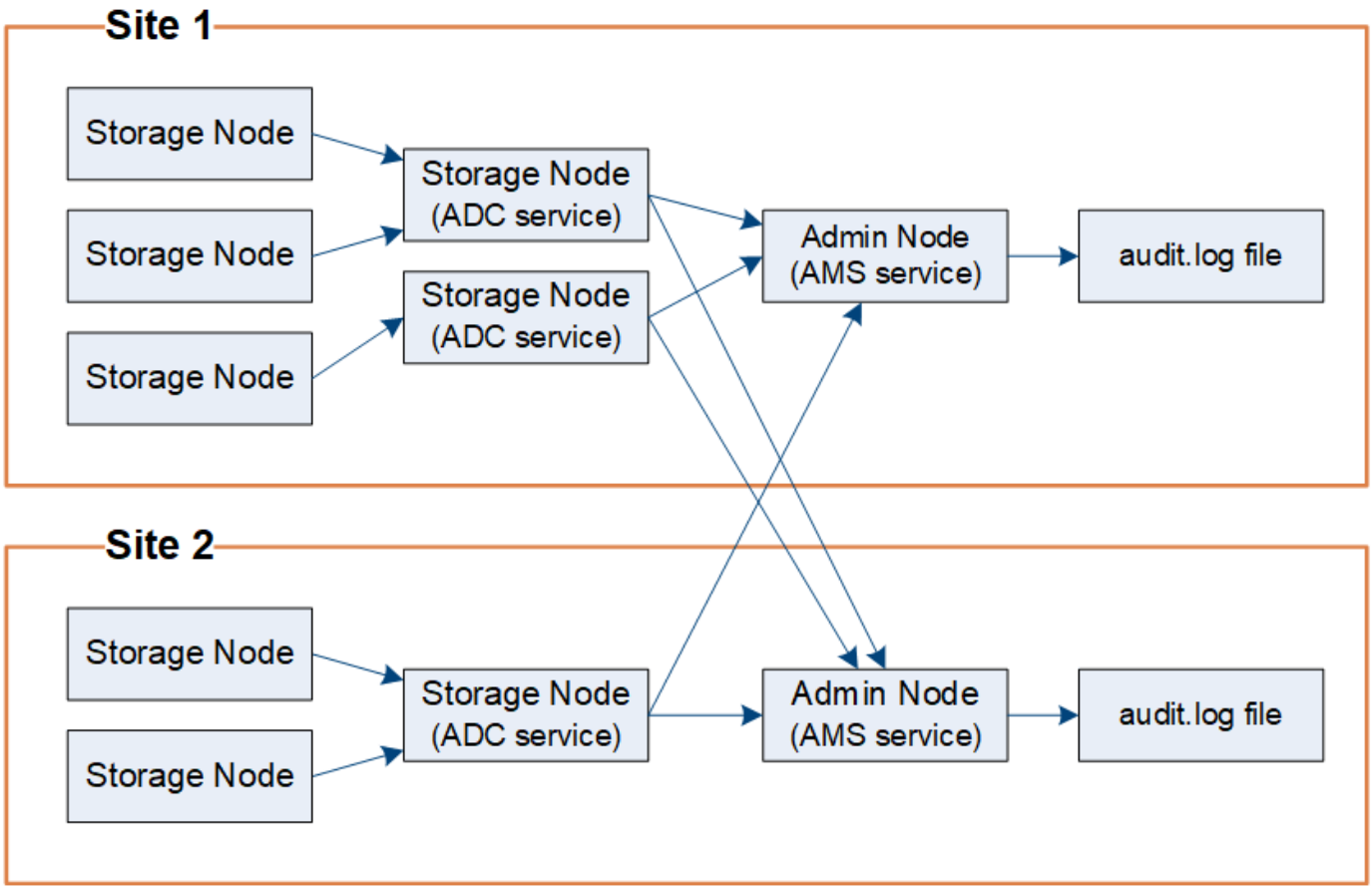
Flux de messages d’audit

Les messages d’audit sont traités par les nœuds d’administration et par les nœuds de stockage dotés d’un service de contrôleur de domaine administratif (ADC).

Comme indiqué dans le diagramme de flux de messages d’audit, chaque nœud StorageGRID envoie ses messages d’audit à l’un des services ADC sur le site du centre de données. Le service ADC est automatiquement activé pour les trois premiers nœuds de stockage installés sur chaque site.

À 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.

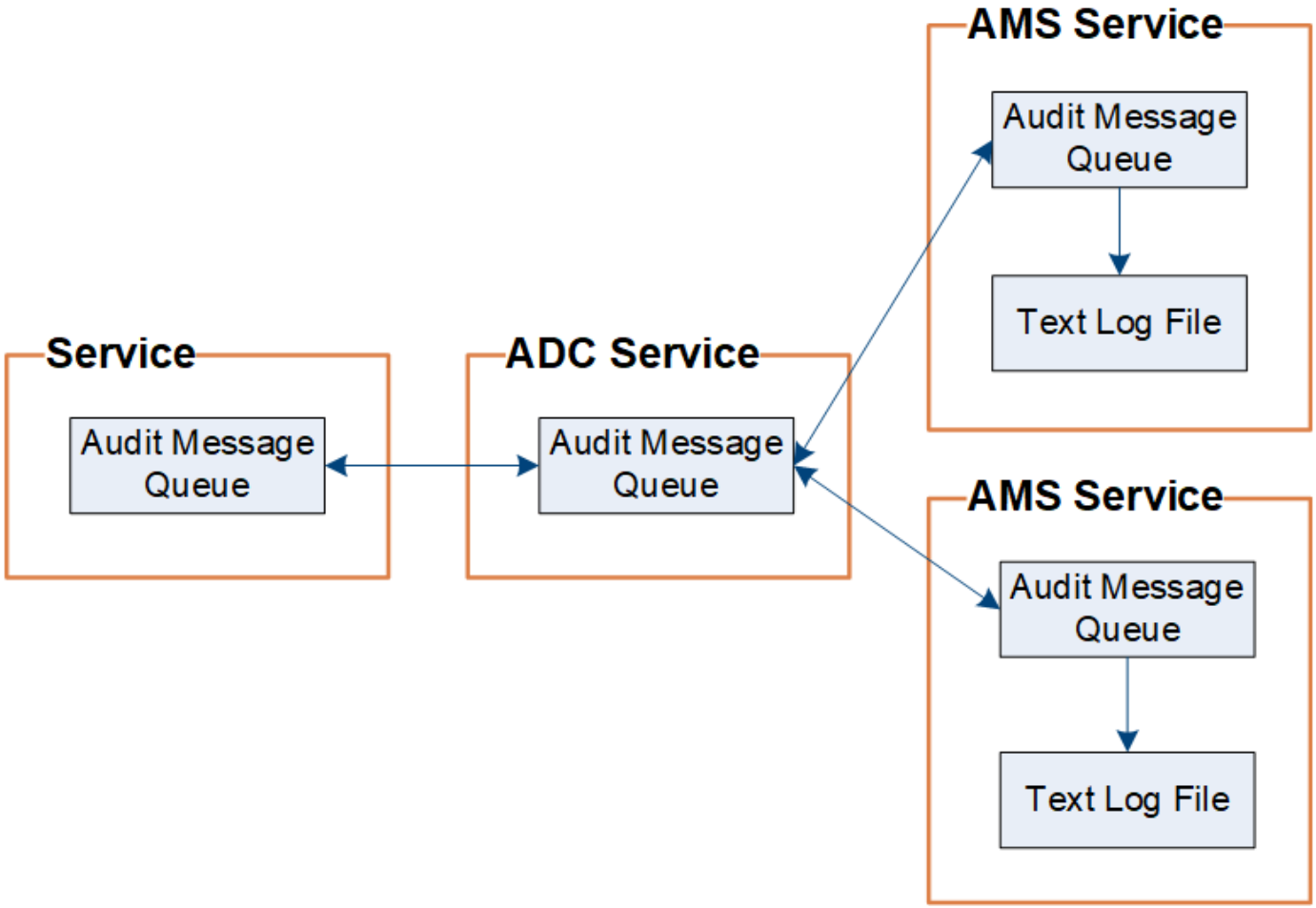
Chaque nœud d’administration stocke les messages d’audit dans des fichiers journaux texte ; le fichier journal actif est nommé `audit.log` .



Rétention des messages d'audit

StorageGRID utilise un processus de copie et de suppression pour garantir qu'aucun message d'audit n'est perdu avant de pouvoir être écrit dans le journal d'audit.

Lorsqu'un nœud génère ou relaie un message d'audit, le message est stocké dans une file d'attente de messages d'audit sur le disque système du nœud de 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 du nœud d'administration. `/var/local/log` annuaire. 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. À mesure que les files d'attente augmentent, elles consomment davantage d'espace disponible dans chaque nœud. `/var/local/` annuaire. Si le problème persiste et que le répertoire des messages d'audit d'un nœud devient trop plein, les nœuds individuels donneront la priorité au traitement de leur arriéré et deviendront temporairement indisponibles pour les nouveaux messages.

Plus précisément, vous pourriez observer les comportements suivants :

- Si le `/var/local/log` le répertoire utilisé par un nœud d'administration devient plein, le nœud d'administration sera marqué comme indisponible pour les nouveaux messages d'audit jusqu'à ce que le répertoire ne soit plus plein. Les demandes des clients S3 ne sont pas affectées. L'alarme XAMS (Unreachable Audit Repositories) est déclenchée lorsqu'un référentiel d'audit est inaccessible.
- Si le `/var/local/` le répertoire utilisé par un nœud de stockage avec le service ADC devient plein à 92 %, le nœud sera marqué comme indisponible pour les messages d'audit jusqu'à ce que le répertoire ne soit plein qu'à 87 %. Les demandes des clients S3 adressées à 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 le `/var/local/log/localaudit.log` déposer.

- Si le `/var/local/` répertoire utilisé par un nœud de stockage devient plein à 85 %, le nœud commencera à refuser les demandes des clients S3 avec `503 Service Unavailable`.

Les types de problèmes suivants peuvent entraîner une augmentation considérable de la taille des files d'attente de messages d'audit :

- La 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 être en retard.
- Un taux d'activité soutenu qui dépasse la capacité d'audit du système.
- Le `/var/local/` l'espace sur un nœud de stockage ADC devient plein pour des raisons sans rapport avec les messages d'audit. Lorsque cela se produit, le nœud cesse d'accepter de nouveaux messages d'audit et donne la priorité à son arriéré actuel, ce qui peut entraîner des arriérés sur d'autres nœuds.

Alerte de file d'attente d'audit volumineuse 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 au fil du 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 devraient se résoudre au fil du temps et peuvent être ignorées.

Si l'alerte ou l'alarme persiste et augmente en gravité, affichez un graphique de la taille de la file d'attente. Si le nombre 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 enregistrés en modifiant le niveau d'audit pour les écritures et les lectures du client sur Erreur ou Désactivé. Voir "Configurer les messages d'audit et les destinations des journaux" .

Messages en double

Le système StorageGRID adopte une approche conservatrice en cas de défaillance d'un réseau ou d'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 les éléments actifs `audit.log` fichier 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

- Tu as"autorisations d'accès spécifiques" .
- Vous devez avoir le `Passwords.txt` déposer.
- 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. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
   c. Entrez la commande suivante pour passer en root : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

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. Affichez le fichier journal d'audit actuel ou enregistré, selon les besoins.

Rotation du fichier journal d'audit

Les fichiers journaux d'audit sont enregistrés sur un nœud d'administration `/var/local/log` annuaire. Les fichiers journaux d'audit actifs sont nommés `audit.log` .

> En option, vous pouvez modifier la destination des journaux d'audit et envoyer les informations d'audit à un serveur syslog externe. Les journaux locaux des enregistrements d'audit continuent d'être générés et stockés lorsqu'un serveur syslog externe est configuré. Voir "Configurer les messages d'audit et les destinations des journaux" .

Une fois par jour, l'actif `audit.log` le fichier est enregistré et un nouveau `audit.log` le fichier est démarré. 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 fichiers utilisent la date d'enregistrement du fichier, suivie d'un numéro, 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 une journée, le fichier enregistré est compressé et renommé, au format *`yyyy-mm-dd.txt.gz`* , qui préserve la date originale. Au fil du temps, cela entraîne une consommation de stockage allouée 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` annuaire. Les journaux d'audit sont supprimés en fonction de la date de leur création, le plus ancien étant supprimé en premier. Vous pouvez surveiller les actions du script dans le fichier suivant : `/var/local/log/manage-audit.log` .

Cet exemple montre l'actif `audit.log` fichier, le fichier de la veille(`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 une collection de messages d'audit individuels.

Chaque message d'audit contient les éléments suivants :

- Le 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, placé 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 plus de lisibilité). Ces messages ont été générés lorsqu'un locataire a créé un bucket S3 et ajouté deux objets à ce bucket.

```
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 combien d'opérations d'écriture, de lecture et de suppression ont été enregistrées et combien de temps ces opérations ont pris.

Utiliser l'outil d'audit-explication

Vous pouvez utiliser le `audit-explain` outil permettant de traduire les messages

d’audit du journal d’audit dans un format facile à lire.

Avant de commencer

- Tu as"autorisations d’accès spécifiques" .
- Vous devez avoir le `Passwords.txt` déposer.
- Vous devez connaître l’adresse IP du nœud d’administration principal.

À propos de cette tâche

Le `audit-explain` L’outil, disponible sur le nœud d’administration principal, fournit des résumés simplifiés des messages d’audit dans un journal d’audit.

> Le `audit-explain` L’outil est principalement destiné à être utilisé par le support technique lors des opérations de dépannage. Traitement `audit-explain` les requêtes peuvent consommer une grande quantité de puissance CPU, ce qui peut avoir un impact sur les opérations StorageGRID .

Cet exemple montre une sortie typique de la `audit-explain` outil. Ces quatre"CRACHER" des messages d’audit ont été générés lorsque le locataire S3 avec l’ID de compte 92484777680322627870 a utilisé des requêtes S3 PUT pour créer un bucket nommé « bucket1 » et ajouter trois objets à ce bucket.

```
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
```

Le `audit-explain` L’outil peut effectuer les opérations suivantes :

- Traiter les journaux d’audit simples ou compressés. Par exemple:

  ```
  audit-explain audit.log

  audit-explain 2019-08-12.txt.gz
  ```

- Traiter 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 tube, ce qui vous permet de filtrer et de prétraiter l’entrée à l’aide du `grep` commandement ou autres moyens. Par exemple:

  ```
  grep SPUT audit.log | audit-explain

  grep bucket-name audit.log | audit-explain
  ```

Étant donné que les journaux d'audit peuvent être très volumineux et lents à analyser, vous pouvez gagner du temps en filtrant les parties que vous souhaitez consulter et en les exécutant. `audit-explain` sur les parties, au lieu du fichier entier.

> Le `audit-explain` l'outil n'accepte pas les fichiers compressés comme entrée canalisée. Pour traiter les fichiers compressés, fournissez leurs noms de fichiers comme arguments de ligne de commande ou utilisez le `zcat` outil pour décompresser les fichiers en premier. Par exemple:
>
> ```
> zcat audit.log.gz | audit-explain
> ```

Utilisez le `help (-h)` option pour voir les options disponibles. Par exemple:

```
$ audit-explain -h
```

Étapes

1. Connectez-vous au nœud d'administration principal :
   a. Entrez la commande suivante : `ssh admin@`*`primary_Admin_Node_IP`*
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
   c. Entrez la commande suivante pour passer en root : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

   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 que vous souhaitez analyser :

   ```
   $ audit-explain /var/local/log/audit.log
   ```

   Le `audit-explain` L'outil imprime des interprétations lisibles par l'homme de tous les messages dans le ou les fichiers spécifiés.

   > Pour réduire la longueur des lignes et améliorer la lisibilité, les horodatages ne sont pas affichés par défaut. Si vous souhaitez voir les horodatages, utilisez l'horodatage(`-t`) option.

Utiliser l'outil d'audit-somme

Vous pouvez utiliser le `audit-sum` outil permettant de compter les messages d'audit d'écriture, de lecture, d'en-tête et de suppression et de voir le temps minimum, maximum et moyen (ou la taille) pour chaque type d'opération.

Avant de commencer

- Tu as"autorisations d'accès spécifiques" .
- Vous devez avoir le `Passwords.txt` déposer.
- Vous devez connaître l'adresse IP du nœud d'administration principal.

À propos de cette tâche

Le `audit-sum` L'outil, disponible sur le nœud d'administration principal, résume le nombre d'opérations d'écriture, de lecture et de suppression enregistrées et la durée de ces opérations.

> Le `audit-sum` L'outil est principalement destiné à être utilisé par le support technique lors des opérations de dépannage. Traitement `audit-sum` les requêtes peuvent consommer une grande quantité de puissance CPU, ce qui peut avoir un impact sur les opérations StorageGRID .

Cet exemple montre une sortie typique de la `audit-sum` outil. Cet exemple montre combien de temps ont pris les opérations du protocole.

```
  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
```

Le `audit-sum` L'outil fournit les décomptes et les heures 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 à mesure que les fonctionnalités sont obsolètes. Si vous rencontrez un code d'audit qui n'est pas répertorié ici, vérifiez les versions précédentes de cette rubrique pour les anciennes versions de SG. Par exemple : "Documentation de l'outil d'audit de StorageGRID 11.8" .

Code	Description	Se référer à
IDEL	Suppression initiée par ILM : enregistre le moment où ILM démarre le processus de suppression d'un objet.	"IDEL : suppression initiée par ILM"
SDEL	S3 DELETE : enregistre une transaction réussie pour supprimer un objet ou un bucket.	"SDEL : SUPPRESSION S3"
SGET	S3 GET : enregistre une transaction réussie pour récupérer un objet ou répertorier les objets dans un bucket.	"SGET : S3 OBTENIR"
KARITÉ	S3 HEAD : enregistre une transaction réussie pour vérifier l'existence d'un objet ou d'un bucket.	"SHEA : TÊTE S3"

Code	Description	Se référer à
CRACHER	S3 PUT : enregistre une transaction réussie pour créer un nouvel objet ou un nouveau bucket.	"SPUT : S3 PUT"
WDEL	Swift DELETE : enregistre une transaction réussie pour supprimer un objet ou un conteneur.	"WDEL : SUPPRESSION rapide"
WGET	Swift GET : enregistre une transaction réussie pour récupérer un objet ou répertorier les objets dans un conteneur.	"WGET : Swift GET"
WHEA	Swift HEAD : enregistre une transaction réussie pour vérifier l'existence d'un objet ou d'un conteneur.	"WHEA : TÊTE RAPIDE"
WPUT	Swift PUT : enregistre une transaction réussie pour créer un nouvel objet ou conteneur.	"WPUT : Swift PUT"

Le `audit-sum` L'outil peut effectuer les opérations suivantes :

- Traiter les journaux d'audit simples ou compressés. Par exemple:

```
audit-sum audit.log

audit-sum 2019-08-12.txt.gz
```

- Traiter 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 tube, ce qui vous permet de filtrer et de prétraiter l'entrée à l'aide du `grep` commandement ou 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 canalisée. Pour traiter les fichiers compressés, fournissez leurs noms de fichiers comme arguments de ligne de commande ou utilisez le `zcat` outil pour décompresser les fichiers en premier. Par exemple:
>
> ```
> audit-sum audit.log.gz
>
> zcat audit.log.gz | audit-sum
> ```

Vous pouvez utiliser des options de ligne de commande pour résumer les opérations sur les buckets séparément des opérations sur les objets ou pour regrouper les résumés de messages par nom de bucket, par

période ou par type de cible. Par défaut, les résumés affichent le temps de fonctionnement minimum, maximum et moyen, mais vous pouvez utiliser le `size (-s)` option permettant de regarder la taille de l'objet à la place.

Utilisez le `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. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
   c. Entrez la commande suivante pour passer en root : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

      Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#` .

2. Si vous souhaitez analyser tous les messages liés aux opérations d'écriture, de lecture, de lecture et de suppression, suivez ces étapes :
   a. Entrez la commande suivante, où `/var/local/log/audit.log` représente le nom et l'emplacement du ou des fichiers que vous souhaitez analyser :

      ```
      $ audit-sum /var/local/log/audit.log
      ```

      Cet exemple montre une sortie typique de la `audit-sum` outil. Cet exemple montre combien de temps ont pris les opérations du protocole.

      ```
        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 plus lentes en moyenne avec 1,13 seconde, mais les opérations SGET et SPUT (S3 PUT) affichent toutes deux des temps de pire cas longs d'environ 1 770 secondes.

   b. Pour afficher les 10 opérations de récupération les plus lentes, utilisez la commande grep pour sélectionner uniquement les messages SGET et ajoutez 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 bucket) et le chemin, ce qui vous permet de rechercher dans le journal d'audit d'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/r9O1OaQ8JB-1566861764-4519.iso
        1624414429   10.96.101.125       object   5375001556
backup/r9O1OaQ8JB-1566861764-6618.iso
        1533143793   10.96.101.125       object   5183661466
backup/r9O1OaQ8JB-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
```

+
À partir de cet exemple de sortie, vous pouvez voir que les trois requêtes S3 GET les plus lentes concernaient des objets d'une taille d'environ 5 Go, ce qui est beaucoup plus grand que les autres objets. La grande taille explique les temps de récupération les plus lents dans le pire des cas.

3. Si vous souhaitez déterminer les tailles des objets ingérés et récupérés dans votre grille, utilisez l'option de taille(`-s`):

```
audit-sum -s audit.log
```

```
  message group           count       min(MB)          max(MB)
average(MB)
  =============           =====     ========        ========
============
  IDEL                      274        0.004        5000.000
1654.502
  SDEL                   213371        0.000          10.504
1.695
  SGET                   201906        0.000        5000.000
14.920
  SHEA                    22716        0.001          10.504
2.967
  SPUT                 1771398        0.000        5000.000
2.495
```

Dans cet exemple, la taille moyenne de l'objet pour SPUT est inférieure à 2,5 Mo, mais la taille moyenne pour SGET est beaucoup plus grande. Le nombre de messages SPUT est bien supérieur au nombre de messages SGET, ce qui indique que la plupart des objets ne sont jamais récupérés.

4. Si vous souhaitez déterminer si les récupérations ont été lentes hier :

   a. Émettez la commande sur le journal d'audit approprié et utilisez l'option de regroupement par heure(`-gt`), suivi de la période (par exemple, 15M, 1H, 10S) :

      ```
      grep SGET audit.log | audit-sum -gt 1H
      ```

```
  message group           count    min(sec)       max(sec)
average(sec)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.010        1481.867
1.254
  2019-09-05T01            4173        0.011        1740.290
1.115
  2019-09-05T02           20142        0.011        1274.961
1.562
  2019-09-05T03           57591        0.010        1383.867
1.254
  2019-09-05T04          124171        0.013        1740.290
1.405
  2019-09-05T05          420182        0.021        1274.511
1.562
  2019-09-05T06         1220371        0.015        6274.961
5.562
  2019-09-05T07          527142        0.011        1974.228
2.002
  2019-09-05T08          384173        0.012        1740.290
1.105
  2019-09-05T09           27591        0.010        1481.867
1.354
```

Ces résultats montrent que le trafic S3 GET a augmenté entre 06h00 et 07h00. Les temps maximum et moyen sont également considérablement plus élevés à ces moments-là, et ils n'augmentent pas progressivement à mesure que le nombre augmente. Cela suggère que la capacité a été dépassée quelque part, peut-être dans le réseau ou dans la capacité du réseau à traiter les demandes.

b. Pour déterminer la taille des objets récupérés chaque heure hier, ajoutez l'option de taille(`-s`) à la commande :

```
grep SGET audit.log | audit-sum -gt 1H -s
```

```
  message group           count       min(B)          max(B)
average(B)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.040        1481.867
1.976
  2019-09-05T01            4173        0.043        1740.290
2.062
  2019-09-05T02           20142        0.083        1274.961
2.303
  2019-09-05T03           57591        0.912        1383.867
1.182
  2019-09-05T04          124171        0.730        1740.290
1.528
  2019-09-05T05          420182        0.875        4274.511
2.398
  2019-09-05T06         1220371        0.691  5663711385.961
51.328
  2019-09-05T07          527142        0.130        1974.228
2.147
  2019-09-05T08          384173        0.625        1740.290
1.878
  2019-09-05T09           27591        0.689        1481.867
1.354
```

Ces résultats indiquent que certaines récupérations très importantes ont eu lieu lorsque le trafic de récupération global était à son maximum.

c. Pour voir plus de détails, utilisez le"outil d'audit-explication" pour passer en revue 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 comporter plusieurs lignes, ajoutez le `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 buckets sont plus lentes que les opérations SPUT pour les objets :

a. Commencez par utiliser le `-go` option, qui regroupe séparément les messages pour les opérations d'objet et de compartiment :

```
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 buckets ont des caractéristiques de performances différentes des opérations SPUT pour les objets.

b. Pour déterminer quels buckets ont les opérations SPUT les plus lentes, utilisez le `-gb` option, qui regroupe les messages par bucket :

```
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 buckets ont la plus grande taille d'objet SPUT, utilisez à la fois le `-gb` et le `-s` options:

```
grep SPUT audit.log | audit-sum -gb -s
```

```
  message group                    count       min(B)          max(B)
average(B)
  =============                    =====     ========        ========
============
  SPUT.cho-non-versioning          71943        2.097        5000.000
21.672
  SPUT.cho-versioning              54277        2.097        5000.000
21.120
  SPUT.cho-west-region             80615        2.097         800.000
14.433
  SPUT.ldt002                    1564563        0.000         999.972
0.352
```

Format du message d'audit

Format du message d'audit

Les messages d'audit échangés au sein du système StorageGRID incluent des informations standard communes à tous les messages et un contenu spécifique décrivant l'événement ou l'activité signalé.

Si les informations récapitulatives fournies par le"audit-explication" et"somme d'audit" les outils sont insuffisants, 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 pourrait apparaître dans le fichier journal d'audit :

```
2014-07-17T03:50:47.484627
[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP(F
C32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265006
03516]]
```

Chaque message d'audit contient une chaîne d'éléments d'attribut. La chaîne entière est entourée de crochets(`[ ]`), et chaque élément d'attribut dans la chaîne a les caractéristiques suivantes :

- Entouré de 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 comprend un code d'attribut, un type de données et une valeur qui sont rapportés 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 d'autres sont spécifiques à chaque événement.
- `type`est un identifiant à quatre caractères du type de données de programmation de la valeur, tel que 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 de type de données CSTR sont entourées de guillemets doubles « ».

Types de données

Différents types de données sont utilisés pour stocker des informations dans les messages d'audit.

Type	Description
UI32	Entier long non signé (32 bits) ; il peut stocker les nombres de 0 à 4 294 967 295.
UI64	Entier long double non signé (64 bits) ; il peut stocker les nombres de 0 à 18 446 744 073 709 551 615.
FC32	Constante à quatre caractères ; une valeur entière non signée de 32 bits représentée par quatre caractères ASCII tels que « ABCD ».
iPad	Utilisé pour les adresses IP.
CSTR	Un tableau de longueur variable de caractères UTF-8. Les caractères peuvent être échappés avec les conventions suivantes : • La barre oblique inverse est \\. • Le retour chariot est \r. • Les guillemets doubles sont \". • Le saut de ligne (nouvelle ligne) est \n. • Les caractères peuvent être remplacés par leurs équivalents hexadécimaux (au format \xHH, où HH est la valeur hexadécimale représentant le caractère).

Données spécifiques à l'événement

Chaque message d'audit dans le journal d'audit enregistre des données spécifiques à un événement système.

Après l'ouverture `[AUDT:` conteneur 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 :

```
2018-12-05T08:24:45.921845 [AUDT:*\[RSLT\(FC32\):SUCS\]*
\[TIME\(UI64\):11454\]\[SAIP\(IPAD\):"10.224.0.100"\]\[S3AI\(CSTR\):"60025621595611246499"\]
\[SACC\(CSTR\):"compte"\]\[S3AK\(CSTR\):"SGKH4_Nc8SO1H6w3w0nCOFCGgk__E6dYzKlumRsK
JA=="\] \[SUSR\(CSTR\):"urn:sgws:identity::60025621595611246499:root"\]
\[SBAI\(CSTR\):"60025621595611246499"\]\[SBAC\(CSTR\):"account"\]\[S3BK\(CSTR\):"bucket"\]
\[S3KY\(CSTR\):"object"\]\[CBID\(UI64\):0xCC128B9B9E428347\] \[UUID\(CSTR\):"B975D2CE-E4DA-
4D14-8A23-1CB4B83F2CD8"\]\[CSIZ\(UI64\):30720\][AVER(UI32):10]
\[ATIM(UI64):1543998285921845]\[ATYP\(FC32\):SHEA\][ANID(UI32):12281045][AMID(FC32):S3RQ]
\[ATID(UI64):15552417629170647261]]
```

Le `ATYP` L'élément (souligné dans l'exemple) identifie quel événement a généré le message. Cet exemple de message inclut le"KARITÉ" code de message ([ATYP(FC32):SHEA]), indiquant qu'il a été généré par une demande S3 HEAD réussie.

Éléments communs aux messages d'audit

Tous les messages d'audit contiennent les éléments communs.

Code	Type	Description
AU MILIEU DE	FC32	ID du module : identifiant à quatre caractères de l'ID du module qui a généré le message. Cela indique le segment de code dans lequel le message d'audit a été généré.
ANID	UI32	ID de nœud : l'ID de nœud de grille attribué au service qui a généré le message. Chaque service se voit attribuer un identifiant unique au moment de la configuration et de l'installation du système StorageGRID . Cet identifiant ne peut pas être modifié.
ASES	UI64	Identifiant de session d'audit : dans les versions précédentes, cet élément indiquait l'heure à laquelle le système d'audit était 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). **Remarque :** cet élément est obsolète et n'apparaît plus dans les messages d'audit.

Code	Type	Description
ASQN	UI64	Nombre de séquences : dans les versions précédentes, ce compteur était incrémenté pour chaque message d'audit généré sur le nœud de grille (ANID) et réinitialisé à zéro au redémarrage du service. **Remarque :** cet élément est obsolète et n'apparaît plus dans les messages d'audit.
ATID	UI64	ID de trace : un identifiant partagé par l'ensemble des messages déclenchés par un événement unique.
ATIM	UI64	Horodatage : l'heure à laquelle l'événement a été généré et a déclenché le message d'audit, mesurée 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. L'arrondi ou la troncature de l'horodatage enregistré peut être nécessaire. L'heure lisible par l'homme qui apparaît au début du message d'audit dans le `audit.log` le fichier est l'attribut ATIM au format ISO 8601. La date et l'heure sont représentées comme *`YYYY-MMDDTHH:MM:SS.UUUUUU`* , où le `T` est une chaîne de caractères littérale indiquant le début du segment de temps de la date. *`UUUUUU`* sont des microsecondes.
ATYP	FC32	Type d'événement : identifiant à quatre caractères de l'événement enregistré. Cela régit le contenu de la « charge utile » du message : les attributs qui sont inclus.
MOYENNE	UI32	Version : la version du message d'audit. À mesure que le logiciel StorageGRID évolue, de nouvelles versions de services peuvent intégrer de nouvelles fonctionnalités dans les rapports d'audit. Ce champ permet la compatibilité descendante dans le service AMS pour traiter les messages provenant d'anciennes versions de services.
RSLT	FC32	Résultat : le résultat d'un événement, d'un processus ou d'une transaction. Si ce n'est pas pertinent pour un message, NONE est utilisé plutôt que SUCS afin que le message ne soit pas filtré accidentellement.

Exemples de messages d'audit

Vous pouvez trouver des informations détaillées dans chaque message d'audit. Tous les messages d'audit utilisent le même format.

Ce qui suit est un exemple de message d'audit tel qu'il pourrait apparaître dans le `audit.log` déposer:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][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 enregistré, ainsi que des informations sur le message d'audit lui-même.

Pour identifier quel événement est 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):"s3small1"][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. "CRACHER" représente une transaction S3 PUT, qui enregistre l'ingestion d'un objet dans un bucket.

Le message d'audit suivant indique également le compartiment auquel 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\(CSTR\):"s3small1"][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 UTC (Universal Coordinated Time) au début du message d'audit. Cette valeur est une version lisible par l'homme 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):"s3small1"][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 juillet 2014 21:17:59 UTC.

Messages d'audit et cycle de vie des objets

Quand les messages d'audit sont-ils générés ?

Des messages d'audit sont générés chaque fois qu'un objet est ingéré, récupéré ou supprimé. 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 via des identifiants spécifiques à chaque protocole.

Protocole	Code
Liaison des opérations S3	S3BK (godet), S3KY (clé) ou les deux
Lier les opérations Swift	WCON (conteneur), WOBJ (objet) ou les deux
Lier les opérations internes	CBID (identifiant interne de l'objet)

Moment des messages d'audit

En raison de facteurs tels que les différences de synchronisation entre les nœuds de grille, la taille des objets et les délais du réseau, l'ordre des messages d'audit générés par les différents services peut varier par rapport à celui indiqué dans les exemples de cette section.

Transactions d'ingestion d'objets

Vous pouvez identifier les transactions d'ingestion client 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'ingestion ne sont pas répertoriés dans les tableaux suivants. Seuls les messages nécessaires au suivi de la transaction d'ingestion sont inclus.

Messages d'audit d'ingestion S3

Code	Nom	Description	Tracer	Voir
CRACHER	Transaction S3 PUT	Une transaction d'ingestion S3 PUT s'est terminée avec succès.	CBID, S3BK, S3KY	"SPUT : S3 PUT"
ORLM	Règles d'objet respectées	La politique ILM a été satisfaite pour cet objet.	CBID	"ORLM : Règles d'objet respectées"

Messages d'audit d'ingestion rapide

Code	Nom	Description	Tracer	Voir
WPUT	Transaction PUT rapide	Une transaction d'ingestion Swift PUT a été effectuée avec succès.	CBID, WCON, WOBJ	"WPUT : Swift PUT"
ORLM	Règles d'objet respectées	La politique ILM a été satisfaite pour cet objet.	CBID	"ORLM : Règles d'objet respectées"

Exemple : ingestion d'objets 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 dans un nœud de stockage (service LDR).

Dans cet exemple, la stratégie ILM active inclut la règle ILM « Créer 2 copies ».

> Tous les messages d'audit générés lors d'une transaction ne sont pas répertoriés dans l'exemple ci-dessous. Seuls ceux liés à la transaction d'ingestion S3 (SPUT) sont répertoriés.

Cet exemple suppose qu'un bucket S3 a été précédemment créé.

SPUT : S3 PUT

Le message SPUT est généré pour indiquer qu'une transaction S3 PUT 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):"SGKHyalRU_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 qui a été appliquée.

Pour les objets répliqués, le champ LOCS inclut l'ID du nœud LDR et l'ID du volume des emplacements des 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 à codage d'effacement, le champ LOCS inclut l'ID du profil de codage d'effacement et l'ID du groupe de codage 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 PATH inclut des informations sur le bucket S3 et la clé ou des informations sur le conteneur et l'objet Swift, 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'objets

Vous pouvez identifier les transactions de suppression d'objet 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 suppression ne sont pas répertoriés dans les tableaux suivants. Seuls les messages nécessaires au suivi de la transaction de suppression sont inclus.

S3 supprime les messages d'audit

Code	Nom	Description	Tracer	Voir
SDEL	S3 Supprimer	Demande effectuée pour supprimer l'objet d'un bucket.	CBID, S3KY	"SDEL : SUPPRESSION S3"

Suppression rapide des messages d'audit

Code	Nom	Description	Tracer	Voir
WDEL	Suppression rapide	Demande effectuée pour supprimer l'objet d'un conteneur, ou le 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 d'audit.

> Tous les messages d'audit générés lors d'une transaction de suppression ne sont pas répertoriés dans l'exemple ci-dessous. Seuls ceux liés à la transaction de suppression S3 (SDEL) sont répertoriés.

SDEL : Suppression S3

La suppression d'objet commence lorsque le client envoie une demande DeleteObject à un service LDR. Le message contient le bucket à partir duquel supprimer l'objet et la clé S3 de l'objet, qui est utilisée pour 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):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
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'objets

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 nécessaires au suivi de la transaction de récupération sont inclus.

Messages d'audit de récupération S3

Code	Nom	Description	Tracer	Voir
SGET	GET S3	Demande effectuée pour récupérer un objet d'un bucket.	CBID, S3BK, S3KY	"SGET : S3 OBTENIR"

Messages d'audit de récupération rapide

Code	Nom	Description	Tracer	Voir
WGET	Swift GET	Demande effectuée pour récupérer un objet d'un conteneur.	CBID, WCON, WOBJ	"WGET : Swift GET"

Exemple : récupération d'objet 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 lors d'une transaction ne sont pas répertoriés dans l'exemple ci-dessous. Seuls ceux liés à la transaction de récupération S3 (SGET) sont répertoriés.

SGET : S3 OBTENIR

La récupération d'objet commence lorsque le client envoie une demande GetObject à un service LDR. Le message contient le bucket à partir duquel récupérer l'objet et la clé S3 de l'objet, qui est utilisée pour 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][CS
IZ(UI64):12][AVER(UI32):10][ATIM(UI64):1505947988782605]\[ATYP\(FC32\):SGE
T\][ANID(UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):17742374343649889669]
]
```

Si la politique de compartiment le permet, un client peut récupérer des objets de manière anonyme ou récupérer des objets à partir d'un compartiment appartenant à un autre compte de locataire. Le message d'audit contient des informations sur le compte locataire du propriétaire du bucket 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 bucket dont il n'est pas propriétaire. Les valeurs de SBAI et SBAC enregistrent l'ID et le nom du compte locataire du propriétaire du bucket, qui diffèrent de l'ID et du nom du compte locataire du client enregistrés

dans S3AI et SACC.

```
2017-09-20T22:53:15.876415
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):53244][SAIP(IPAD):"10.96.112.26"]\[S3AI
\(CSTR\):"17915054115450519830"\]\[SACC\(CSTR\):"s3-account-
b"\][S3AK(CSTR):"SGKHpoblWlP_kBkqSCbTi754Ls8lBUog67I2LlSiUg=="][SUSR(CSTR)
:"urn:sgws:identity::17915054115450519830:root"]\[SBAI\(CSTR\):"4397929817
8977966408"\]\[SBAC\(CSTR\):"s3-account-a"\][S3BK(CSTR):"bucket-
anonymous"][S3KY(CSTR):"Hello.txt"][CBID(UI64):0x83D70C6F1F662B02][CSIZ(UI
64):12][AVER(UI32):10][ATIM(UI64):1505947995876415][ATYP(FC32):SGET][ANID(
UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):6888780247515624902]]
```

Exemple : S3 Sélectionner 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 lors d'une transaction ne sont pas répertoriés dans l'exemple ci-dessous. Seuls ceux liés à la transaction S3 Select (SelectObjectContent) sont répertoriés.

Chaque requête génère deux messages d'audit : l'un qui exécute l'autorisation de la demande S3 Select (le champ S3SR est défini sur « select ») et une opération GET standard ultérieure 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][SAI
P(IPAD):"192.168.7.44"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Ten
ant1636027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:id
entity::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBA
C(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][SA
IP(IPAD):"192.168.7.44"][HTRH(CSTR):"{\"x-forwarded-
for\":\"unix:\"}"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Tenant16
36027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:identit
y::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBAC(CST
R):"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][A
MID(FC32):S3RQ][ATID(UI64):16562288121152341130]]
```

Messages de mise à jour des métadonnées

Les messages d'audit sont générés lorsqu'un client S3 met à jour les métadonnées d'un objet.

Messages d'audit de mise à jour des métadonnées S3

Code	Nom	Description	Tracer	Voir
SUPD	Métadonnées S3 mises à jour	Généré lorsqu'un client S3 met à jour les métadonnées d'un objet ingéré.	CBID, S3KY, HTRH	"SUPD : Métadonnées S3 mises à jour"

Exemple : mise à jour des métadonnées S3

L'exemple montre une transaction réussie pour mettre à jour les métadonnées d'un objet S3 existant.

SUPD : mise à jour des métadonnées S3

Le client S3 fait une demande (SUPD) pour 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 il a été configuré comme en-tête de protocole d'audit (**CONFIGURATION** > **Surveillance** > **Serveur d'audit et syslog**). Voir "Configurer 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 de filtrage des messages d’audit souhaité.

Les messages d’audit sont également répertoriés par ordre alphabétique en fonction de leurs codes 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, consultez"Configurer les

messages d’audit et les destinations des journaux"

Catégories de messages d’audit

Messages d’audit du système

Les messages d’audit appartenant à la catégorie d’audit système sont utilisés pour les événements liés au système d’audit lui-même, aux états des nœuds de grille, à l’activité des tâches à l’échelle du système (tâches de grille) et aux opérations de sauvegarde de service.

Code	Titre et description du message	Voir
ECMC	Fragment de données codées par effacement manquant : indique qu’un fragment de données codées par effacement manquant a été détecté.	"ECMC : Fragment de données codées par effacement manquant"
ECOC	Fragment de données codées par effacement corrompu : indique qu’un fragment de données codées par effacement corrompu a été détecté.	"ECOC : fragment de données corrompu et codé par effacement"
ETAF	Échec de l’authentification de sécurité : une tentative de connexion utilisant Transport Layer Security (TLS) a échoué.	"ETAF : échec de l’authentification de sécurité"
GNRG	Enregistrement GNDS : un service a mis à jour ou enregistré des informations le concernant dans le système StorageGRID .	"GNRG : Enregistrement GNDS"
GNUR	Désinscription GNDS : un service s’est désinscrit du système StorageGRID .	"GNUR : Désinscription 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 soumise au service CMN.	"GTSU : tâche de grille soumise"
LLST	Emplacement perdu : ce message d’audit est généré lorsqu’un emplacement est perdu.	"LLST : Localisation perdue"
OLST	Objet perdu : un objet demandé ne peut pas être localisé dans le système StorageGRID .	"OLST : le système a détecté un objet perdu"
SADD	Désactivation de l’audit de sécurité : la journalisation des messages d’audit a été désactivée.	"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 : un bloc de contenu a échoué aux contrôles de vérification.	"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 inconnu"
SYSD	Arrêt du nœud : un arrêt a été demandé.	"SYSD : arrêt du nœud"
SYST	Arrêt du nœud : un service a initié un arrêt gracieux.	"SYST : arrêt du nœud"
SYSU	Démarrage du nœud : un service a démarré ; la nature de l'arrêt précédent est indiquée dans le message.	"SYSU : démarrage du nœud"

Messages d'audit du stockage d'objets

Les messages d'audit appartenant à la catégorie d'audit de stockage d'objets sont utilisés pour les événements liés au stockage et à la gestion des objets au sein du système StorageGRID . Il s'agit notamment du stockage et de la récupération d'objets, des transferts de nœud de grille à nœud de grille et des vérifications.

> Les codes d'audit sont supprimés du produit et de la documentation à mesure que les fonctionnalités sont obsolètes. Si vous rencontrez un code d'audit qui n'est pas répertorié ici, vérifiez les versions précédentes de cette rubrique pour les anciennes versions de SG. Par exemple : "Messages d'audit du stockage d'objets StorageGRID 11.8" .

Code	Description	Voir
FRÈRE	Demande de lecture seule de bucket : un bucket est entré ou sorti du mode lecture seule.	"BROR : demande de lecture seule du bucket"
CBSE	Fin d'envoi de l'objet : l'entité source a terminé une opération de transfert de données de nœud de grille à nœud de grille.	"CBSE : Fin d'envoi d'objet"
CBRE	Fin de réception de l'objet : l'entité de destination a terminé une opération de transfert de données de nœud de grille à nœud de grille.	"CBRE : extrémité de réception d'objet"

Code	Description	Voir
CGRR	Demande de réplication inter-grille : StorageGRID a tenté une opération de réplication inter-grille pour répliquer des objets entre des buckets dans une connexion de fédération de grille.	"CGRR : demande de réplication inter-réseau"
EBDL	Suppression d'un compartiment vide : le scanner ILM a supprimé un objet dans un compartiment qui supprime tous les objets (effectuant une opération de vidage de compartiment).	"EBDL : Suppression du bucket vide"
EBKR	Demande de compartiment vide : un utilisateur a envoyé une demande pour activer ou désactiver le compartiment vide (c'est-à-dire pour supprimer des objets du compartiment ou pour arrêter la suppression d'objets).	"EBKR : demande de seau vide"
SCMT	Validation du magasin d'objets : un bloc de contenu a été entièrement stocké et vérifié et peut désormais être demandé.	"SCMT : demande de validation du magasin d'objets"
SREM	Supprimer le 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"

Le client lit les messages d'audit

Les messages d'audit de lecture du client sont enregistrés lorsqu'une application client S3 effectue une demande de récupération d'un objet.

Code	Description	Utilisé par	Voir
S3SL	Requête S3 Select : enregistre une fin après qu'une requête S3 Select a été renvoyée au client. Le message S3SL peut inclure des détails sur le message d'erreur et le code d'erreur. La demande n'a peut-être pas abouti.	Client S3	"S3SL : Demande de sélection S3"
SGET	S3 GET : enregistre une transaction réussie pour récupérer un objet ou répertorier les objets dans un bucket. **Remarque :** si la transaction fonctionne sur une sous-ressource, le message d'audit inclura le champ S3SR.	Client S3	"SGET : S3 OBTENIR"
KARITÉ	S3 HEAD : enregistre une transaction réussie pour vérifier l'existence d'un objet ou d'un bucket.	Client S3	"SHEA : TÊTE S3"

Code	Description	Utilisé par	Voir
WGET	Swift GET : enregistre une transaction réussie pour récupérer un objet ou répertorier les objets dans un conteneur.	Client Swift	"WGET : Swift GET"
WHEA	Swift HEAD : enregistre une transaction réussie pour vérifier l'existence d'un objet ou d'un conteneur.	Client Swift	"WHEA : TÊTE RAPIDE"

Le client écrit des messages d'audit

Les messages d'audit d'écriture client sont enregistrés lorsqu'une application client S3 effectue une demande de création ou de modification d'un objet.

Code	Description	Utilisé par	Voir
OVWR	Écrasement d'objet : enregistre une transaction pour écraser un objet par un autre objet.	Clients S3 et Swift	"OVWR : écrasement d'objet"
SDEL	S3 DELETE : enregistre une transaction réussie pour supprimer un objet ou un bucket. **Remarque :** si la transaction fonctionne sur une sous-ressource, le message d'audit inclura le champ S3SR.	Client S3	"SDEL : SUPPRESSION S3"
SPOS	S3 POST : enregistre une transaction réussie pour restaurer un objet du stockage AWS Glacier vers un pool de stockage cloud.	Client S3	"SPOS : POST S3"
CRACHER	S3 PUT : enregistre une transaction réussie pour créer un nouvel objet ou un nouveau bucket. **Remarque :** si la transaction fonctionne sur une sous-ressource, le message d'audit inclura le champ S3SR.	Client S3	"SPUT : S3 PUT"
SUPD	Métadonnées S3 mises à jour : enregistre une transaction réussie pour mettre à jour les métadonnées d'un objet ou d'un compartiment existant.	Client S3	"SUPD : Métadonnées S3 mises à jour"
WDEL	Swift DELETE : enregistre une transaction réussie pour supprimer un objet ou un conteneur.	Client Swift	"WDEL : SUPPRESSION rapide"
WPUT	Swift PUT : enregistre une transaction réussie pour créer un nouvel objet ou conteneur.	Client Swift	"WPUT : Swift PUT"

Message d'audit de gestion

La catégorie Gestion enregistre les demandes des utilisateurs dans l'API de gestion.

Code	Titre et description du message	Voir
MGAU	Message d'audit de l'API de gestion : un journal des demandes des utilisateurs.	"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 de l'information (ILM).

Code	Titre et description du message	Voir
IDEL	Suppression initiée par ILM : ce message d'audit est généré lorsque ILM démarre le processus de suppression d'un objet.	"IDEL : suppression initiée par ILM"
LKCU	Nettoyage des objets écrasés. Ce message d'audit est généré lorsqu'un objet écrasé est automatiquement supprimé pour libérer de l'espace de stockage.	"LKCU : Nettoyage des objets écrasés"
ORLM	Règles d'objet respectées : ce message d'audit est généré lorsque les données d'objet sont stockées comme spécifié par les règles ILM.	"ORLM : Règles d'objet respectées"

Référence du message d'audit

BROR : demande de lecture seule du bucket

Le service LDR génère ce message d'audit lorsqu'un bucket entre ou sort du mode lecture seule. Par exemple, un bucket entre en mode lecture seule pendant que tous les objets sont supprimés.

Code	Champ	Description
BKHD	UUID du bucket	L'ID du bucket.
BROV	Valeur de la demande en lecture seule du bucket	Si le bucket est mis en lecture seule ou quitte l'état de lecture seule (1 = lecture seule, 0 = non en lecture seule).
FRÈRES	Raison de lecture seule du bucket	La raison pour laquelle le bucket est mis en lecture seule ou quitte l'état de lecture seule. Par exemple, emptyBucket.

Code	Champ	Description
S3AI	ID de compte locataire S3	L'ID du compte locataire qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Godet S3	Le nom du bucket S3.

CBRB : Début de la réception de l'objet

Lors du fonctionnement normal du système, les blocs de contenu sont continuellement transférés entre différents nœuds à mesure que les données sont consultées, répliquées et conservées. Lorsque le transfert d'un bloc de contenu d'un nœud à un autre est initié, ce message est émis par l'entité de destination.

Code	Champ	Description
CNID	Identifiant de connexion	L'identifiant unique de la session/connexion nœud à nœud.
CBID	Identifiant du bloc de contenu	L'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. PULL : L'opération de transfert a été demandée par l'entité réceptrice.
CTSR	Entité source	L'ID du nœud de la source (expéditeur) du transfert CBID.
CTDS	Entité de destination	L'ID du nœud de destination (récepteur) du transfert CBID.
CTSS	Démarrage du comptage de séquences	Indique le premier nombre de séquences demandé. En cas de succès, le transfert commence à partir de ce décompte de séquence.
CTES	Nombre de séquences de fin attendu	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 de transfert	Statut au moment du début du transfert : SUCS : Le transfert a démarré avec succès.

Ce message d'audit signifie qu'une opération de transfert de données de nœud à nœud a été lancée sur un seul élément de contenu, tel qu'identifié par son identifiant de bloc de contenu. L'opération demande des données allant du « Nombre de séquences de début » au « Nombre de séquences de fin attendu ». Les nœuds d'envoi et de réception sont identifiés par leurs identifiants de nœud. Ces informations peuvent être

utilisées pour suivre le flux de données du système et, lorsqu'elles sont combinées avec des messages d'audit de stockage, pour vérifier le nombre de réplicas.

CBRE : extrémité de réception d'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	Identifiant de connexion	L'identifiant unique de la session/connexion nœud à nœud.
CBID	Identifiant du bloc de contenu	L'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. PULL : L'opération de transfert a été demandée par l'entité réceptrice.
CTSR	Entité source	L'ID du nœud de la source (expéditeur) du transfert CBID.
CTDS	Entité de destination	L'ID du nœud de destination (récepteur) du transfert CBID.
CTSS	Démarrage du comptage de séquences	Indique le nombre de séquences sur lequel le transfert a commencé.
CTAS	Nombre réel de séquences finales	Indique le dernier nombre de séquences transférées avec succès. Si le nombre réel de séquences de fin est identique au nombre réel de séquences de début et que le résultat du transfert n'a pas réussi, aucune donnée n'a été échangée.
RSLT	Résultat du transfert	Le résultat de l'opération de transfert (du point de vue de l'entité expéditrice) : SUCS : transfert terminé avec succès ; tous les comptages de séquences demandés ont été envoyés. CONL : connexion perdue pendant le transfert CTMO : connexion expirée lors de l'établissement ou du transfert UNRE : ID du nœud de destination inaccessible CRPT : transfert terminé en raison de la réception de données corrompues ou invalides

Ce message d'audit signifie qu'une opération de transfert de données de nœud à nœud a été effectuée. Si le résultat du transfert a réussi, l'opération a transféré les données de « Nombre de séquences de départ » vers « Nombre de séquences de fin réel ». Les nœuds d'envoi et de réception sont identifiés par leurs identifiants de nœud. Ces informations peuvent être utilisées pour suivre le flux de données du système et pour localiser, tabuler et analyser les erreurs. Associé à des messages d'audit de stockage, il peut également être utilisé pour vérifier le nombre de réplicas.

CBSB : Début de l'envoi de l'objet

Lors du fonctionnement normal du système, les blocs de contenu sont continuellement transférés entre différents nœuds à mesure que les données sont consultées, répliquées et conservées. Lorsque le transfert d'un bloc de contenu d'un nœud à un autre est initié, ce message est émis par l'entité source.

Code	Champ	Description
CNID	Identifiant de connexion	L'identifiant unique de la session/connexion nœud à nœud.
CBID	Identifiant du bloc de contenu	L'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. PULL : L'opération de transfert a été demandée par l'entité réceptrice.
CTSR	Entité source	L'ID du nœud de la source (expéditeur) du transfert CBID.
CTDS	Entité de destination	L'ID du nœud de destination (récepteur) du transfert CBID.
CTSS	Démarrage du comptage de séquences	Indique le premier nombre de séquences demandé. En cas de succès, le transfert commence à partir de ce décompte de séquence.
CTES	Nombre de séquences de fin attendu	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 de transfert	Statut au moment du début du transfert : SUCS : le transfert a démarré avec succès.

Ce message d'audit signifie qu'une opération de transfert de données de nœud à nœud a été lancée sur un seul élément de contenu, tel qu'identifié par son identifiant de bloc de contenu. L'opération demande des données allant du « Nombre de séquences de début » au « Nombre de séquences de fin attendu ». Les nœuds d'envoi et de réception sont identifiés par leurs identifiants de nœud. Ces informations peuvent être utilisées pour suivre le flux de données du système et, lorsqu'elles sont combinées avec des messages d'audit

de stockage, pour vérifier le nombre de réplicas.

CBSE : Fin d'envoi d'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	Identifiant de connexion	L'identifiant unique de la session/connexion nœud à nœud.
CBID	Identifiant du bloc de contenu	L'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. PULL : L'opération de transfert a été demandée par l'entité réceptrice.
CTSR	Entité source	L'ID du nœud de la source (expéditeur) du transfert CBID.
CTDS	Entité de destination	L'ID du nœud de destination (récepteur) du transfert CBID.
CTSS	Démarrage du comptage de séquences	Indique le nombre de séquences sur lequel le transfert a commencé.
CTAS	Nombre réel de séquences finales	Indique le dernier nombre de séquences transférées avec succès. Si le nombre réel de séquences de fin est identique au nombre réel de séquences de début et que le résultat du transfert n'a pas réussi, aucune donnée n'a été échangée.
RSLT	Résultat du transfert	Le résultat de l'opération de transfert (du point de vue de l'entité expéditrice) : SUCS : transfert terminé avec succès ; tous les comptages de séquences demandés ont été envoyés. CONL : connexion perdue pendant le transfert CTMO : connexion expirée lors de l'établissement ou du transfert UNRE : ID du nœud de destination inaccessible CRPT : transfert terminé en raison de la réception de données corrompues ou invalides

Ce message d'audit signifie qu'une opération de transfert de données de nœud à nœud a été effectuée. Si le

résultat du transfert a réussi, l'opération a transféré les données de « Nombre de séquences de départ » vers « Nombre de séquences de fin réel ». Les nœuds d'envoi et de réception sont identifiés par leurs identifiants de nœud. Ces informations peuvent être utilisées pour suivre le flux de données du système et pour localiser, tabuler et analyser les erreurs. Associé à des messages d'audit de stockage, il peut également être utilisé pour vérifier le nombre de réplicas.

CGRR : demande de réplication inter-réseau

Ce message est généré lorsque StorageGRID tente une opération de réplication inter-grille pour répliquer des objets entre des buckets dans une connexion de fédération de grille.

Code	Champ	Description
CSIZ	Taille de l'objet	La taille de l'objet en octets. L'attribut CSIZ a été introduit dans StorageGRID 11.8. Par conséquent, les demandes de réplication inter-grille couvrant une mise à niveau de StorageGRID 11.7 vers 11.8 peuvent avoir une taille d'objet totale inexacte.
S3AI	ID de compte locataire S3	L'ID du compte locataire propriétaire du bucket à partir duquel l'objet est répliqué.
GFID	ID de connexion à la fédération de grille	L'ID de la connexion de fédération de grille utilisée pour la réplication inter-grille.
OPÉRER	Opération CGR	Le type d'opération de réplication inter-grille qui a été tenté : • 0 = Répliquer l'objet • 1 = Répliquer l'objet en plusieurs parties • 2 = Répliquer le marqueur de suppression
S3BK	Godet S3	Le nom du bucket S3.
S3KY	Touche S3	Le nom de la clé S3, sans inclure le nom du bucket.
VSID	ID de version	L'ID de version de la version spécifique d'un objet en cours de réplication.
RSLT	Code de résultat	Renvoie une erreur réussie (SUCS) ou générale (GERR).

EBDL : Suppression du bucket vide

Le scanner ILM a supprimé un objet dans un bucket qui supprime tous les objets (effectuant une opération de bucket vide).

Code	Champ	Description
CSIZ	Taille de l'objet	La taille de l'objet en octets.
CHEMIN	Seau/clé S3	Le nom du compartiment S3 et le 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	L'identifiant de l'objet dans le système StorageGRID .
RSLT	Résultat de l'opération de suppression	Le résultat d'un événement, d'un processus ou d'une transaction. Si ce n'est pas pertinent pour un message, NONE est utilisé plutôt que SUCS afin que le message ne soit pas filtré accidentellement.

EBKR : demande de seau vide

Ce message indique qu'un utilisateur a envoyé une demande pour activer ou désactiver le compartiment vide (c'est-à-dire pour supprimer des objets du compartiment ou pour arrêter la suppression d'objets).

Code	Champ	Description
CONSTRUIRE	UUID du bucket	L'ID du bucket.
EBJS	Configuration JSON du bucket vide	Contient le JSON représentant la configuration actuelle du bucket vide.
S3AI	ID de compte locataire S3	L'ID du compte locataire de l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Godet S3	Le nom du bucket S3.

ECMC : Fragment de données codées par effacement manquant

Ce message d'audit indique que le système a détecté un fragment de données codé par effacement manquant.

Code	Champ	Description
VCMC	ID VCS	Le nom du VCS qui contient le bloc manquant.
MCID	ID de bloc	L'identifiant du fragment codé par effacement manquant.

Code	Champ	Description
RSLT	Résultat	Ce champ a la valeur « AUCUN ». RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message particulier. « NONE » est utilisé plutôt que « SUCS » afin que ce message ne soit pas filtré.

ECOC : fragment de données corrompu et codé par effacement

Ce message d'audit indique que le système a détecté un fragment de données codé par effacement corrompu.

Code	Champ	Description
VCCO	ID VCS	Le nom du VCS qui contient le bloc corrompu.
VLID	ID du volume	Le volume RangeDB qui contient le fragment codé par effacement corrompu.
CCID	ID de bloc	L'identifiant du fragment codé par effacement corrompu.
RSLT	Résultat	Ce champ a la valeur « AUCUN ». RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message particulier. « NONE » est utilisé plutôt que « SUCS » afin que ce message ne soit pas filtré.

ETAF : échec de l'authentification de sécurité

Ce message est généré lorsqu'une tentative de connexion utilisant Transport Layer Security (TLS) a échoué.

Code	Champ	Description
CNID	Identifiant de connexion	L'identifiant système unique pour la connexion TCP/IP sur laquelle l'authentification a échoué.
RUID	Identité de l'utilisateur	Un identifiant dépendant du service représentant l'identité de l'utilisateur distant.

Code	Champ	Description
RSLT	Code de raison	La raison de l'échec : SCNI : l'établissement de la connexion sécurisée a échoué. CERM : Le certificat était manquant. CERT : Le certificat n'était pas valide. CERE : Le certificat a expiré. CERR : Le certificat a été révoqué. CSGN : la signature du certificat n'était pas valide. CSGU : le signataire du certificat était inconnu. UCRM : les informations d'identification de l'utilisateur étaient manquantes. UCRI : les informations d'identification de l'utilisateur n'étaient pas valides. UCRU : les informations d'identification de l'utilisateur n'ont pas été autorisées. TOUT : L'authentification a expiré.

Lorsqu'une connexion est établie avec un service sécurisé qui utilise TLS, les informations d'identification de l'entité distante sont vérifiées à l'aide du profil TLS et d'une logique supplémentaire intégrée au service. Si cette authentification échoue en raison de certificats ou d'informations d'identification non valides, inattendus ou non autorisés, un message d'audit est enregistré. Cela permet d'effectuer des requêtes sur les tentatives d'accès non autorisées et d'autres problèmes de connexion liés à la sécurité.

Le message peut résulter d'une entité distante ayant une configuration incorrecte ou de tentatives de présentation d'informations d'identification non valides ou non autorisées 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 le concernant dans le système StorageGRID .

Code	Champ	Description
RSLT	Résultat	Le résultat de la demande de mise à jour : • SUCS : Réussi • SUNV : Service indisponible • GERR : Autre échec

Code	Champ	Description
GNID	Nœud ID	L'ID de nœud du service qui a initié la demande de mise à jour.
GNTP	Type d'appareil	Le type de périphérique du nœud de grille (par exemple, BLDR pour un service LDR).
GNDV	Version du modèle d'appareil	La chaîne identifiant la version du modèle de périphérique du nœud de grille dans le bundle DMDL.
GNGP	Groupe	Le groupe auquel appartient le nœud de grille (dans le contexte des coûts de liaison et du classement des requêtes de service).
GNIA	Adresse IP	L'adresse IP du nœud de grille.

Ce message est généré chaque fois qu'un nœud de grille met à jour son entrée dans le bundle de nœuds de grille.

GNUR : Désinscription GNDS

Le service CMN génère ce message d'audit lorsqu'un service dispose d'informations non enregistrées le concernant auprès du système StorageGRID .

Code	Champ	Description
RSLT	Résultat	Le résultat de la demande de mise à jour : • SUCS : Réussi • SUNV : Service indisponible • GERR : Autre échec
GNID	Nœud ID	L'ID de nœud du service qui a initié 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 SUCS, ABRT ou ROLF, un message d'audit correspondant indiquant que la tâche de grille a démarré s'affichera. Les autres résultats indiquent que le traitement de cette tâche de grille n'a jamais commencé.

Code	Champ	Description
TSID	ID de tâche	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. **Remarque :** l'ID de tâche est attribué au moment où une tâche de grille est générée, et non au moment où elle est soumise. Il est possible qu'une tâche de grille donnée soit soumise plusieurs fois et, dans ce cas, le champ ID de tâche n'est pas suffisant pour lier de manière unique les messages d'audit Soumis, Démarré et Terminé.
RSLT	Résultat	Le résultat final de la tâche de grille : • SUCS : la tâche de grille s'est terminée avec succès. • ABRT : la tâche de grille a été terminée sans erreur de restauration. • ROLF : La tâche de grille a été interrompue et n'a pas pu terminer le processus de restauration. • CANC : la tâche de grille a été annulée par l'utilisateur avant d'être démarrée. • EXPR : La tâche de grille a expiré avant d'avoir été démarrée. • IVLD : La tâche de grille n'était pas valide. • AUTH : La tâche de grille n'était pas autorisée. • DUPL : la tâche de grille a été rejetée comme doublon.

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 Tâche de grille soumise pour les tâches de grille initiées par le service de soumission de tâche de grille interne 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
TSID	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. **Remarque :** l'ID de tâche est attribué au moment où une tâche de grille est générée, et non au moment où elle est soumise. Il est possible qu'une tâche de grille donnée soit soumise plusieurs fois et, dans ce cas, le champ ID de tâche n'est pas suffisant pour lier de manière unique les messages d'audit Soumis, Démarré et Terminé.
RSLT	Résultat	Le résultat. Ce champ n'a qu'une seule valeur : • SUCS : 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 soumise au service CMN.

Code	Champ	Description
TSID	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. **Remarque :** l'ID de tâche est attribué au moment où une tâche de grille est générée, et non au moment où elle est soumise. Il est possible qu'une tâche de grille donnée soit soumise plusieurs fois et, dans ce cas, le champ ID de tâche n'est pas suffisant pour lier de manière unique les messages d'audit Soumis, Démarré et Terminé.
TTYP	Type de tâche	Le type de tâche de grille.
TVER	Version de la tâche	Un numéro indiquant la version de la tâche de grille.
TDSC	Description de la tâche	Une description lisible par l'homme de la tâche de grille.
TVA	Valide après l'horodatage	L'heure la plus ancienne (UINT64 microsecondes à partir du 1er janvier 1970 - heure UNIX) à laquelle la tâche de grille est valide.
VBTS	Valide avant l'horodatage	La dernière heure (UINT64 microsecondes à partir du 1er janvier 1970 - heure UNIX) à laquelle la tâche de grille est valide.
TSRC	Source	La source de la tâche : • TXTB : la tâche de grille a été soumise via le système StorageGRID sous la forme d'un bloc de texte signé. • GRILLE : la tâche de grille a été soumise via le service de soumission de tâches de grille interne.
ACTV	Type d'activation	Le type d'activation : • AUTO : La tâche de grille a été soumise à une activation automatique. • PEND : la tâche de grille a été soumise dans la table en attente. C'est la seule possibilité pour la source TXTB.
RSLT	Résultat	Le résultat de la soumission : • SUCS : la tâche de grille a été soumise avec succès. • ÉCHEC : La tâche a été déplacée directement vers la table historique.

IDEL : suppression initiée par ILM

Ce message est généré lorsque ILM démarre le processus de suppression d'un objet.

Le message IDEL est généré dans l'une de ces situations :

- **Pour les objets dans les compartiments S3 conformes** : ce message est généré lorsque ILM démarre le processus de suppression automatique d'un objet car 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 buckets S3 non conformes**. Ce message est généré lorsque ILM démarre le processus de suppression d'un objet car aucune instruction de placement dans les stratégies ILM actives ne s'applique actuellement à l'objet.

Code	Champ	Description
CBID	Identifiant du bloc de contenu	Le CBID de l'objet.
CMPA	Conformité : Suppression automatique	Pour les objets dans les buckets S3 conformes uniquement. 0 (faux) ou 1 (vrai), indiquant si un objet conforme doit être supprimé automatiquement à la fin de sa période de conservation, à moins que le bucket ne soit soumis à une suspension légale.
CMPL	Conformité : Conservation légale	Pour les objets dans les buckets S3 conformes uniquement. 0 (faux) ou 1 (vrai), indiquant si le bucket est actuellement sous une suspension légale.
CMPR	Conformité : Durée de conservation	Pour les objets dans les buckets S3 conformes uniquement. La durée de la période de rétention de l'objet en minutes.
CTME	Conformité : Heure d'ingestion	Pour les objets dans les buckets S3 conformes uniquement. L'heure 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 bucket.
DMRK	Supprimer l'ID de version du marqueur	L'ID de version du marqueur de suppression créé lors de la suppression d'un objet d'un bucket versionné. Les opérations sur les buckets n'incluent pas ce champ.
CSIZ	Taille du contenu	La taille de l'objet en octets.

Code	Champ	Description
LOC	Emplacements	L'emplacement de stockage des données d'objet dans le système StorageGRID . La valeur de LOCS est "" si l'objet n'a aucun emplacement (par exemple, il a été supprimé). CLEC : pour les objets à codage d'effacement, l'ID de profil de codage d'effacement et l'ID de groupe de codage d'effacement appliqué aux données de l'objet. CLDI : pour les objets répliqués, l'ID du nœud LDR et l'ID du volume de l'emplacement de l'objet. CLNL : ID du nœud ARC de l'emplacement de l'objet si les données de l'objet sont archivées.
CHEMIN	Seau/clé S3	Le nom du compartiment S3 et le nom de la clé S3.
RSLT	Résultat	Le résultat de l'opération ILM. SUCS : L'opération ILM a réussi.
RÈGLE	Étiquette des règles	• Si un objet dans un compartiment S3 conforme est supprimé automatiquement parce que sa période de conservation a expiré, ce champ est vide. • Si l'objet est supprimé parce qu'il n'existe 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 qui s'appliquait à l'objet.
SGRP	Site (Groupe)	Si présent, l'objet a été supprimé sur le site spécifié, qui n'est pas le site où l'objet a été ingéré.
UUID	Identifiant unique universel	L'identifiant de l'objet dans le système StorageGRID .
VSID	ID de version	L'ID de version de la version spécifique d'un objet qui a été supprimé. Les opérations sur les buckets et les objets dans les buckets non versionnés n'incluent pas ce champ.

LKCU : Nettoyage des objets écrasés

Ce message est généré lorsque StorageGRID supprime un objet écrasé qui nécessitait auparavant un nettoyage pour libérer de l'espace de stockage. Un objet est écrasé lorsqu'un client S3 écrit un objet dans un chemin contenant déjà un objet. Le processus de suppression se produit automatiquement et en arrière-plan.

Code	Champ	Description
CSIZ	Taille du contenu	La taille de l'objet en octets.
LTYP	Type de nettoyage	*Usage interne uniquement.*
LUID	UUID de l'objet supprimé	L'identifiant de l'objet qui a été supprimé.
CHEMIN	Seau/clé S3	Le nom du compartiment S3 et le 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	L'identifiant de l'objet qui existe encore. Cette valeur n'est disponible que si l'objet n'a pas été supprimé.

LKDM : Nettoyage des objets divulgués

Ce message est généré lorsqu'un fragment divulgué a été nettoyé ou supprimé. Un bloc peut faire partie d'un objet répliqué ou d'un objet codé par effacement.

Code	Champ	Description
CLOC	Emplacement du bloc	Le chemin du fichier du morceau divulgué qui a été supprimé.

CTYP	Type de morceau	Type de morceau :
		
		`ec: Erasure-coded object chunk`
		
		`repl: Replicated object chunk`

Code	Champ	Description

LTYP	Type de fuite	Les cinq types de fuites qui peuvent être détectées :
		
		`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 du bloc	Il est temps que le morceau divulgué soit créé.
UUID	Identifiant unique universel	L’identifiant de l’objet auquel appartient le bloc.
CBID	Identifiant du bloc de contenu	CBID de l’objet auquel appartient le fragment divulgué.
CSIZ	Taille du contenu	La taille du bloc en octets.

LLST : Localisation perdue

Ce message est généré chaque fois qu’un emplacement pour une copie d’objet (répliquée ou codée par effacement) ne peut pas être trouvé.

Code	Champ	Description
CBIL	CBID	Le CBID affecté.
ECPR	Profil de codage d’effacement	Pour les données d’objet codées par effacement. L’ID du profil de codage d’effacement utilisé.
LTYP	Type d’emplacement	CLDI (en ligne) : pour les données d’objets répliquées CLEC (en ligne) : pour les données d’objets codées par effacement CLNL (Nearline) : pour les données d’objets répliquées archivées

Code	Champ	Description
NOID	ID du nœud source	L'ID du nœud sur lequel les emplacements ont été perdus.
PCLD	Chemin vers l'objet répliqué	Le 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 la forme `/var/local/rangedb/2/p/13/13/00oJs6X%{h{U)SeUFxE@`
RSLT	Résultat	Toujours AUCUN. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message. NONE est utilisé plutôt que SUCS afin que ce message ne soit pas filtré.
TSRC	Source de déclenchement	UTILISATEUR : Déclenché par l'utilisateur SYST : système déclenché
UUID	ID unique universel	L'identifiant de l'objet affecté dans le système StorageGRID .

MGAU : Message d'audit de gestion

La catégorie Gestion enregistre les demandes des utilisateurs dans l'API de gestion. Chaque requête HTTP qui n'est pas une requête GET ou HEAD vers un URI d'API valide enregistre une réponse contenant le nom d'utilisateur, l'IP et le type de requête vers l'API. Les URI d'API non valides (tels que /api/v3-authorize) et les demandes non valides adressées à des URI d'API valides ne sont pas enregistrées.

Code	Champ	Description
MDIP	Adresse IP de destination	L'adresse IP du serveur (destination).
MDNA	Nom de domaine	Le nom de domaine de l'hôte.
MPAT	Demande PATH	Le chemin de la demande.
MPQP	Paramètres de requête de demande	Les paramètres de requête pour la demande.

Code	Champ	Description
MRBD	Corps de la requête	Le contenu du corps de la requête. Alors que le corps de la réponse est enregistré par défaut, le corps de la demande est enregistré dans certains cas lorsque le corps de la réponse est vide. Étant donné que les informations suivantes ne sont pas disponibles dans le corps de la réponse, elles sont extraites du corps de la requête pour les méthodes POST suivantes : • Nom d'utilisateur et identifiant de compte dans **POST authorize** • Nouvelle configuration des sous-réseaux dans **POST /grid/grid-networks/update** • Nouveaux serveurs NTP dans **POST /grid/ntp-servers/update** • ID de serveur mis hors service dans **POST /grid/servers/decommission** **Remarque :** les informations sensibles sont soit supprimées (par exemple, une clé d'accès S3), soit masquées par des astérisques (par exemple, un mot de passe).
MRMD	Méthode de requête	La méthode de requête HTTP : • POSTE • METTRE • SUPPRIMER • CORRECTIF
MRSC	Code de réponse	Le code de réponse.
MRSP	Corps de la réponse	Le contenu de la réponse (le corps de la réponse) est enregistré par défaut. **Remarque :** les informations sensibles sont soit supprimées (par exemple, une clé d'accès S3), soit masquées par des astérisques (par exemple, un mot de passe).
MSIP	Adresse IP source	L'adresse IP du client (source).
MUUN	URN de l'utilisateur	L'URN (nom de ressource uniforme) de l'utilisateur qui a envoyé la demande.
RSLT	Résultat	Renvoie une réussite (SUCS) ou l'erreur signalée par le backend.

OLST : le système a détecté un objet perdu

Ce message est généré lorsque le service DDS ne parvient pas à localiser de copies

d’un objet dans le système StorageGRID .

Code	Champ	Description
CBID	Identifiant du bloc de contenu	Le CBID de l’objet perdu.
NOID	Nœud ID	Si disponible, le dernier emplacement direct ou proche connu de l’objet perdu. Il est possible d’avoir uniquement l’ID de nœud sans ID de volume si les informations de volume ne sont pas disponibles.
CHEMIN	Seau/clé S3	Si disponible, le nom du compartiment S3 et le nom de la clé S3.
RSLT	Résultat	Ce champ a la valeur AUCUN. RSLT est un champ de message obligatoire, mais n’est pas pertinent pour ce message. NONE est utilisé plutôt que SUCS afin que ce message ne soit pas filtré.
UUID	ID unique universel	L’identifiant de l’objet perdu dans le système StorageGRID .
VOLI	ID du volume	Si 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 avec succès comme spécifié par les règles ILM.

> Le message ORLM n’est pas généré lorsqu’un objet est stocké avec succès par la règle par défaut Créer 2 copies si une autre règle de la stratégie utilise le filtre avancé Taille de l’objet.

Code	Champ	Description
CONSTRUIRE	En-tête de godet	Champ d’ID du bucket. Utilisé pour les opérations internes. Apparaît uniquement si STAT est PRGD.
CBID	Identifiant du bloc de contenu	Le CBID de l’objet.
CSIZ	Taille du contenu	La taille de l’objet en octets.

Code	Champ	Description
LOC	Emplacements	L'emplacement de stockage des données d'objet dans le système StorageGRID . La valeur de LOCS est "" si l'objet n'a aucun emplacement (par exemple, il a été supprimé). CLEC : pour les objets à codage d'effacement, l'ID de profil de codage d'effacement et l'ID de groupe de codage d'effacement appliqué aux données de l'objet. CLDI : pour les objets répliqués, l'ID du nœud LDR et l'ID du volume de l'emplacement de l'objet. CLNL : ID du nœud ARC de l'emplacement de l'objet si les données de l'objet sont archivées.
CHEMIN	Seau/clé S3	Le nom du compartiment S3 et le nom de la clé S3.
RSLT	Résultat	Le résultat de l'opération ILM. SUCS : L'opération ILM a réussi.
RÈGLE	Étiquette des règles	L'étiquette lisible par l'homme attribuée 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	Conteneur CBID	CBID du conteneur pour l'objet segmenté. Cette valeur est disponible uniquement pour les objets segmentés et en plusieurs parties.
STAT	Statut	L'état de fonctionnement de l'ILM. TERMINÉ : les opérations ILM sur l'objet sont terminées. DFER : L'objet a été marqué pour une future réévaluation ILM. PRGD : l'objet a été supprimé du système StorageGRID . NLOC : les données de l'objet ne peuvent plus être trouvées dans le système StorageGRID . Ce statut peut indiquer que toutes les copies des données de l'objet sont manquantes ou endommagées.
UUID	Identifiant unique universel	L'identifiant de l'objet dans le système StorageGRID .
VSID	ID de version	L'ID de version d'un nouvel objet créé dans un bucket versionné. Les opérations sur les buckets et les objets dans les buckets non versionnés n'incluent pas ce champ.

Le message d'audit ORLM peut être émis plusieurs fois pour un même objet. Par exemple, il est émis chaque

fois que l'un des événements suivants se produit :

- Les règles ILM pour l'objet sont satisfaites pour toujours.
- Les règles ILM pour 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 répliquées est corrompue. Le système StorageGRID effectue une évaluation ILM pour remplacer l'objet corrompu.

Informations connexes

- "Transactions d'ingestion d'objets"
- "Transactions de suppression d'objets"

OVWR : écrasement d'objet

Ce message est généré lorsqu'une opération externe (demandée par le client) entraîne l'écrasement d'un objet par un autre objet.

Code	Champ	Description
CBID	Identifiant du bloc de contenu (nouveau)	Le CBID du nouvel objet.
CSIZ	Taille de l'objet précédent	La taille, en octets, de l'objet écrasé.
trouble obsessionnel compulsif (TOC)	Identifiant du bloc de contenu (précédent)	Le CBID de l'objet précédent.
UUID	ID unique universel (nouveau)	L'identifiant du nouvel objet dans le système StorageGRID .
OUID	ID unique universel (précédent)	L'identifiant de l'objet précédent dans le système StorageGRID .
CHEMIN	Chemin de l'objet S3	Le chemin d'accès à l'objet S3 utilisé pour l'objet précédent et le nouvel objet
RSLT	Code de résultat	Résultat de la transaction d'écrasement d'objet. Le résultat est toujours : SUCS : Réussi
SGRP	Site (Groupe)	Si présent, l'objet écrasé a été supprimé sur le site spécifié, qui n'est pas le site où l'objet écrasé a été ingéré.

S3SL : Demande de sélection S3

Ce message enregistre une fin après qu'une demande S3 Select a été renvoyée au client. Le message S3SL peut inclure des détails sur le message d'erreur et le 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 sera le nombre d'octets après décompression.
BYPR	Octets traités	Nombre d'octets traités. Indique combien d'octets de « Octets analysés » ont été réellement traités ou traités par une tâche S3 Select.
BYRT	Octets renvoyés	Nombre d'octets qu'une tâche S3 Select a renvoyé au client.
REPR	Enregistrements traités	Nombre d'enregistrements ou de lignes qu'une tâche S3 Select a reçus des nœuds de stockage.
RERT	Dossiers retournés	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 cela est faux, la tâche n'a pas pu se terminer et les champs d'erreur contiendront probablement des données. Le client a peut-être reçu des résultats partiels, voire aucun résultat du tout.
REID	ID de la demande	Identifiant de la demande S3 Select.
EXTM	Temps d'exécution	Le temps, en secondes, qu'il a fallu pour terminer la tâche S3 Select.
ERMG	Message d'erreur	Message d'erreur généré par la tâche S3 Select.
ERTY	Type d'erreur	Type d'erreur généré par le travail S3 Select.
ERST	Trace de pile d'erreurs	Erreur Stacktrace générée par le travail S3 Select.
S3BK	Godet S3	Le nom du bucket S3.

Code	Champ	Description
S3AK	ID de clé d'accès S3 (expéditeur de la demande)	L'ID de clé d'accès S3 pour l'utilisateur qui a envoyé la demande.
S3AI	ID de compte locataire S3 (expéditeur de la demande)	L'ID du compte locataire de l'utilisateur qui a envoyé la demande.
S3KY	Touche S3	Le nom de la clé S3, sans inclure le nom du bucket.

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 ni livrés.

Code	Champ	Description
AETM	Méthode d'activation	La méthode utilisée pour désactiver l'audit.
AEUN	Nom d'utilisateur	Le nom d'utilisateur qui a exécuté la commande pour désactiver la journalisation d'audit.
RSLT	Résultat	Ce champ a la valeur AUCUN. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message. NONE est utilisé plutôt que SUCS afin que ce message ne soit pas filtré.

Le message implique que la journalisation était auparavant activée, mais qu'elle est désormais désactivée. Ceci est généralement utilisé uniquement lors de l'ingestion en masse pour améliorer les performances du système. Suite à l'activité en masse, l'audit est restauré (SADE) et la possibilité de désactiver l'audit est alors définitivement bloquée.

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 à nouveau collectés et livrés.

Code	Champ	Description
AETM	Méthode d'activation	La méthode utilisée pour permettre l'audit.
AEUN	Nom d'utilisateur	Le nom d'utilisateur qui a exécuté la commande pour activer la journalisation d'audit.

Code	Champ	Description
RSLT	Résultat	Ce champ a la valeur AUCUN. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message. NONE est utilisé plutôt que SUCS afin que ce message ne soit pas filtré.

Le message implique que la journalisation était auparavant désactivée (SADD), mais qu'elle a maintenant été restaurée. Ceci est généralement utilisé uniquement lors de l'ingestion en masse pour améliorer les performances du système. Après l'activité en masse, l'audit est restauré et la possibilité de désactiver l'audit est alors définitivement bloquée.

SCMT : validation du magasin d'objets

Le contenu de la grille n'est pas rendu disponible ou reconnu comme stocké tant qu'il n'a pas été validé (ce qui signifie qu'il a été stocké de manière persistante). Le contenu stocké de manière persistante a été entièrement écrit sur le disque et a réussi les contrôles d'intégrité associés. Ce message est émis lorsqu'un bloc de contenu est validé dans le stockage.

Code	Champ	Description
CBID	Identifiant du bloc de contenu	L'identifiant unique du bloc de contenu dédié au stockage permanent.
RSLT	Code de résultat	État au moment où l'objet a été stocké sur le disque : SUCS : Objet stocké avec succès.

Ce message signifie qu'un bloc de contenu donné a été entièrement stocké et vérifié et peut désormais être demandé. Il peut être utilisé pour suivre le flux de données au sein du système.

SDEL : SUPPRESSION S3

Lorsqu'un client S3 émet une transaction DELETE, une demande est effectuée pour supprimer l'objet ou le bucket spécifié, ou pour supprimer une sous-ressource bucket/objet. Ce message est émis par le serveur si la transaction réussit.

Code	Champ	Description
CBID	Identifiant du bloc de contenu	L'identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les buckets n'incluent pas ce champ.
CNCH	En-tête de contrôle de cohérence	La valeur de l'en-tête de requête HTTP Consistency-Control, si présent dans la requête.
CNID	Identifiant de connexion	L'identifiant système unique pour la connexion TCP/IP.

Code	Champ	Description
CSIZ	Taille du contenu	La taille de l'objet supprimé en octets. Les opérations sur les buckets n'incluent pas ce champ.
DMRK	Supprimer l'ID de version du marqueur	L'ID de version du marqueur de suppression créé lors de la suppression d'un objet d'un bucket versionné. Les opérations sur les buckets n'incluent pas ce champ.
GFID	ID de connexion à la fédération de grille	L'ID de connexion de la connexion de fédération de grille associée à une demande de suppression de réplication inter-grille. Uniquement inclus dans les journaux d'audit sur la grille de destination.
GFSA	ID du compte source de la Grid Federation	L'ID de compte du locataire sur la grille source pour une demande de suppression de réplication inter-grille. Uniquement inclus dans les journaux d'audit sur la grille de destination.
HTRH	En-tête de requête HTTP	Liste des noms et valeurs d'en-tête de requête HTTP enregistrés tels que sélectionnés lors de la configuration. `X-Forwarded-For`est automatiquement inclus s'il est présent dans la demande et si le `X-Forwarded-For` la valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP). `x-amz-bypass-governance-retention`est automatiquement inclus s'il est présent dans la demande.
MTME	Heure de la dernière modification	L'horodatage Unix, en microsecondes, indiquant quand l'objet a été modifié pour la dernière fois.
RSLT	Code de résultat	Résultat de la transaction DELETE. Le résultat est toujours : SUCS : Réussi
S3AI	ID de compte locataire S3 (expéditeur de la demande)	L'ID du compte 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)	L'ID de clé d'accès S3 haché pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Godet S3	Le nom du bucket S3.

Code	Champ	Description
S3KY	Touche S3	Le nom de la clé S3, sans inclure le nom du bucket. Les opérations sur les buckets n'incluent pas ce champ.
S3SR	Sous-ressource S3	Le compartiment ou la sous-ressource d'objet sur lequel l'opération est effectuée, le cas échéant.
SACC	Nom du compte locataire S3 (expéditeur de la demande)	Le nom du compte locataire de l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SAIP	Adresse IP (expéditeur de la requête)	L'adresse IP de l'application cliente qui a effectué la demande.
SBAC	Nom du compte locataire S3 (propriétaire du bucket)	Le nom du compte locataire pour le propriétaire du bucket. Utilisé pour identifier l'accès inter-comptes ou anonyme.
SBAI	ID de compte locataire S3 (propriétaire du bucket)	L'ID de compte locataire du propriétaire du bucket cible. Utilisé pour identifier l'accès inter-comptes ou anonyme.
SGRP	Site (Groupe)	Si présent, l'objet a été supprimé sur le site spécifié, qui n'est pas le site où l'objet a été ingéré.
SUSR	URN utilisateur S3 (expéditeur de la requête)	L'ID du compte locataire et le nom d'utilisateur de l'utilisateur effectuant la demande. L'utilisateur peut être un utilisateur local ou un utilisateur LDAP. Par exemple : `urn:sgws:identity::03393893651506583485:root` Vide pour les demandes anonymes.
TEMPS	Durée	Temps total de traitement de la demande en microsecondes.
TLIP	Adresse IP de l'équilibreur de charge approuvé	Si la demande a été acheminée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
UUDM	Identifiant unique universel pour un marqueur de suppression	L'identifiant d'un marqueur de suppression. Les messages du journal d'audit spécifient UUDM ou UUID, où UUDM indique un marqueur de suppression créé à la suite d'une demande de suppression d'objet et UUID indique un objet.

Code	Champ	Description
UUID	Identifiant unique universel	L'identifiant de l'objet dans le système StorageGRID .
VSID	ID de version	L'ID de version de la version spécifique d'un objet qui a été supprimé. Les opérations sur les buckets et les objets dans les buckets non versionnés n'incluent pas ce champ.

SGET : S3 OBTENIR

Lorsqu'un client S3 émet une transaction GET, une demande est effectuée pour récupérer un objet ou répertorier les objets dans un bucket, ou pour supprimer une sous-ressource bucket/objet. Ce message est émis par le serveur si la transaction réussit.

Code	Champ	Description
CBID	Identifiant du bloc de contenu	L'identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les buckets n'incluent pas ce champ.
CNCH	En-tête de contrôle de cohérence	La valeur de l'en-tête de requête HTTP Consistency-Control, si présent dans la requête.
CNID	Identifiant de connexion	L'identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	La taille de l'objet récupéré en octets. Les opérations sur les buckets n'incluent pas ce champ.
HTRH	En-tête de requête HTTP	Liste des noms et valeurs d'en-tête de requête HTTP enregistrés tels que sélectionnés lors de la configuration. `X-Forwarded-For`est automatiquement inclus s'il est présent dans la demande et si le `X-Forwarded-For` la valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP).
LITÉ	ListObjectsV2	Une réponse au format *v2* a été demandée. Pour plus de détails, voir "AWS ListObjectsV2" . Pour les opérations de bucket GET uniquement.
NCHD	Nombre d'enfants	Inclut les clés et les préfixes courants. Pour les opérations de bucket GET uniquement.

Code	Champ	Description
RANG	Lecture de la portée	Pour les opérations de lecture de plage uniquement. Indique la plage d'octets lus par cette requête. 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 : SUCS : Réussi
S3AI	ID de compte locataire S3 (expéditeur de la demande)	L'ID du compte 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)	L'ID de clé d'accès S3 haché pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Godet S3	Le nom du bucket S3.
S3KY	Touche S3	Le nom de la clé S3, sans inclure le nom du bucket. Les opérations sur les buckets n'incluent pas ce champ.
S3SR	Sous-ressource S3	Le compartiment ou la sous-ressource d'objet sur lequel l'opération est effectuée, le cas échéant.
SACC	Nom du compte locataire S3 (expéditeur de la demande)	Le nom du compte locataire de l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SAIP	Adresse IP (expéditeur de la requête)	L'adresse IP de l'application cliente qui a effectué la demande.
SBAC	Nom du compte locataire S3 (propriétaire du bucket)	Le nom du compte locataire pour le propriétaire du bucket. Utilisé pour identifier l'accès inter-comptes ou anonyme.
SBAI	ID de compte locataire S3 (propriétaire du bucket)	L'ID de compte locataire du propriétaire du bucket cible. Utilisé pour identifier l'accès inter-comptes ou anonyme.

Code	Champ	Description
SUSR	URN utilisateur S3 (expéditeur de la requête)	L'ID du compte locataire et le nom d'utilisateur de l'utilisateur effectuant la demande. L'utilisateur peut être un utilisateur local ou un utilisateur LDAP. Par exemple : `urn:sgws:identity::03393893651506583485:root` Vide pour les demandes anonymes.
TEMPS	Durée	Temps total de traitement de la demande en microsecondes.
TLIP	Adresse IP de l'équilibreur de charge approuvé	Si la demande a été acheminée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
RTCN	Tronqué ou non tronqué	Définissez sur faux si tous les résultats ont été renvoyés. Définissez sur vrai si davantage de résultats sont disponibles à renvoyer. Pour les opérations de bucket GET uniquement.
UUID	Identifiant unique universel	L'identifiant de l'objet dans le système StorageGRID .
VSID	ID de version	L'ID de version de la version spécifique d'un objet qui a été demandé. Les opérations sur les buckets et les objets dans les buckets non versionnés n'incluent pas ce champ.

SHEA : TÊTE S3

Lorsqu'un client S3 émet une transaction HEAD, une demande est effectuée pour vérifier l'existence d'un objet ou d'un bucket et récupérer les métadonnées relatives à un objet. Ce message est émis par le serveur si la transaction réussit.

Code	Champ	Description
CBID	Identifiant du bloc de contenu	L'identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les buckets n'incluent pas ce champ.
CNID	Identifiant de connexion	L'identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	La taille de l'objet vérifié en octets. Les opérations sur les buckets 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 enregistrés tels que sélectionnés lors de la configuration. `X-Forwarded-For`est automatiquement inclus s'il est présent dans la demande et si le `X-Forwarded-For` la valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP).
RSLT	Code de résultat	Résultat de la transaction GET. Le résultat est toujours : SUCS : Réussi
S3AI	ID de compte locataire S3 (expéditeur de la demande)	L'ID du compte 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)	L'ID de clé d'accès S3 haché pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Godet S3	Le nom du bucket S3.
S3KY	Touche S3	Le nom de la clé S3, sans inclure le nom du bucket. Les opérations sur les buckets n'incluent pas ce champ.
SACC	Nom du compte locataire S3 (expéditeur de la demande)	Le nom du compte locataire de l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SAIP	Adresse IP (expéditeur de la requête)	L'adresse IP de l'application cliente qui a effectué la demande.
SBAC	Nom du compte locataire S3 (propriétaire du bucket)	Le nom du compte locataire pour le propriétaire du bucket. Utilisé pour identifier l'accès inter-comptes ou anonyme.
SBAI	ID de compte locataire S3 (propriétaire du bucket)	L'ID de compte locataire du propriétaire du bucket cible. Utilisé pour identifier l'accès inter-comptes ou anonyme.

Code	Champ	Description
SUSR	URN utilisateur S3 (expéditeur de la requête)	L'ID du compte locataire et le nom d'utilisateur de l'utilisateur effectuant la demande. L'utilisateur peut être un utilisateur local ou un utilisateur LDAP. Par exemple : `urn:sgws:identity::03393893651506583485:root` Vide pour les demandes anonymes.
TEMPS	Durée	Temps total de traitement de la demande en microsecondes.
TLIP	Adresse IP de l'équilibreur de charge approuvé	Si la demande a été acheminée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
UUID	Identifiant unique universel	L'identifiant de l'objet dans le système StorageGRID .
VSID	ID de version	L'ID de version de la version spécifique d'un objet qui a été demandé. Les opérations sur les buckets et les objets dans les buckets non versionnés n'incluent pas ce champ.

SPOS : POST S3

Lorsqu'un client S3 émet une demande d'objet POST, ce message est émis par le serveur si la transaction réussit.

Code	Champ	Description
CBID	Identifiant du bloc de contenu	L'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	La valeur de l'en-tête de requête HTTP Consistency-Control, si présent dans la requête.
CNID	Identifiant de connexion	L'identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	La taille de l'objet récupéré en octets.

Code	Champ	Description
HTRH	En-tête de requête HTTP	Liste des noms et valeurs d'en-tête de requête HTTP enregistrés tels que sélectionnés lors de la configuration. `X-Forwarded-For`est automatiquement inclus s'il est présent dans la demande et si le `X-Forwarded-For` la valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP). (Non prévu pour SPOS).
RSLT	Code de résultat	Résultat de la requête RestoreObject. Le résultat est toujours : SUCS : Réussi
S3AI	ID de compte locataire S3 (expéditeur de la demande)	L'ID du compte 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)	L'ID de clé d'accès S3 haché pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Godet S3	Le nom du bucket S3.
S3KY	Touche S3	Le nom de la clé S3, sans inclure le nom du bucket. Les opérations sur les buckets n'incluent pas ce champ.
S3SR	Sous-ressource S3	Le compartiment ou la sous-ressource d'objet sur lequel l'opération est effectuée, le cas échéant. Réglez sur « sélectionner » pour une opération de sélection S3.
SACC	Nom du compte locataire S3 (expéditeur de la demande)	Le nom du compte locataire de l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SAIP	Adresse IP (expéditeur de la requête)	L'adresse IP de l'application cliente qui a effectué la demande.

Code	Champ	Description
SBAC	Nom du compte locataire S3 (propriétaire du bucket)	Le nom du compte locataire pour le propriétaire du bucket. Utilisé pour identifier l'accès inter-comptes ou anonyme.
SBAI	ID de compte locataire S3 (propriétaire du bucket)	L'ID de compte locataire du propriétaire du bucket cible. Utilisé pour identifier l'accès inter-comptes ou anonyme.
SRCF	Configuration des sous-ressources	Restaurer les informations.
SUSR	URN utilisateur S3 (expéditeur de la requête)	L'ID du compte locataire et le nom d'utilisateur de l'utilisateur effectuant la demande. L'utilisateur peut être un utilisateur local ou un utilisateur LDAP. Par exemple : `urn:sgws:identity::03393893651506583485:root` Vide pour les demandes anonymes.
TEMPS	Durée	Temps total de traitement de la demande en microsecondes.
TLIP	Adresse IP de l'équilibreur de charge approuvé	Si la demande a été acheminée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
UUID	Identifiant unique universel	L'identifiant de l'objet dans le système StorageGRID .
VSID	ID de version	L'ID de version de la version spécifique d'un objet qui a été demandé. Les opérations sur les buckets et les objets dans les buckets non versionnés n'incluent pas ce champ.

SPUT : S3 PUT

Lorsqu'un client S3 émet une transaction PUT, une demande est effectuée pour créer un nouvel objet ou un nouveau compartiment, ou pour supprimer une sous-ressource de compartiment/objet. Ce message est émis par le serveur si la transaction réussit.

Code	Champ	Description
CBID	Identifiant du bloc de contenu	L'identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les buckets n'incluent pas ce champ.

Code	Champ	Description
CMPS	Paramètres de conformité	Les paramètres de conformité utilisés lors de la création du bucket, s'ils sont présents dans la demande (tronqués aux 1024 premiers caractères).
CNCH	En-tête de contrôle de cohérence	La valeur de l'en-tête de requête HTTP Consistency-Control, si présent dans la requête.
CNID	Identifiant de connexion	L'identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	La taille de l'objet récupéré en octets. Les opérations sur les buckets n'incluent pas ce champ.
GFID	ID de connexion à la fédération de grille	L'ID de connexion de la connexion de la fédération de grille associée à une demande PUT de réplication inter-grille. Uniquement inclus dans les journaux d'audit sur la grille de destination.
GFSA	ID du compte source de la Grid Federation	L'ID de compte du locataire sur la grille source pour une demande PUT de réplication inter-grille. Uniquement inclus dans les journaux d'audit sur la grille de destination.
HTRH	En-tête de requête HTTP	Liste des noms et valeurs d'en-tête de requête HTTP enregistrés tels que sélectionnés lors de la configuration. `X-Forwarded-For`est automatiquement inclus s'il est présent dans la demande et si le `X-Forwarded-For` la valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP). `x-amz-bypass-governance-retention`est automatiquement inclus s'il est présent dans la demande.
LKEN	Verrouillage d'objet activé	Valeur de l'en-tête de la requête `x-amz-bucket-object-lock-enabled` , si présent dans la demande.
LKLH	Verrouillage d'objet Conservation légale	Valeur de l'en-tête de la requête `x-amz-object-lock-legal-hold` , s'il est présent dans la requête PutObject.

Code	Champ	Description
LKMD	Mode de rétention du verrouillage des objets	Valeur de l'en-tête de la requête `x-amz-object-lock-mode` , s'il est présent dans la requête PutObject.
LKRU	Verrouillage d'objet Conserver jusqu'à la date	Valeur de l'en-tête de la requête `x-amz-object-lock-retain-until-date` , s'il est présent dans la requête PutObject. Les valeurs sont limitées à 100 ans à compter de la date d'ingestion de l'objet.
MTME	Heure de la dernière modification	L'horodatage Unix, en microsecondes, indiquant quand l'objet a été modifié pour la dernière fois.
RSLT	Code de résultat	Résultat de la transaction PUT. Le résultat est toujours : SUCS : Réussi
S3AI	ID de compte locataire S3 (expéditeur de la demande)	L'ID du compte 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)	L'ID de clé d'accès S3 haché pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Godet S3	Le nom du bucket S3.
S3KY	Touche S3	Le nom de la clé S3, sans inclure le nom du bucket. Les opérations sur les buckets n'incluent pas ce champ.
S3SR	Sous-ressource S3	Le compartiment ou la sous-ressource d'objet sur lequel l'opération est effectuée, le cas échéant.
SACC	Nom du compte locataire S3 (expéditeur de la demande)	Le nom du compte locataire de l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SAIP	Adresse IP (expéditeur de la requête)	L'adresse IP de l'application cliente qui a effectué la demande.

Code	Champ	Description
SBAC	Nom du compte locataire S3 (propriétaire du bucket)	Le nom du compte locataire pour le propriétaire du bucket. Utilisé pour identifier l'accès inter-comptes ou anonyme.
SBAI	ID de compte locataire S3 (propriétaire du bucket)	L'ID de compte locataire du propriétaire du bucket cible. Utilisé pour identifier l'accès inter-comptes ou anonyme.
SRCF	Configuration des sous-ressources	La nouvelle configuration de sous-ressource (tronquée aux 1024 premiers caractères).
SUSR	URN utilisateur S3 (expéditeur de la requête)	L'ID du compte locataire et le nom d'utilisateur de l'utilisateur effectuant la demande. L'utilisateur peut être un utilisateur local ou un utilisateur LDAP. Par exemple : `urn:sgws:identity::03393893651506583485:root` Vide pour les demandes anonymes.
TEMPS	Durée	Temps total de traitement de la demande en microsecondes.
TLIP	Adresse IP de l'équilibreur de charge approuvé	Si la demande a été acheminée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
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	L'identifiant de l'objet dans le système StorageGRID .
VSID	ID de version	L'ID de version d'un nouvel objet créé dans un bucket versionné. Les opérations sur les buckets et les objets dans les buckets non versionnés n'incluent pas ce champ.
VSST	État de versionnage	Le nouvel état de version d'un bucket. 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 les API standard.

Code	Champ	Description
CBID	Identifiant du bloc de contenu	L'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 au sein du système.

SUPD : Métadonnées S3 mises à jour

Ce message est généré par l'API S3 lorsqu'un client S3 met à jour les métadonnées d'un objet ingéré. Le message est émis par le serveur si la mise à jour des métadonnées est réussie.

Code	Champ	Description
CBID	Identifiant du bloc de contenu	L'identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les buckets n'incluent pas ce champ.
CNCH	En-tête de contrôle de cohérence	La valeur de l'en-tête de requête HTTP Consistency-Control, si présent dans la requête, lors de la mise à jour des paramètres de conformité d'un bucket.
CNID	Identifiant de connexion	L'identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	La taille de l'objet récupéré en octets. Les opérations sur les buckets n'incluent pas ce champ.
HTRH	En-tête de requête HTTP	Liste des noms et valeurs d'en-tête de requête HTTP enregistrés tels que sélectionnés lors de la configuration. `X-Forwarded-For`est automatiquement inclus s'il est présent dans la demande et si le `X-Forwarded-For` la valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP).

Code	Champ	Description
RSLT	Code de résultat	Résultat de la transaction GET. Le résultat est toujours : SUCS : réussi
S3AI	ID de compte locataire S3 (expéditeur de la demande)	L'ID du compte 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)	L'ID de clé d'accès S3 haché pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Godet S3	Le nom du bucket S3.
S3KY	Touche S3	Le nom de la clé S3, sans inclure le nom du bucket. Les opérations sur les buckets n'incluent pas ce champ.
SACC	Nom du compte locataire S3 (expéditeur de la demande)	Le nom du compte locataire de l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SAIP	Adresse IP (expéditeur de la requête)	L'adresse IP de l'application cliente qui a effectué la demande.
SBAC	Nom du compte locataire S3 (propriétaire du bucket)	Le nom du compte locataire pour le propriétaire du bucket. Utilisé pour identifier l'accès inter-comptes ou anonyme.
SBAI	ID de compte locataire S3 (propriétaire du bucket)	L'ID de compte locataire du propriétaire du bucket cible. Utilisé pour identifier l'accès inter-comptes ou anonyme.
SUSR	URN utilisateur S3 (expéditeur de la requête)	L'ID du compte locataire et le nom d'utilisateur de l'utilisateur effectuant la demande. L'utilisateur peut être un utilisateur local ou un utilisateur LDAP. Par exemple : `urn:sgws:identity::03393893651506583485:root` Vide pour les demandes anonymes.
TEMPS	Durée	Temps total de traitement de la demande en microsecondes.

Code	Champ	Description
TLIP	Adresse IP de l'équilibreur de charge approuvé	Si la demande a été acheminée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
UUID	Identifiant unique universel	L'identifiant de l'objet dans le système StorageGRID .
VSID	ID de version	L'ID de version de la version spécifique d'un objet dont les métadonnées ont été mises à jour. Les opérations sur les buckets et les objets dans les buckets 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 des données d'objet répliquées sont lues ou écrites sur le disque, plusieurs contrôles de vérification et d'intégrité sont effectués pour garantir que les données envoyées à l'utilisateur demandeur sont identiques aux données initialement ingérées dans le système. Si l'une de ces vérifications échoue, le système met automatiquement en quarantaine les données de l'objet répliqué corrompu pour empêcher leur récupération ultérieure.

Code	Champ	Description
CBID	Identifiant du bloc de contenu	L'identifiant unique du bloc de contenu dont la vérification a échoué.
RSLT	Code de résultat	Type d'échec de vérification : CRCF : échec du contrôle de redondance cyclique (CRC). HMAC : la vérification du code d'authentification de message basé sur le hachage (HMAC) a échoué. EHSH : hachage de contenu chiffré inattendu. PHSH : hachage de contenu original inattendu. SEQC : séquence de données incorrecte sur le disque. PERR : structure non valide du fichier disque. DERR : Erreur de disque. FNAM : Mauvais nom de fichier.

Ce message doit être surveillé de près. Les échecs de vérification du contenu peuvent indiquer des pannes matérielles imminentes.

Pour déterminer quelle opération a déclenché le message, consultez la valeur du champ AMID (ID du module). Par exemple, une valeur SVFY indique que le message a été généré par le module Storage Verifier, c'est-à-dire une vérification en arrière-plan, et STOR indique que le message a été déclenché par une récupération de contenu.

SVRU : Vérification du magasin d'objets inconnu

Le composant Stockage du service LDR analyse en continu toutes les copies des données d'objet répliquées dans le magasin d'objets. Ce message est émis lorsqu'une copie inconnue ou inattendue des données d'objet répliquées est détectée dans le magasin d'objets et déplacée vers le répertoire de quarantaine.

Code	Champ	Description
FPTH	Chemin du fichier	Le chemin du fichier de la copie d'objet inattendue.
RSLT	Résultat	Ce champ a la valeur « AUCUN ». RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message. « NONE » est utilisé plutôt que « SUCS » afin que ce message ne soit pas filtré.

Le message d'audit SVRU : Object Store Verify Unknown doit être surveillé de près. Cela signifie que des copies inattendues de données d'objet ont été détectées dans le magasin d'objets. Cette situation doit être étudiée immédiatement pour déterminer comment ces copies ont été créées, car elle peut indiquer des pannes matérielles imminentes.

SYSD : arrêt du nœud

Lorsqu'un service est arrêté correctement, ce message est généré pour indiquer que l'arrêt a été demandé. En général, 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	Arrêt propre	La nature de l'arrêt : SUCS : Le système a été arrêté proprement.

Le message n'indique pas si le serveur hôte est arrêté, uniquement le service de reporting. Le RSLT d'un SYSD ne peut pas indiquer un arrêt « sale », car le message est généré uniquement par des arrêts « propres ».

SYST : arrêt du nœud

Lorsqu'un service est arrêté correctement, 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	Arrêt propre	La nature de l'arrêt : SUCS : Le système a été arrêté proprement.

Le message n'indique pas si le serveur hôte est arrêté, uniquement le service de reporting. Le code RSLT d'un message SYST ne peut pas indiquer un arrêt « sale », car le message est généré uniquement par des arrêts « propres ».

SYSU : démarrage du nœud

Lorsqu'un service est redémarré, ce message est généré pour indiquer si l'arrêt précédent était propre (commandé) ou désordonné (inattendu).

Code	Champ	Description
RSLT	Arrêt propre	La nature de l'arrêt : SUCS : Le système a été arrêté proprement. DSDN : le système n'a pas été arrêté correctement. 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, uniquement le service de reporting. Ce message peut être utilisé pour :

- Détecter la discontinuité dans la piste d'audit.
- Déterminez si un service échoue pendant son fonctionnement (car la nature distribuée du système StorageGRID peut masquer ces échecs). Le Gestionnaire de serveur redémarre automatiquement un service défaillant.

WDEL : SUPPRESSION rapide

Lorsqu'un client Swift émet une transaction DELETE, une demande est effectuée pour supprimer l'objet ou le conteneur spécifié. Ce message est émis par le serveur si la transaction réussit.

Code	Champ	Description
CBID	Identifiant du bloc de contenu	L'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	La 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 enregistrés tels que sélectionnés lors de la configuration. `X-Forwarded-For`est automatiquement inclus s'il est présent dans la demande et si le `X-Forwarded-For` la valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP).
MTME	Heure de la dernière modification	L'horodatage Unix, en microsecondes, indiquant quand l'objet a été modifié pour la dernière fois.
RSLT	Code de résultat	Résultat de la transaction DELETE. Le résultat est toujours : SUCS : Réussi
SAIP	Adresse IP du client demandeur	L'adresse IP de l'application cliente qui a effectué la demande.
SGRP	Site (Groupe)	Si présent, l'objet a été supprimé sur le site spécifié, qui n'est pas le site où l'objet a été ingéré.
TEMPS	Durée	Temps total de traitement de la demande en microsecondes.
TLIP	Adresse IP de l'équilibreur de charge approuvé	Si la demande a été acheminée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
UUID	Identifiant unique universel	L'identifiant de l'objet dans le système StorageGRID .
CMPC	ID de compte Swift	L'ID de compte unique tel que spécifié par le système StorageGRID .
WCON	Conteneur Swift	Le nom du conteneur Swift.
WOBJ	Objet Swift	L'identifiant de l'objet Swift. Les opérations sur les conteneurs n'incluent pas ce champ.
WUSR	Utilisateur du compte Swift	Le 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 effectuée 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 réussit.

Code	Champ	Description
CBID	Identifiant du bloc de contenu	L'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	La 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 enregistrés tels que sélectionnés lors de la configuration. `` `X-Forwarded-For`est automatiquement inclus s'il est présent dans la demande et si le `X-Forwarded-For` la valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP). ``
RSLT	Code de résultat	Résultat de la transaction GET. Le résultat est toujours SUCS : réussi
SAIP	Adresse IP du client demandeur	L'adresse IP de l'application cliente qui a effectué la demande.
TEMPS	Durée	Temps total de traitement de la demande en microsecondes.
TLIP	Adresse IP de l'équilibreur de charge approuvé	Si la demande a été acheminée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
UUID	Identifiant unique universel	L'identifiant de l'objet dans le système StorageGRID .
CMPC	ID de compte Swift	L'ID de compte unique tel que spécifié par le système StorageGRID .
WCON	Conteneur Swift	Le nom du conteneur Swift. Les opérations sur les comptes n'incluent pas ce champ.

Code	Champ	Description
WOBJ	Objet Swift	L'identifiant de l'objet Swift. Les opérations sur les comptes et les conteneurs n'incluent pas ce champ.
WUSR	Utilisateur du compte Swift	Le nom d'utilisateur du compte Swift qui identifie de manière unique le client effectuant la transaction.

WHEA : TÊTE RAPIDE

Lorsqu'un client Swift émet une transaction HEAD, une demande est effectuée pour vérifier l'existence d'un compte, d'un conteneur ou d'un objet et récupérer toutes les métadonnées pertinentes. Ce message est émis par le serveur si la transaction réussit.

Code	Champ	Description
CBID	Identifiant du bloc de contenu	L'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	La 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 enregistrés tels que sélectionnés lors de la configuration. `` `X-Forwarded-For`est automatiquement inclus s'il est présent dans la demande et si le `X-Forwarded-For` la valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP). ``
RSLT	Code de résultat	Résultat de la transaction HEAD. Le résultat est toujours : SUCS : réussi
SAIP	Adresse IP du client demandeur	L'adresse IP de l'application cliente qui a effectué la demande.
TEMPS	Durée	Temps total de traitement de la demande en microsecondes.
TLIP	Adresse IP de l'équilibreur de charge approuvé	Si la demande a été acheminée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.

Code	Champ	Description
UUID	Identifiant unique universel	L'identifiant de l'objet dans le système StorageGRID .
CMPC	ID de compte Swift	L'ID de compte unique tel que spécifié par le système StorageGRID .
WCON	Conteneur Swift	Le nom du conteneur Swift. Les opérations sur les comptes n'incluent pas ce champ.
WOBJ	Objet Swift	L'identifiant de l'objet Swift. Les opérations sur les comptes et les conteneurs n'incluent pas ce champ.
WUSR	Utilisateur du compte Swift	Le nom d'utilisateur du compte Swift qui identifie de manière unique le client effectuant la transaction.

WPUT : Swift PUT

Lorsqu'un client Swift émet une transaction PUT, une demande est effectuée pour créer un nouvel objet ou conteneur. Ce message est émis par le serveur si la transaction réussit.

Code	Champ	Description
CBID	Identifiant du bloc de contenu	L'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	La 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 enregistrés tels que sélectionnés lors de la configuration. `X-Forwarded-For`est automatiquement inclus s'il est présent dans la demande et si le `X-Forwarded-For` la valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP).
MTME	Heure de la dernière modification	L'horodatage Unix, en microsecondes, indiquant quand l'objet a été modifié pour la dernière fois.

Code	Champ	Description
RSLT	Code de résultat	Résultat de la transaction PUT. Le résultat est toujours : SUCS : réussi
SAIP	Adresse IP du client demandeur	L'adresse IP de l'application cliente qui a effectué la demande.
TEMPS	Durée	Temps total de traitement de la demande en microsecondes.
TLIP	Adresse IP de l'équilibreur de charge approuvé	Si la demande a été acheminée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
UUID	Identifiant unique universel	L'identifiant de l'objet dans le système StorageGRID .
CMPC	ID de compte Swift	L'ID de compte unique tel que spécifié par le système StorageGRID .
WCON	Conteneur Swift	Le nom du conteneur Swift.
WOBJ	Objet Swift	L'identifiant de l'objet Swift. Les opérations sur les conteneurs n'incluent pas ce champ.
WUSR	Utilisateur du compte Swift	Le nom d'utilisateur du compte Swift qui identifie de manière unique le client effectuant la transaction.

Informations sur le copyright

Informations sur les marques commerciales