Surveiller et résoudre les problèmes

StorageGRID

NetApp
October 03, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/storagegrid-115/monitor/web-browser-requirements.html on October 03, 2025. Always check docs.netapp.com for the latest.

Sommaire

Surveiller et résoudre les problèmes . . . 1
- Surveiller un système StorageGRID . . . 1
  - Utilisation de Grid Manager pour la surveillance . . . 1
  - Informations à surveiller régulièrement . . . 41
  - Gestion des alertes et des alarmes . . . 83
  - Utilisation de la surveillance SNMP . . . 133
  - Collecte de données StorageGRID supplémentaires . . . 148
  - Référence des alertes . . . 185
  - Référence des alarmes (système hérité) . . . 230
  - Référence des fichiers journaux . . . 287
- Dépanner un système StorageGRID . . . 306
  - Présentation de la détection des problèmes . . . 306
  - Résolution des problèmes d'objet et de stockage . . . 315
  - Résolution des problèmes de métadonnées . . . 347
  - Dépannage des erreurs de certificat . . . 354
  - Résolution des problèmes liés au nœud d'administration et à l'interface utilisateur . . . 356
  - Résolution des problèmes de réseau, de matériel et de plate-forme . . . 361
- Examiner les journaux d'audit . . . 369
  - Présentation du message d'audit . . . 370
  - Formats du fichier journal d'audit et des messages . . . 376
  - Messages d'audit et cycle de vie de l'objet . . . 395
  - Messages d'audit . . . 402

Surveiller et résoudre les problèmes

Surveiller un système StorageGRID

Découvrez comment contrôler un système StorageGRID et évaluer les problèmes potentiels. Répertorie toutes les alertes système.

- "Utilisation de Grid Manager pour la surveillance"
- "Informations à surveiller régulièrement"
- "Gestion des alertes et des alarmes"
- "Utilisation de la surveillance SNMP"
- "Collecte de données StorageGRID supplémentaires"
- "Dépannage d'un système StorageGRID"
- "Référence des alertes"
- "Référence des alarmes (système hérité)"
- "Référence des fichiers journaux"

Utilisation de Grid Manager pour la surveillance

Le gestionnaire de grille est l'outil le plus important pour la surveillance de votre système StorageGRID. Cette section présente le tableau de bord de Grid Manager et fournit des informations détaillées sur les pages nœuds.

- "Navigateurs Web pris en charge"
- "Affichage du tableau de bord"
- "Affichage de la page nœuds"

Navigateurs Web pris en charge

Vous devez utiliser un navigateur Web pris en charge.

Navigateur Web	Version minimale prise en charge
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

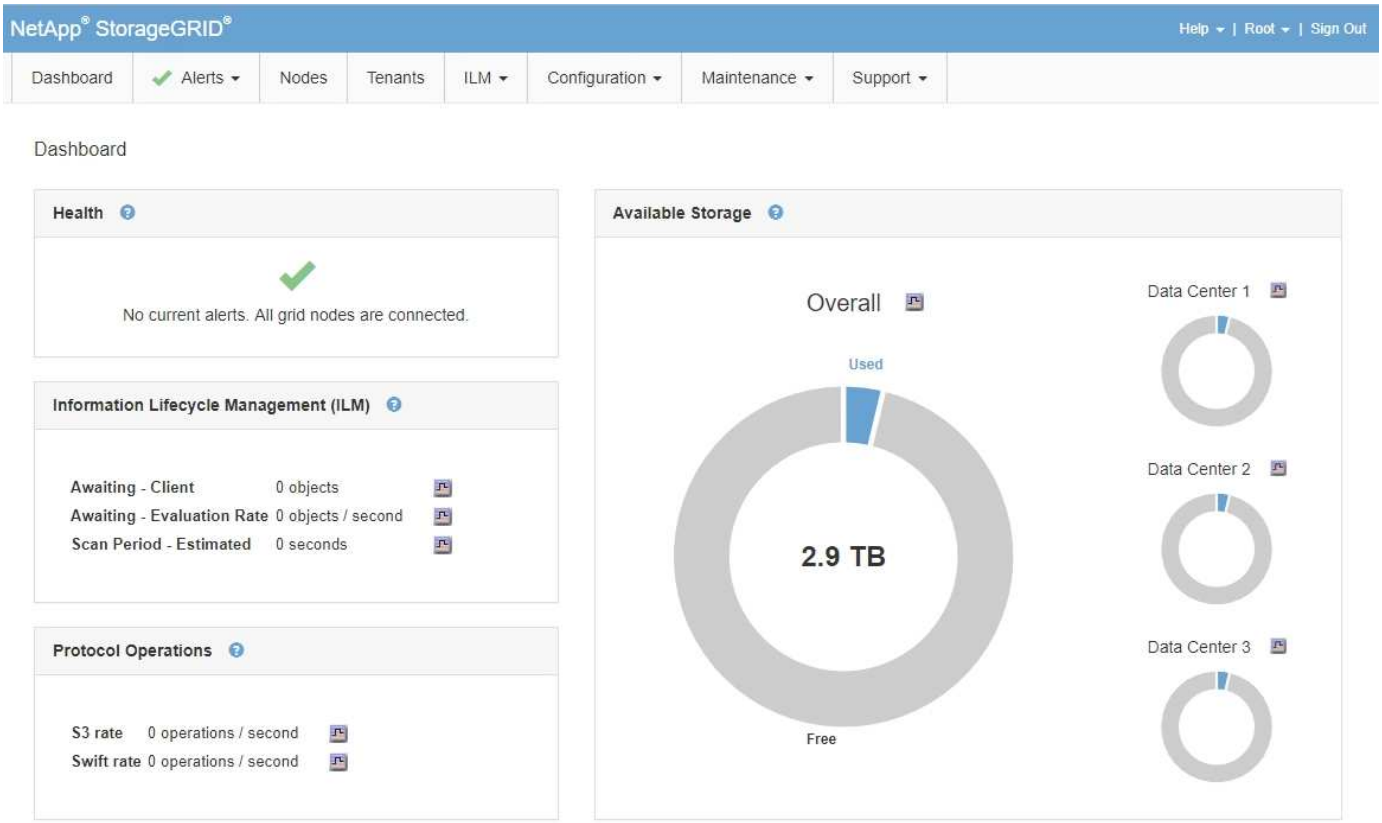
Vous devez régler la fenêtre du navigateur sur une largeur recommandée.

Largeur du navigateur	Pixels
Minimum	1024

Largeur du navigateur	Pixels
Optimale	1280

Affichage du tableau de bord

Lorsque vous vous connectez à Grid Manager pour la première fois, vous pouvez utiliser le tableau de bord pour surveiller en un coup d'œil les activités du système. Le tableau de bord inclut des informations sur l'état du système, les mesures d'utilisation, les tendances et les graphiques opérationnels.



Panneau Santé

Description	Afficher les détails supplémentaires	En savoir plus >>
Récapitule l'état de santé du système. Une coche verte indique qu'il n'y a pas d'alerte en cours et que tous les nœuds de la grille sont connectés. Toute autre icône indique qu'au moins un nœud est en cours d'alerte ou déconnecté.	Un ou plusieurs des liens suivants peuvent s'afficher : • **Détails de la grille** : apparaît si des nœuds sont déconnectés (état de connexion inconnu ou administratif). Cliquez sur le lien ou cliquez sur l'icône bleue ou grise pour déterminer le ou les nœuds concernés. • **Alertes actuelles** : s'affiche si des alertes sont actuellement actives. Cliquez sur le lien ou cliquez sur **critique**, **majeur** ou **mineur** pour voir les détails sur la page **alertes** > **courant**. • **Alertes récemment résolues**: Apparaît si les alertes déclenchées la semaine dernière sont maintenant résolues. Cliquez sur le lien pour voir les détails sur la page **alertes** > **résolu**. • **Alarmes héritées** : s'affiche si des alarmes (système hérité) sont actuellement actives. Cliquez sur le lien pour afficher les détails sur la page **support** > **alarmes (hérité)** > **alarmes actuelles**. • **Licence** : s'affiche en cas de problème avec la licence logicielle de ce système StorageGRID. Cliquez sur le lien pour afficher les détails sur la page **Maintenance** > **système** > **Licence**.	• "Contrôle de l'état de connexion du nœud" • "Affichage des alertes en cours" • "Affichage des alertes résolues" • "Affichage des anciennes alarmes" • "Administrer StorageGRID"

Panneau stockage disponible

Description	Afficher les détails supplémentaires	En savoir plus >>
Affiche la capacité de stockage disponible et utilisée dans toute la grille, sans compter les supports d'archivage. Le graphique global présente les totaux à l'échelle de la grille. S'il s'agit d'une grille multisite, des graphiques supplémentaires apparaissent pour chaque site de centre de données. Vous pouvez utiliser ces informations pour comparer le stockage utilisé avec le stockage disponible. Si vous disposez d'une grille multisite, vous pouvez déterminer quel site consomme plus de stockage.	• Pour afficher la capacité, placez le curseur sur les sections capacité disponible et capacité utilisée du graphique. • Pour afficher les tendances de capacité sur une plage de dates, cliquez sur l'icône du graphique pour la grille globale ou pour un site de data center. • Pour afficher les détails, sélectionnez **nœuds**. Ensuite, affichez l'onglet stockage de la grille entière, d'un site entier ou d'un nœud de stockage unique.	• "Affichage de l'onglet stockage" • "Contrôle de la capacité de stockage"

Panneau gestion du cycle de vie des informations (ILM)

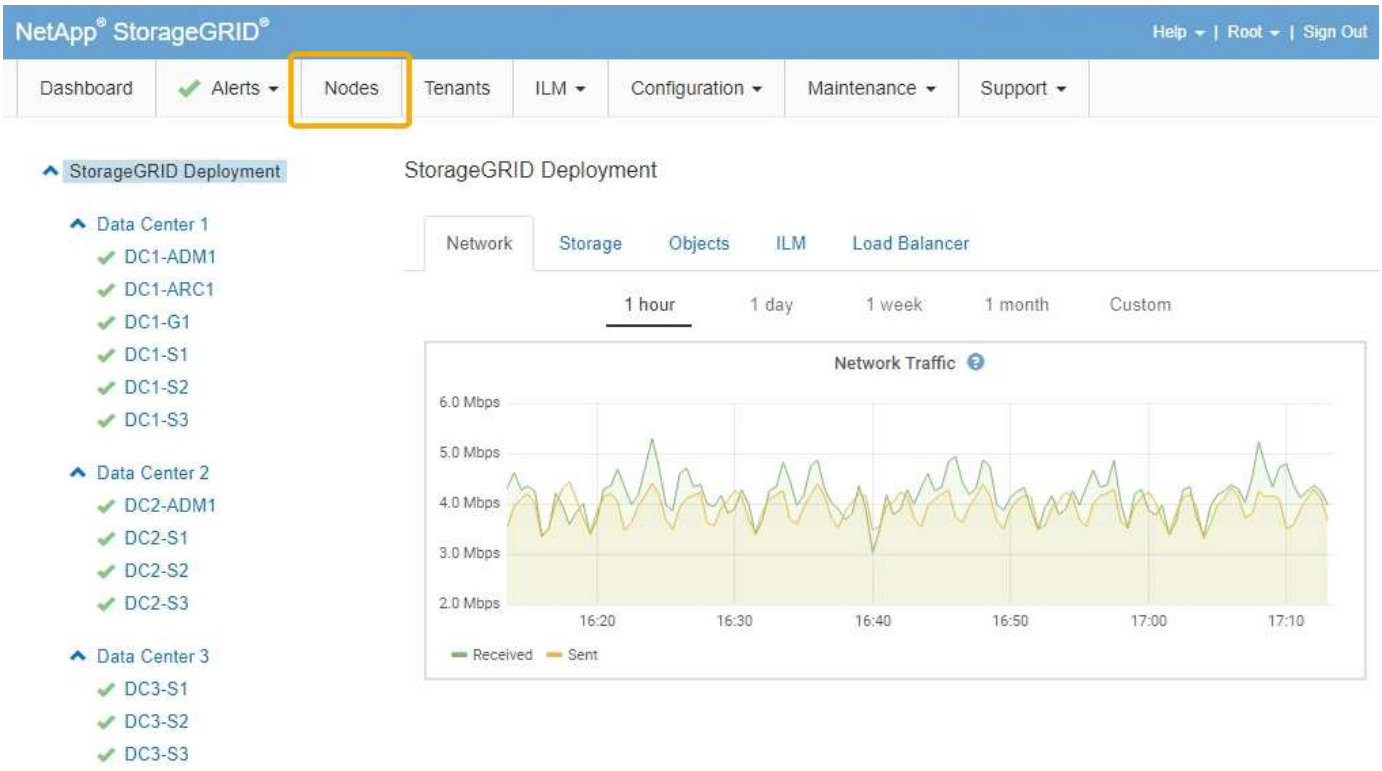
Description	Afficher les détails supplémentaires	En savoir plus >>
Affiche les opérations ILM actuelles et les files d'attente ILM de votre système. Vous pouvez utiliser ces informations pour surveiller la charge de travail de votre système. • **Attente - client** : nombre total d'objets en attente d'évaluation ILM à partir des opérations client (par exemple, ingestion). • **Attente - taux d'évaluation** : taux actuel auquel les objets sont évalués par rapport à la politique ILM de la grille. • **Période d'acquisition - estimé** : temps estimé pour effectuer une analyse ILM complète de tous les objets. **Note:** Une analyse complète ne garantit pas que ILM a été appliquée à tous les objets.	• Pour afficher les détails, sélectionnez **nœuds**. Affichez ensuite l'onglet ILM de la grille complète, un site entier ou un nœud de stockage unique. • Pour afficher les règles ILM existantes, sélectionnez **ILM** > **règles**. • Pour afficher les règles ILM existantes, sélectionnez **ILM** > **Policies**.	• "Affichage de l'onglet ILM" • "Administrer StorageGRID".

Panneau Protocol Operations

Description	Afficher les détails supplémentaires	En savoir plus >>
Affiche le nombre d'opérations spécifiques au protocole (S3 et Swift) effectuées par votre système. Vous pouvez utiliser ces informations pour surveiller les charges de travail et l'efficacité de votre système. La moyenne des débits de protocole est calculée au cours des deux dernières minutes.	• Pour afficher les détails, sélectionnez **nœuds**. Ensuite, affichez l'onglet objets de la grille entière, d'un site entier ou d'un nœud de stockage unique. • Pour afficher les tendances sur une plage de dates, cliquez sur l'icône graphique À droite du débit du protocole S3 ou Swift.	• "Affichage de l'onglet objets" • "Utilisation de S3" • "Utiliser Swift"

Affichage de 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 mesures de la grille dans sa totalité, sur chaque site de la grille et sur chaque nœud d'un site.



Dans la vue arborescente à gauche, vous pouvez voir tous les sites et tous les nœuds de votre système StorageGRID. L'icône de chaque nœud indique si le nœud est connecté ou s'il existe des alertes actives.

Icônes d'état de connexion

Si un nœud est déconnecté de la grille, l'arborescence affiche une icône d'état de connexion bleue ou grise, et non l'icône des alertes sous-jacentes.

- **Non connecté - Inconnu** : Le nœud n'est pas connecté à la grille pour une raison inconnue. Par exemple, la connexion réseau entre les nœuds a été perdue ou l'alimentation est coupée. L'alerte **Impossible de communiquer avec le noeud** peut également être déclenchée. D'autres alertes peuvent également être actives. Cette situation exige une attention immédiate.

  > Un nœud peut apparaître comme inconnu lors des opérations d'arrêt géré. Dans ces cas, vous pouvez ignorer l'état Inconnu.

- **Non connecté - Arrêt administratif** : Le nœud n'est pas connecté à la grille pour une raison attendue. Par exemple, le nœud ou les services du nœud ont été normalement arrêtés, le nœud est en cours de redémarrage ou le logiciel est mis à niveau. Une ou plusieurs alertes peuvent également être actives.

Icônes d'alerte

Si un nœud est connecté à la grille, l'arborescence affiche l'une des icônes suivantes, selon qu'il existe des alertes actuelles pour le nœud.

- **Critique** : Il existe une condition anormale qui a arrêté les opérations normales d'un nœud ou service StorageGRID. Vous devez immédiatement résoudre le problème sous-jacent. Une interruption du service et une perte de données peuvent se produire si le problème n'est pas résolu.
- **Majeur** : Il existe une condition anormale affectant les opérations en cours ou approchant le seuil d'une alerte critique. Vous devez examiner les alertes majeures et résoudre tous les problèmes sous-jacents pour vérifier que leur condition anormale n'arrête pas le fonctionnement normal d'un nœud ou d'un service StorageGRID.
- **Mineur** : Le système fonctionne normalement, mais il existe une condition anormale qui pourrait affecter la capacité du système à fonctionner s'il continue. Vous devez surveiller et résoudre les alertes mineures qui ne sont pas claires par elles-mêmes pour vous assurer qu'elles n'entraînent pas un problème plus grave.
- **Normal** : Aucune alerte n'est active et le nœud est connecté à la grille.

Affichage des détails d'un système, d'un site ou d'un nœud

Pour afficher les informations disponibles, cliquez sur les liens appropriés à gauche, comme suit :

- Sélectionnez le nom de la grille pour afficher un récapitulatif des agrégats des statistiques de l'ensemble du système StorageGRID. (La capture d'écran montre un système nommé StorageGRID Deployment.)
- Sélectionnez un site de data Center spécifique pour afficher un résumé global des statistiques pour tous les nœuds de ce site.
- Sélectionnez un nœud spécifique pour afficher des informations détaillées sur ce nœud.

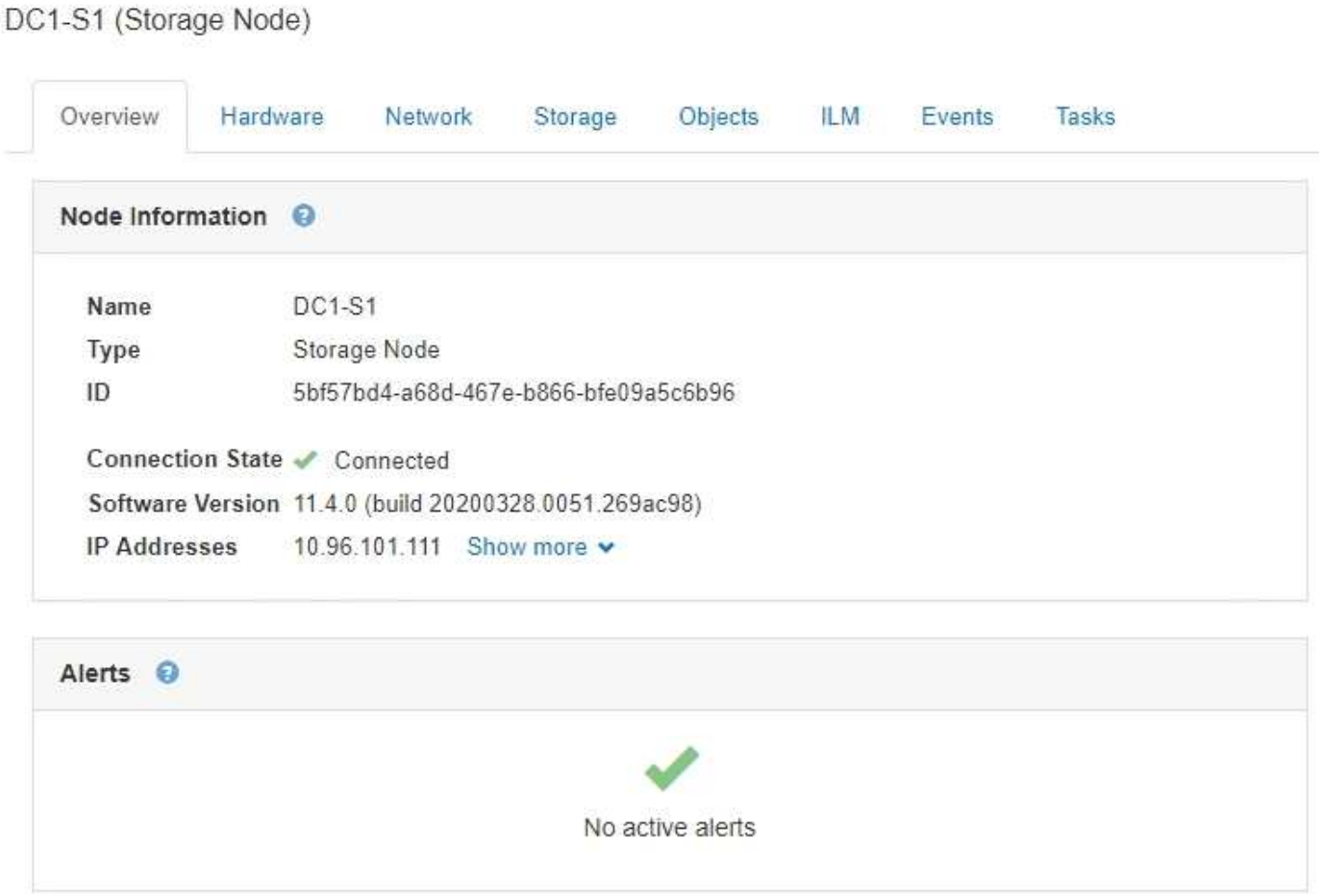
Affichage de l'onglet vue d'ensemble

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

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

Informations sur le nœud

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



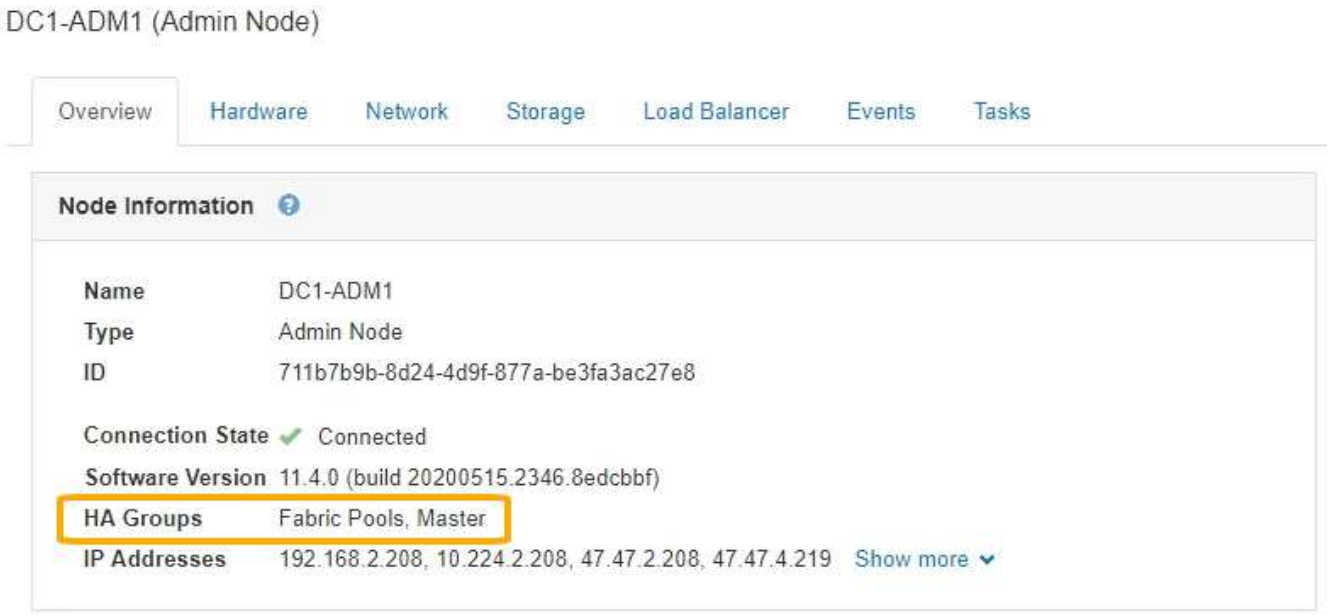
Les informations de présentation d'un nœud incluent les éléments suivants :

- **Nom** : nom d'hôte attribué au nœud et affiché dans le Grid Manager.
- **Type** : type de noeud — noeud d'administration, noeud de stockage, noeud de passerelle ou noeud d'archive.
- **ID** : identificateur unique du noeud, qui est également appelé UUID.
- **État de connexion** : l'un des trois États. L'icône de l'état le plus grave est affichée.
  - **Non connecté - Inconnu** : Le nœud n'est pas connecté à la grille pour une raison inconnue. Par exemple, la connexion réseau entre les nœuds a été perdue ou l'alimentation est coupée. L'alerte **Impossible de communiquer avec le noeud** peut également être déclenchée. D'autres alertes peuvent également être actives. Cette situation exige une attention immédiate.

    > Un nœud peut apparaître comme inconnu lors des opérations d'arrêt géré. Dans ces cas, vous pouvez ignorer l'état Inconnu.

  - **Non connecté - Arrêt administratif** : Le nœud n'est pas connecté à la grille pour une raison attendue. Par exemple, le nœud ou les services du nœud ont été normalement arrêtés, le nœud est en cours de redémarrage ou le logiciel est mis à niveau. Une ou plusieurs alertes peuvent également être actives.

    - * Connecté* ✔ : Le nœud est connecté à la grille.
- **Version du logiciel** : version de StorageGRID installée sur le nœud.
- **Groupes HA** : pour les nœuds d'administration et de passerelle uniquement. Indique si une interface réseau sur le nœud est incluse dans un groupe haute disponibilité et si cette interface est le maître ou la sauvegarde.



- **Adresses IP** : adresses IP du nœud. Cliquez sur **Afficher plus** pour afficher les adresses IPv4 et IPv6 du nœud et les mappages d'interface :
    - Eth0 : réseau grid
    - Eth1 : réseau d'administration
    - Eth2 : réseau client

Alertes

La section alertes de l'onglet vue d'ensemble répertorie toutes les alertes qui affectent actuellement ce nœud qui n'ont pas été réduites au silence. Cliquez sur le nom de l'alerte pour afficher des détails supplémentaires et les actions recommandées.

Informations associées

"Contrôle de l'état de connexion du nœud"

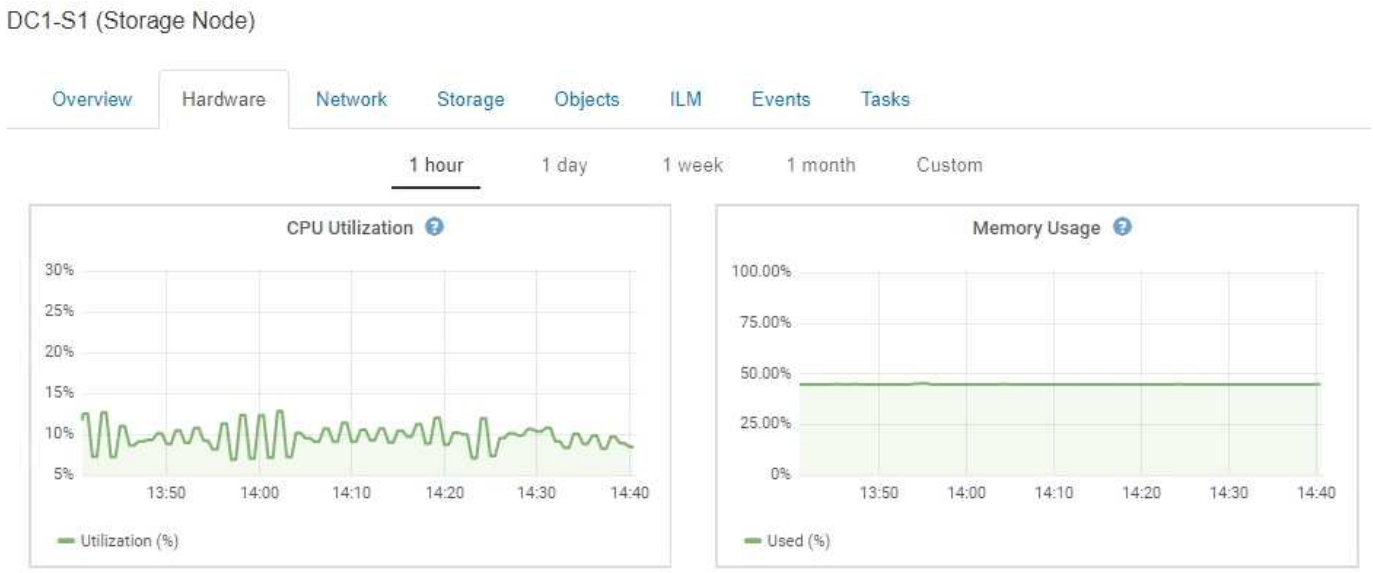
"Affichage des alertes en cours"

"Affichage d'une alerte spécifique"

Affichage de l'onglet matériel

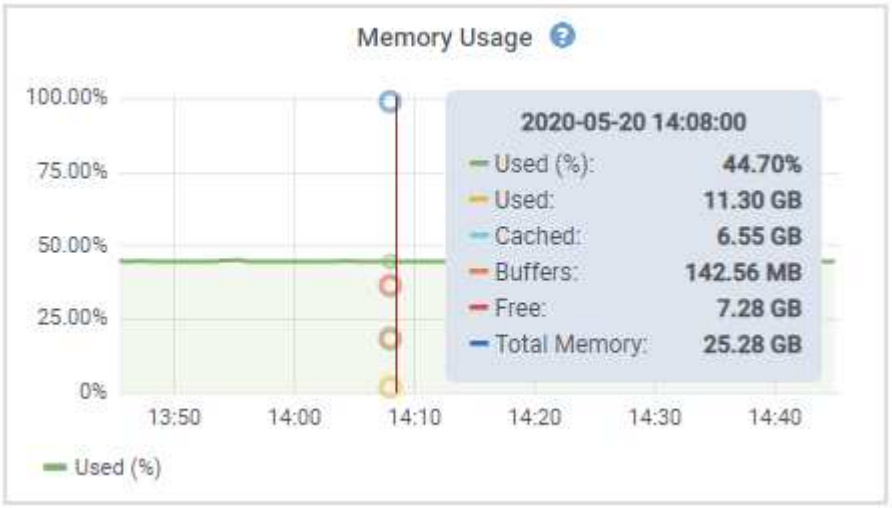
L'onglet matériel affiche l'utilisation du CPU et de la mémoire pour chaque nœud, ainsi que des informations supplémentaires sur le matériel des appliances.

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



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

Pour obtenir des détails sur l'utilisation du CPU et de la mémoire, passez le curseur sur chaque graphique.



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

Informations associées

"Affichage des informations sur les nœuds de stockage de l'appliance"

"Affichage des informations sur les nœuds d'administration de l'appliance et les nœuds de passerelle"

Affichage de l’onglet réseau

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

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

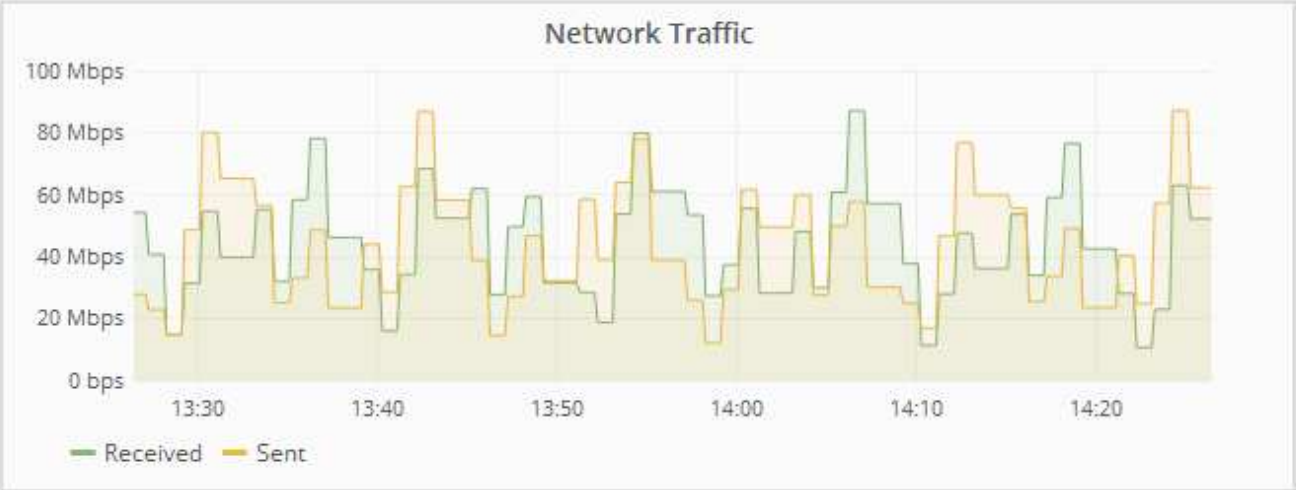
Pour afficher un intervalle de temps différent, sélectionnez l’une des commandes au-dessus du graphique ou du graphique. Vous pouvez afficher les informations disponibles pour les intervalles de 1 heure, 1 jour, 1 semaine ou 1 mois. Vous pouvez également définir un intervalle personnalisé, qui vous permet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

Pour les nœuds, le tableau Network interfaces fournit des informations sur les ports réseau physiques de chaque nœud. Le tableau Communications réseau fournit des détails sur les opérations de réception et de transmission de chaque nœud et sur tous les compteurs de pannes signalés par le conducteur.

DC1-S1-226 (Storage Node)

Overview | Hardware | Network | Storage | Objects | ILM | Events

1 hour | 1 day | 1 week | 1 month | 1 year | Custom



Network Interfaces

Name	Hardware Address	Speed	Duplex	Auto Negotiate	Link Status
eth0	00:50:56:A8:2A:75	10 Gigabit	Full	Off	Up

Network Communication

Receive

Interface	Data	Packets	Errors	Dropped	Frame Overruns	Frames
eth0	738.858 GB	904,587,345	0	14,340	0	0

Transmit

Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	677.555 GB	465,715,998	0	0	0	0

Informations associées

"Contrôle des connexions réseau et des performances"

Affichage de l'onglet stockage

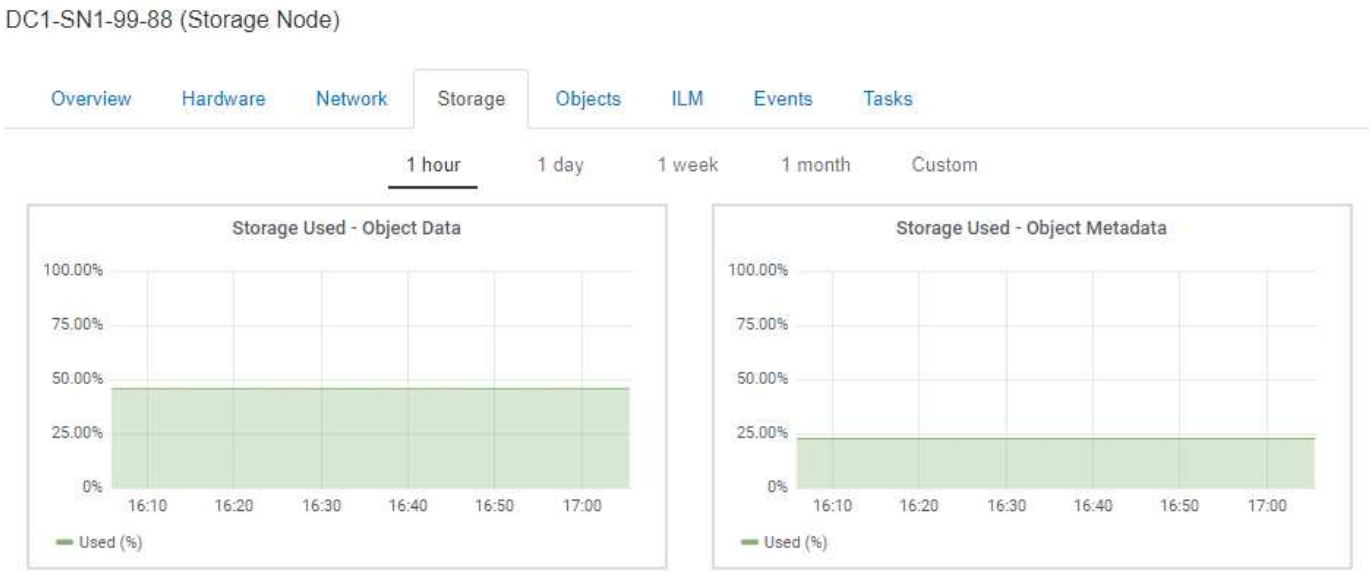
L'onglet stockage récapitule la disponibilité du stockage et d'autres mesures de stockage.

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

Graphiques utilisés pour le stockage

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

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



Unités de disque, volumes et tables de stockage d'objets

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

Disk Devices

Name	World Wide Name	I/O Load	Read Rate	Write Rate
croot(8:1,sda1)	N/A	0.03%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.85%	0 bytes/s	58 KB/s
sdc(8:16,sdb)	N/A	0.00%	0 bytes/s	81 bytes/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	14.90 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.10 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.18 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	96.45 GB	250.90 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

Informations associées

"Surveillance de la capacité de stockage pour l'ensemble de la grille"

"Contrôle de la capacité de stockage pour chaque nœud de stockage"

"Surveillance de la capacité des métadonnées d'objet pour chaque nœud de stockage"

Affichage de l'onglet événements

L'onglet Evénements affiche le nombre d'erreurs système ou d'événements de panne pour un nœud, y compris les erreurs telles que les erreurs réseau.

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

Si vous rencontrez des problèmes avec un nœud spécifique, vous pouvez utiliser l'onglet Events pour en savoir plus sur le problème. Le support technique peut également utiliser les informations de l'onglet événements pour vous aider dans le dépannage.

Vous pouvez effectuer ces tâches à partir de l'onglet événements :

- Utilisez les informations affichées pour le champ **dernier événement** en haut du tableau pour déterminer quel événement s'est produit le plus récemment.
- Cliquez sur l'icône du graphique pour qu'un événement spécifique puisse voir à quel moment cet événement s'est produit au fil du temps.

- Réinitialiser le nombre d'événements à zéro après la résolution de tout problème.

Informations associées

"Contrôle des événements"

"Affichage des graphiques et des graphiques"

"Réinitialisation du nombre d'événements"

Utilisation de l'onglet tâche pour redémarrer un nœud de la grille

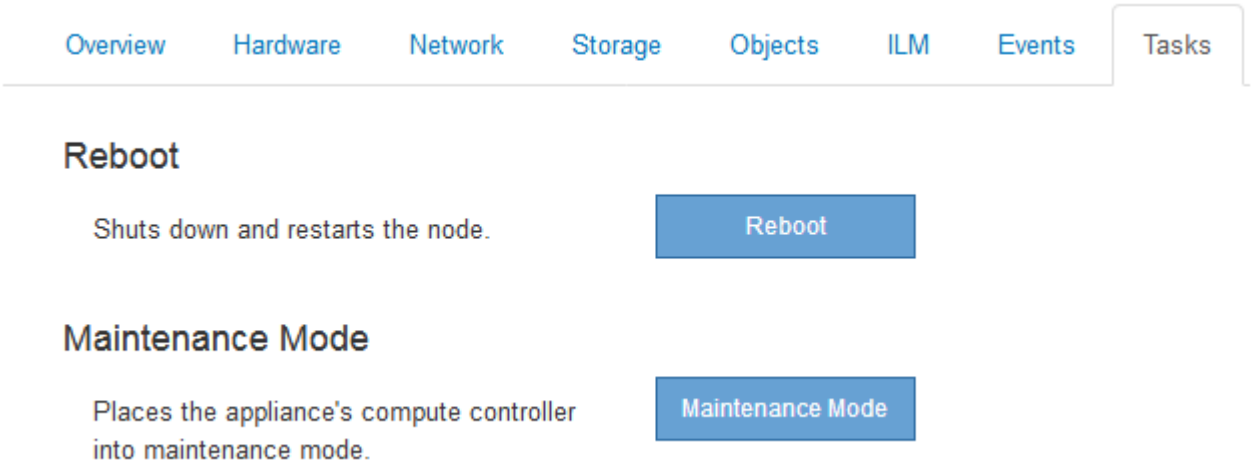
L'onglet tâche permet de redémarrer le nœud sélectionné. L'onglet tâche s'affiche pour tous les nœuds.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer de l'autorisation Maintenance ou accès racine.
- Vous devez disposer de la phrase secrète pour le provisionnement.

Description de la tâche

Vous pouvez utiliser l'onglet tâche pour redémarrer un nœud. Pour les nœuds d'appliance, vous pouvez également utiliser l'onglet tâche pour placer l'appliance en mode maintenance.



- Le redémarrage d'un nœud de grille à partir de l'onglet tâche émet la commande de redémarrage sur le nœud cible. Lorsque vous redémarrez un nœud, celui-ci s'arrête et redémarre. Tous les services sont redémarrés automatiquement.

  Si vous prévoyez de redémarrer un nœud de stockage, notez ce qui suit :

  - Si une règle ILM spécifie un comportement d'entrée de la double allocation ou si la règle indique un équilibrage et qu'il n'est pas possible de créer immédiatement toutes les copies nécessaires, StorageGRID valide immédiatement les objets récemment ingérées sur deux nœuds de stockage du même site, et évalue la ILM plus tard. Si vous souhaitez redémarrer deux ou plusieurs nœuds de stockage sur un site donné, il se peut que vous ne puissiez pas accéder à ces objets pendant la durée du redémarrage.
  - Pour vous assurer que vous pouvez accéder à tous les objets lors du redémarrage d'un nœud de

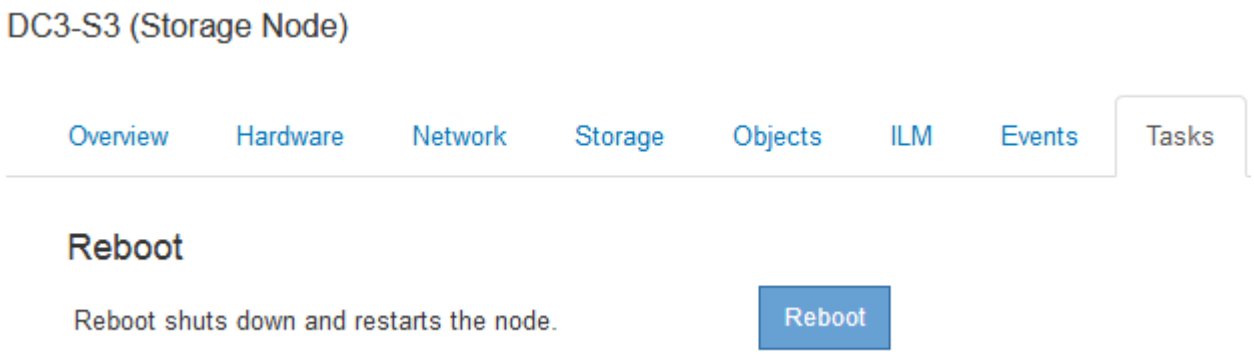
stockage, arrêtez de les ingérer sur un site pendant environ une heure avant de redémarrer le nœud.

- Vous devrez peut-être placer une appliance StorageGRID en mode de maintenance pour effectuer certaines procédures comme la modification de la configuration de la liaison ou le remplacement d'un contrôleur de stockage. Pour obtenir des instructions, reportez-vous aux instructions d'installation et de maintenance du matériel de l'appareil.

> Le passage d'une appliance en mode de maintenance peut rendre l'appliance indisponible pour l'accès à distance.

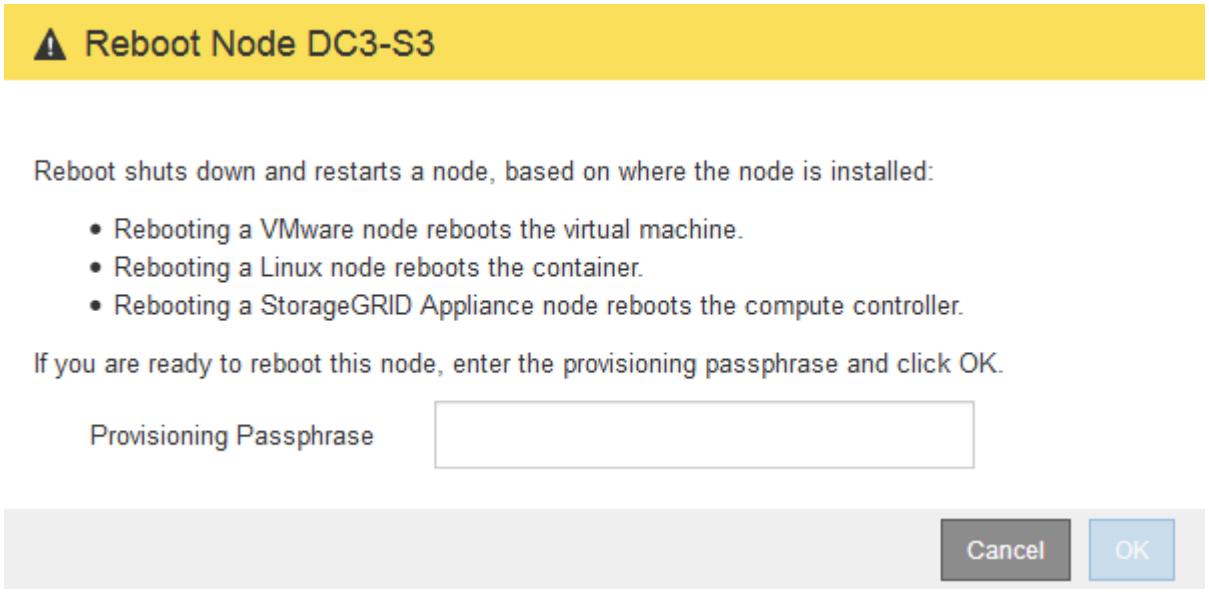
Étapes

1. Sélectionnez **noeuds**.
2. Sélectionnez le nœud de grille que vous souhaitez redémarrer.
3. Sélectionnez l'onglet **tâches**.



4. Cliquez sur **redémarrer**.

Une boîte de dialogue de confirmation s'affiche.



> Si vous redémarrez le nœud d'administration principal, la boîte de dialogue de confirmation vous rappelle que la connexion de votre navigateur au Grid Manager sera interrompue temporairement lorsque les services sont arrêtés.

5. Entrez la phrase de passe de provisionnement, puis cliquez sur **OK**.
6. Attendez que le nœud redémarre.

   La fermeture des services peut prendre un certain temps.

   Lorsque le nœud est en cours de redémarrage, l'icône grise (arrêt administratif) s'affiche sur le côté gauche de la page nœuds. Lorsque tous les services ont redémarré, l'icône revient à sa couleur d'origine.

Informations associées

"Dispositifs de stockage SG6000"

"Appliances de stockage SG5700"

"Appliances de stockage SG5600"

"SG100 etamp ; appareils de services SG1000"

Affichage de l'onglet objets

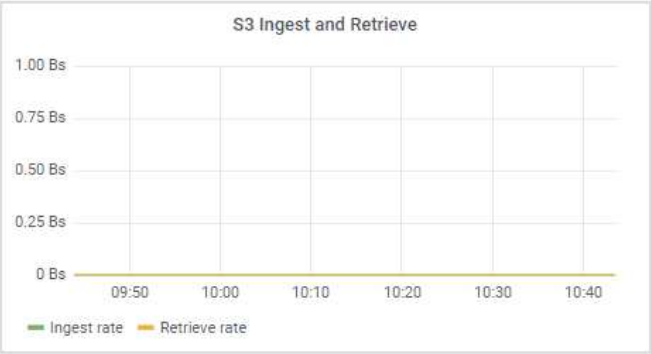
L'onglet objets fournit des informations sur les taux d'entrée et de récupération S3 et Swift.

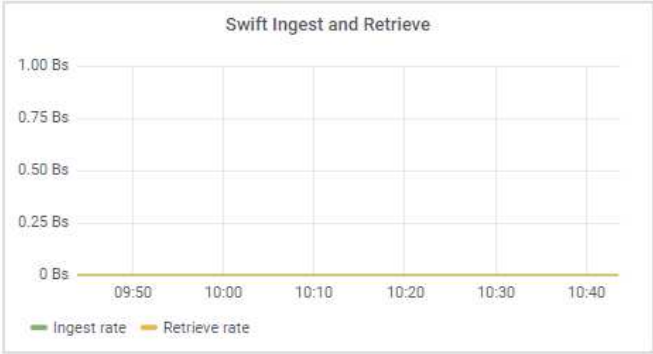
L'onglet objets s'affiche pour chaque nœud de stockage, chaque site et la grille entière. Pour les nœuds de stockage, l'onglet objets fournit également le nombre d'objets et des informations sur les requêtes de métadonnées et la vérification en arrière-plan.

DC1-S1 (Storage Node)

Overview | Hardware | Network | Storage | Objects | ILM | Events | Tasks

1 hour | 1 day | 1 week | 1 month | Custom





Object Counts

Total Objects	0
Lost Objects	0
S3 Buckets and Swift Containers	0

Queries

Average Latency	5.74 milliseconds
Queries - Successful	12,403
Queries - Failed (timed-out)	0
Queries - Failed (consistency level unmet)	0

Verification

Status	No Errors
Rate Setting	Adaptive
Percent Complete	0.00%
Average Stat Time	0.00 microseconds
Objects Verified	0
Object Verification Rate	0.00 objects / second
Data Verified	0 bytes
Data Verification Rate	0.00 bytes / second
Missing Objects	0
Corrupt Objects	0
Corrupt Objects Unidentified	0
Quarantined Objects	0

Informations associées

"Utilisation de S3"

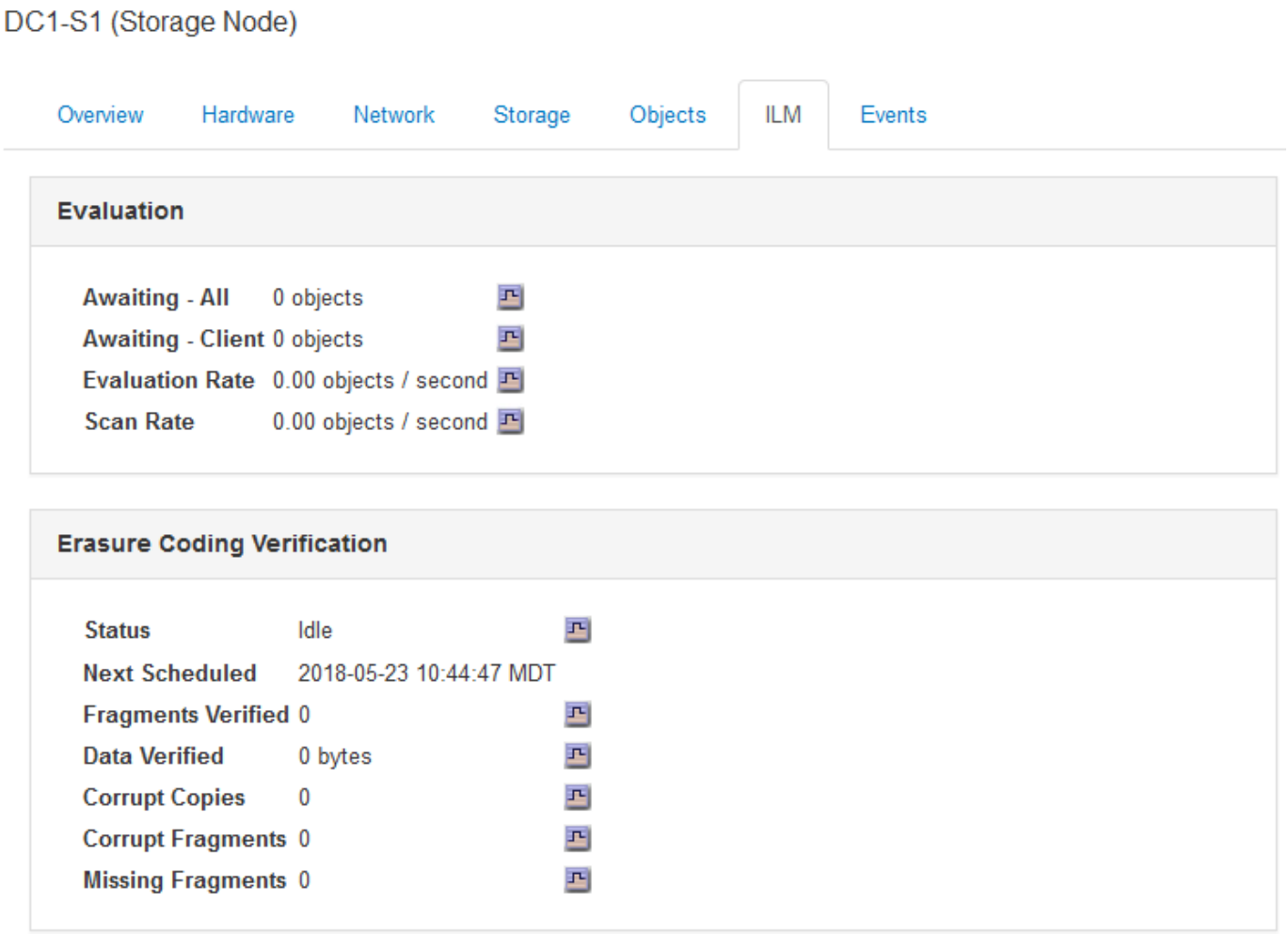
"Utiliser Swift"

Affichage de l'onglet ILM

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

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

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



Informations associées

"Contrôle de la gestion du cycle de vie des informations"

"Administrer StorageGRID"

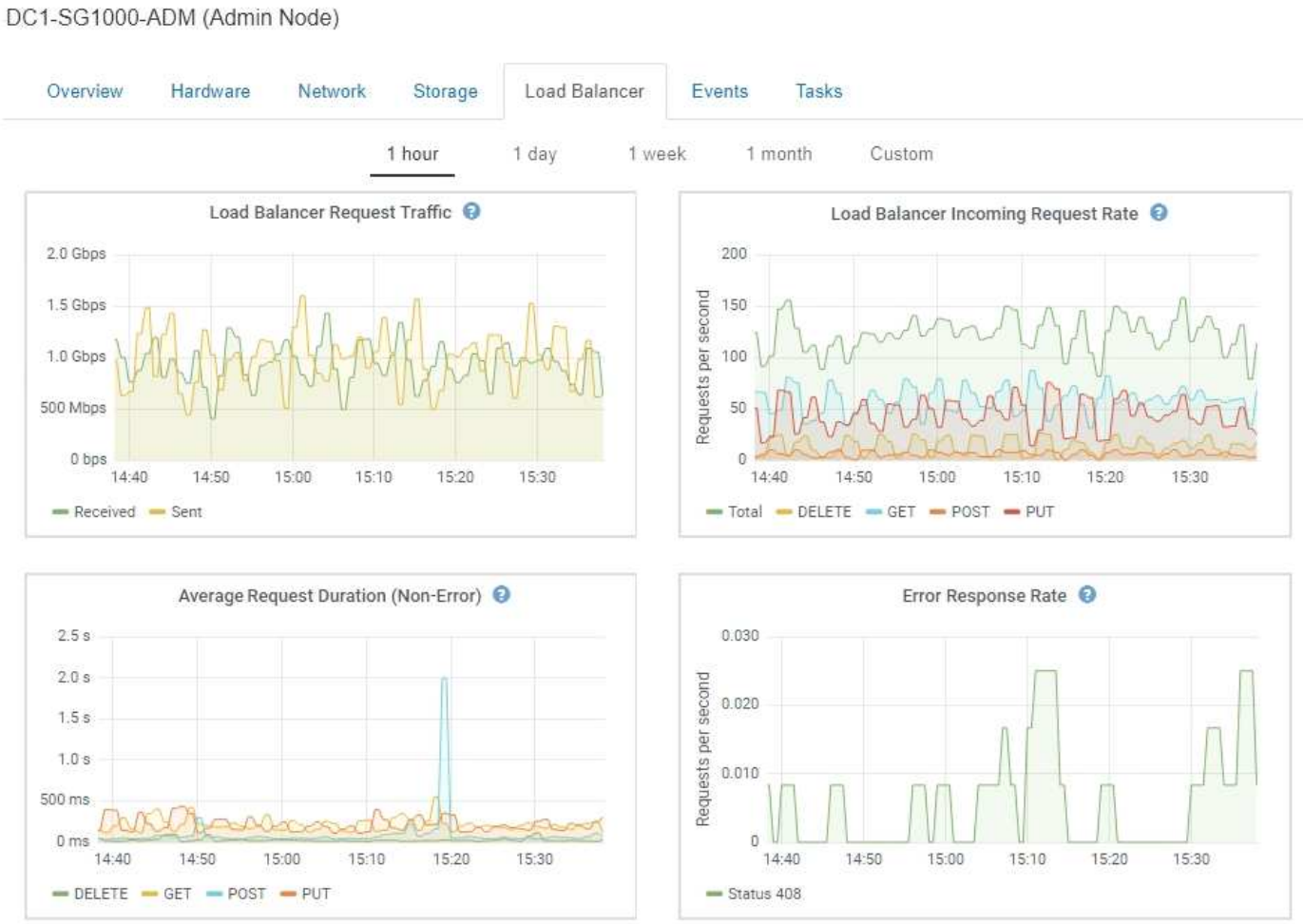
Affichage de l'onglet Load Balancer

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

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

statistiques pour tous les nœuds de ce site. Pour toute la grille, l'onglet Load Balancer fournit un récapitulatif global des statistiques pour tous les sites.

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



Trafic de demande d'équilibrage de charge

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

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

Débit de la demande entrante du équilibreur de charge

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

Durée moyenne de la demande (non-erreur)

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

Taux de réponse d'erreur

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

Informations associées

"Surveillance des opérations d'équilibrage des charges"

"Administrer StorageGRID"

Affichage de l'onglet Platform Services

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

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

Pour plus d'informations sur les services de la plateforme S3, notamment des informations de dépannage, consultez les instructions d'administration de StorageGRID.

Informations associées

"Administrer StorageGRID"

Affichage des informations sur les nœuds de stockage de l'appliance

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

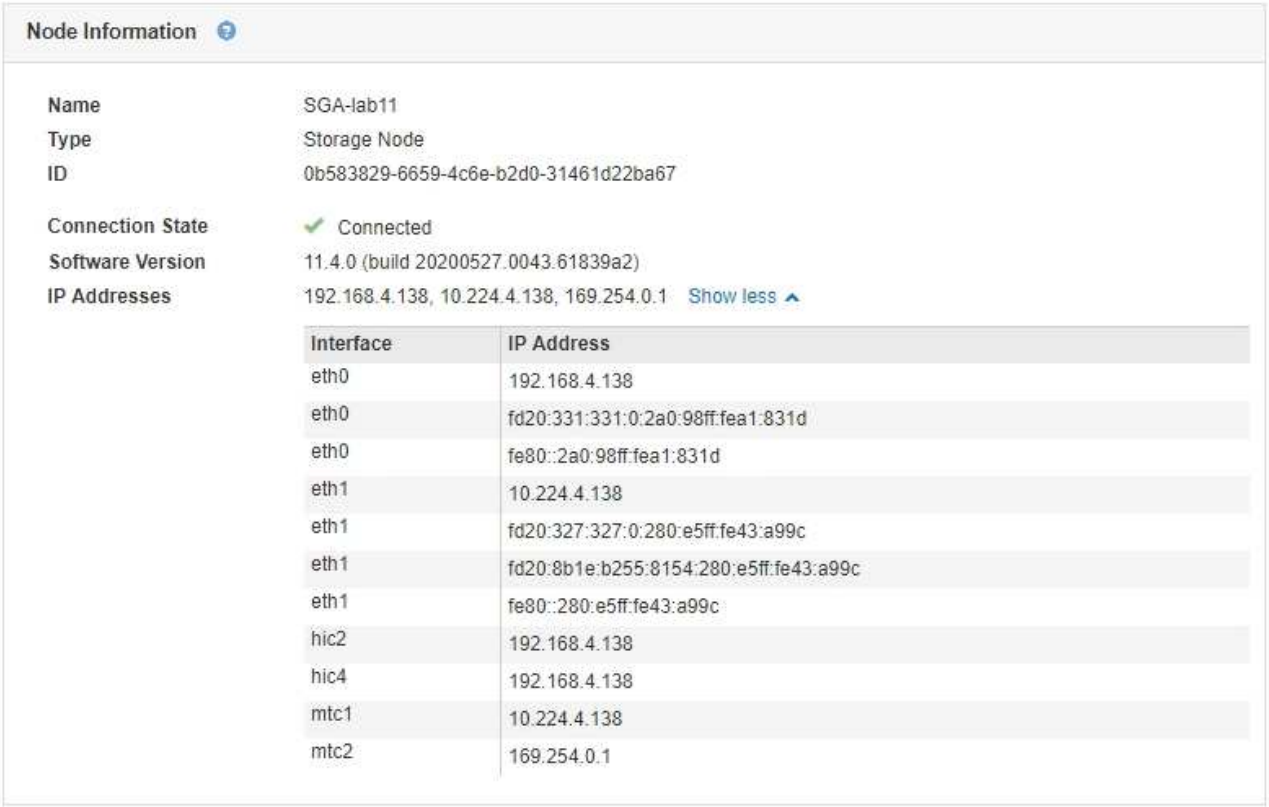
stockage, la version du firmware des contrôleurs, les ressources réseau, les interfaces réseau, les adresses réseau et de réception et de transmission des données.

Étapes

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

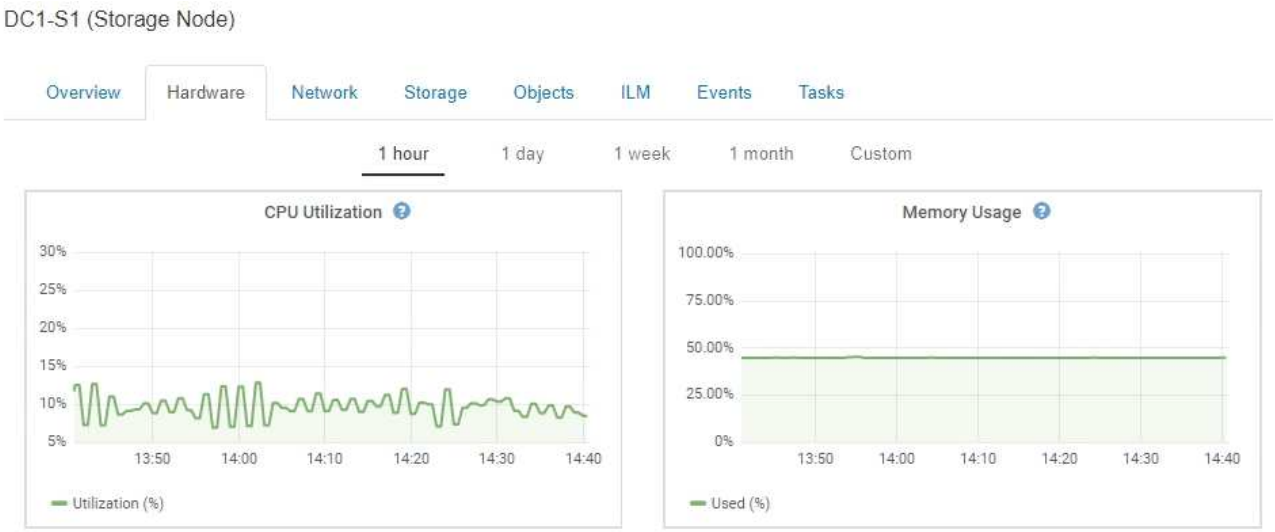
   Le tableau informations sur le nœud de l'onglet vue d'ensemble affiche l'ID et le nom du nœud, le type de nœud, la version logicielle installée et les adresses IP associées au nœud. La colonne interface contient le nom de l'interface, comme suit :

   - **Eth** : réseau Grid, réseau Admin ou réseau client.
   - **Hic** : un des ports physiques 10, 25 ou 100 GbE de l'appareil. Ces ports peuvent être liés ensemble et connectés au réseau StorageGRID Grid Network (eth0) et au réseau client (eth2).
   - **mtc** : l'un des ports physiques 1 GbE de l'appareil, qui peut être lié ou aliasé et connecté au réseau d'administration StorageGRID
     (eth1).



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

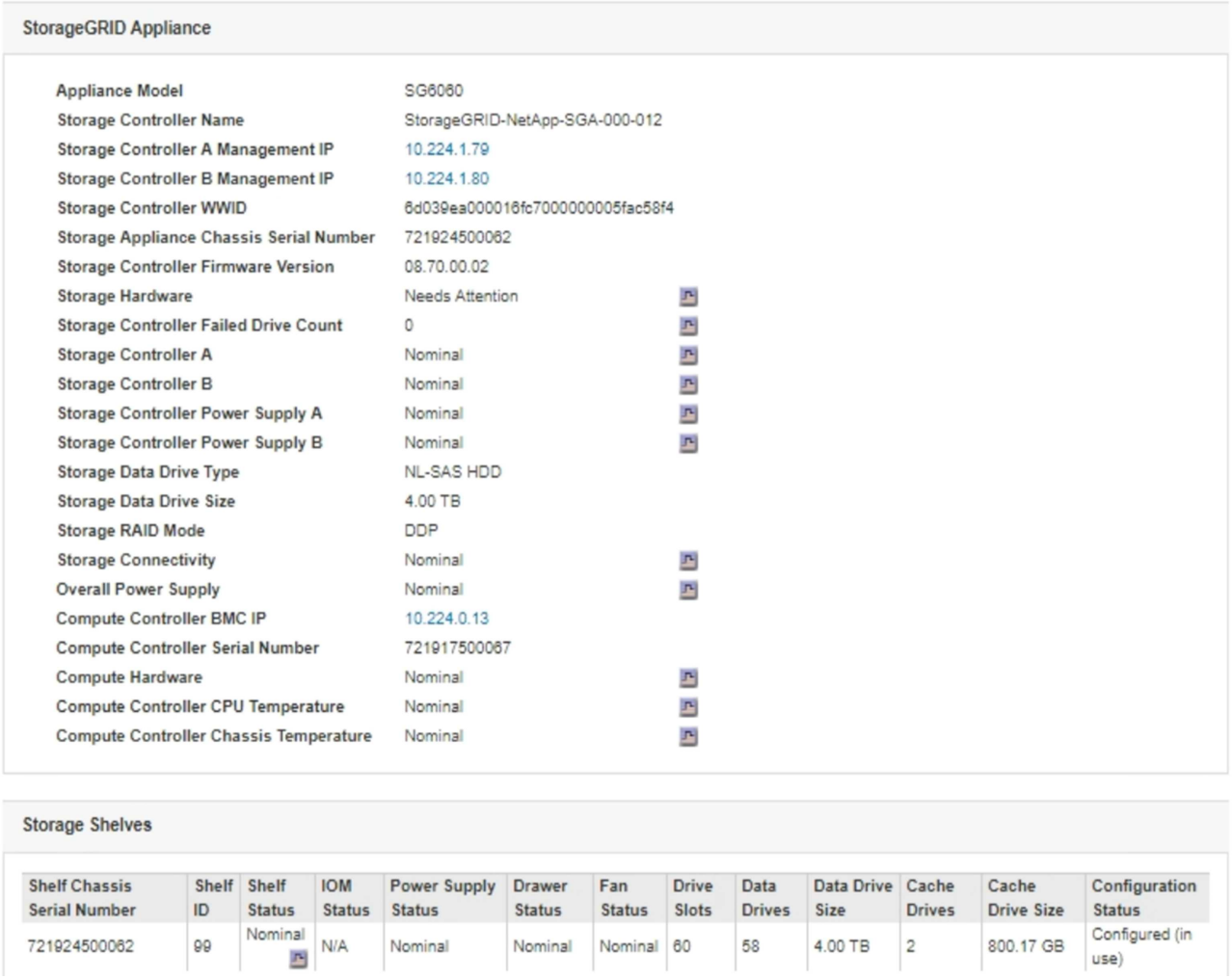
   a. Affichez les graphiques d'utilisation de l'UC et de la mémoire pour déterminer les pourcentages d'utilisation de l'UC et de la mémoire au fil du temps. Pour afficher un intervalle de temps différent, sélectionnez l'une des commandes au-dessus du graphique ou du graphique. Vous pouvez afficher les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



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

> Certains champs, tels que Compute Controller BMC IP et Compute Hardware, apparaissent uniquement pour les appliances dotées de cette fonctionnalité.

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



Dans la table Appliance	Description
Modèle de type appliance	Numéro de modèle de cette appliance StorageGRID présenté dans le logiciel SANtricity.
Nom de contrôleur de stockage	Nom de cette appliance StorageGRID illustré dans le logiciel SANtricity.
IP de gestion du contrôleur de stockage A	Adresse IP du port de gestion 1 sur le contrôleur de stockage A. Cette adresse IP vous permet d'accéder au logiciel SANtricity pour résoudre les problèmes de stockage.
IP de gestion du contrôleur de stockage B	Adresse IP du port de gestion 1 du contrôleur de stockage B. Cette adresse IP vous permet d'accéder au logiciel SANtricity pour résoudre les problèmes de stockage. Certains modèles d'appliance ne disposent pas d'un contrôleur de stockage B.

Dans la table Appliance	Description
WWID du contrôleur de stockage	Identifiant international du contrôleur de stockage représenté dans le logiciel SANtricity.
Numéro de série du châssis de l'appliance de stockage	Numéro de série du châssis de l'appareil.
Version du micrologiciel du contrôleur de stockage	Version du firmware du contrôleur de stockage de cette appliance.
Matériel de stockage	État global du matériel du contrôleur de stockage. Si SANtricity System Manager signale un état de nécessite une intervention pour le matériel de stockage, le système StorageGRID signale également cette valeur. Si le statut est « nécessite une attention », vérifiez d'abord le contrôleur de stockage à l'aide du logiciel SANtricity. Assurez-vous ensuite qu'aucune autre alarme ne s'applique au contrôleur de calcul.
Nombre de disques défaillants du contrôleur de stockage	Nombre de disques 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'appliance ne disposent pas d'un contrôleur de stockage B.
Alimentation A du contrôleur de stockage	L'état de l'alimentation A du contrôleur de stockage.
Alimentation B du contrôleur de stockage	L'état de l'alimentation B du contrôleur de stockage.
Type de disque de données de stockage	Type de disque dur de l'appliance, par exemple HDD (disque dur) ou SSD (disque SSD).
Taille du disque de données de stockage	Capacité totale comprenant tous les disques de données de l'appliance.
Mode de stockage RAID	Mode RAID configuré pour l'appliance.
Connectivité du stockage	État de la connectivité du stockage.
Bloc d'alimentation général	L'état de toutes les alimentations de l'appareil.

Dans la table Appliance	Description
IP BMC du contrôleur de calcul	Adresse IP du port du contrôleur de gestion de la carte mère (BMC) dans le contrôleur de calcul. Vous utilisez cette adresse IP pour vous connecter à l'interface BMC afin de surveiller et de diagnostiquer le matériel de l'appliance. Ce champ ne s'affiche pas pour les modèles d'appliance qui ne contiennent pas de BMC.
Numéro de série du contrôleur de calcul	Numéro de série du contrôleur de calcul.
Matériel de calcul	L'état du matériel du contrôleur de calcul. Ce champ ne s'affiche pas pour les modèles d'appliance ne disposant pas de matériel de calcul et de stockage séparé.
Température du processeur du contrôleur de calcul	L'état de température de l'UC du contrôleur de calcul.
Température du châssis du contrôleur de calcul	État de température du contrôleur de calcul.

+

Dans le tableau tiroirs de stockage	Description
Numéro de série du châssis du tiroir	Numéro de série du châssis du tiroir de stockage.
ID du tiroir	Identificateur numérique du tiroir de stockage. • 99 : tiroir contrôleur de stockage • 0 : premier tiroir d'extension • 1 : second tiroir d'extension **Remarque :** les étagères d'extension s'appliquent uniquement au SG6060.
État du tiroir	État global du shelf de stockage.
État du module d'E/S.	L'état des modules d'entrée/sortie (IOM) de tous les tiroirs d'extension. S/O s'il ne s'agit pas d'un tiroir d'extension.
État de l'alimentation électrique	État global des alimentations du tiroir de stockage.
Etat du tiroir	L'état des tiroirs dans le tiroir de rangement. N/A si la tablette ne contient pas de tiroirs.

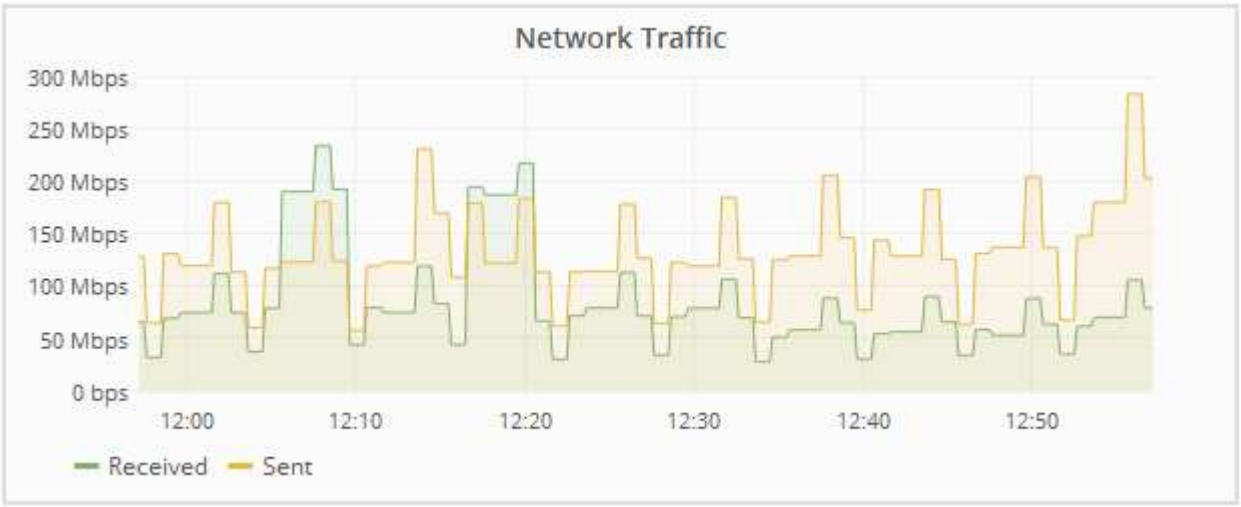
Dans le tableau tiroirs de stockage	Description
État du ventilateur	État général des ventilateurs dans le shelf de stockage.
Emplacements d'entraînement	Nombre total de slots de disque dans le shelf de stockage.
Disques de données	Nombre de disques du tiroir de stockage utilisés pour le stockage de données.
Taille du lecteur de données	Taille effective d'un disque de données dans le tiroir de stockage.
Lecteurs de cache	Nombre de disques du tiroir de stockage utilisés comme cache.
Taille du lecteur de cache	La taille du plus petit lecteur de cache dans le tiroir de stockage. En principe, les disques en cache sont de la même taille.
État de la configuration	L'état de configuration du tiroir de stockage.

4. Confirmer que tous les États sont « nominaux ».

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

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

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



   a. Consultez la section interfaces réseau.

Network Interfaces

Name	Hardware Address	Speed	Duplex	Auto Negotiate	Link Status
eth0	50:6B:4B:42:D7:11	100 Gigabit	Full	Off	Up
eth1	D8:C4:97:2A:E4:9E	Gigabit	Full	Off	Up
eth2	50:6B:4B:42:D7:11	100 Gigabit	Full	Off	Up
hic1	50:6B:4B:42:D7:11	25 Gigabit	Full	Off	Up
hic2	50:6B:4B:42:D7:11	25 Gigabit	Full	Off	Up
hic3	50:6B:4B:42:D7:11	25 Gigabit	Full	Off	Up
hic4	50:6B:4B:42:D7:11	25 Gigabit	Full	Off	Up
mtc1	D8:C4:97:2A:E4:9E	Gigabit	Full	On	Up
mtc2	D8:C4:97:2A:E4:9F	Gigabit	Full	On	Up

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

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

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

Pour plus d'informations sur la configuration des ports 10/25-GbE, reportez-vous aux instructions d'installation et de maintenance de votre appareil.

b. Passez en revue la section communication réseau.

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

Network Communication

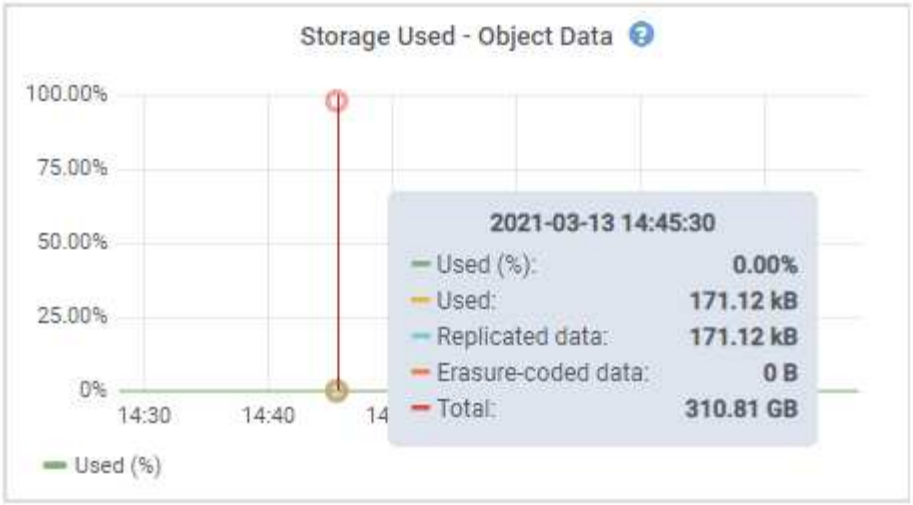
Receive

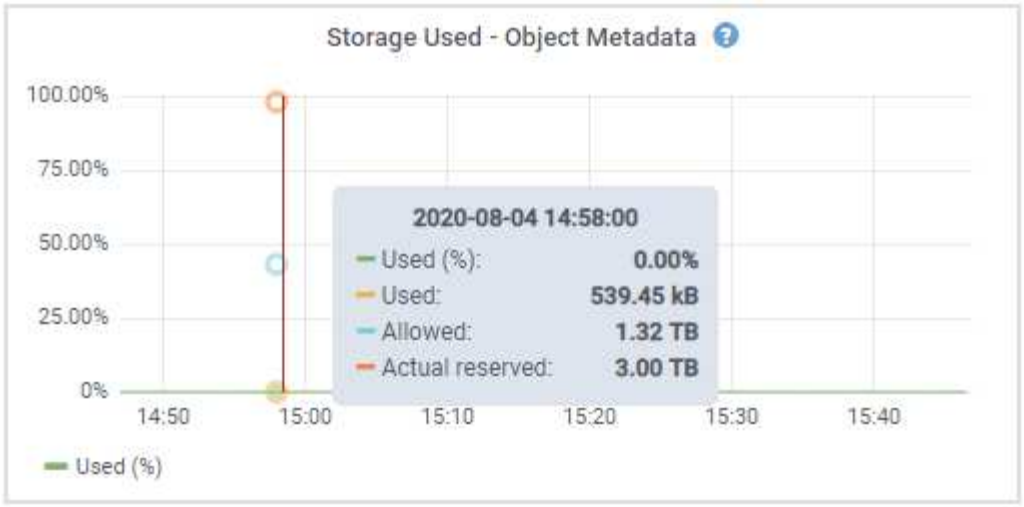
Interface	Data	Packets	Errors	Dropped	Frame Overruns	Frames
eth0	3.250 TB	5,610,578,144	0	8,327	0	0
eth1	1.205 GB	9,828,095	0	32,049	0	0
eth2	849.829 GB	186,349,407	0	10,269	0	0
hic1	114.864 GB	303,443,393	0	0	0	0
hic2	2.315 TB	5,351,180,956	0	305	0	0
hic3	1.690 TB	1,793,580,230	0	0	0	0
hic4	194.283 GB	331,640,075	0	0	0	0
mtc1	1.205 GB	9,828,096	0	0	0	0
mtc2	1.168 GB	9,564,173	0	32,050	0	0

Transmit

Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	5.759 TB	5,789,638,626	0	0	0	0
eth1	4.563 MB	41,520	0	0	0	0
eth2	855.404 GB	139,975,194	0	0	0	0
hic1	289.248 GB	326,321,151	5	0	0	5
hic2	1.636 TB	2,640,416,419	18	0	0	18
hic3	3.219 TB	4,571,516,003	33	0	0	33
hic4	1.687 TB	1,658,180,262	22	0	0	22
mtc1	4.563 MB	41,520	0	0	0	0
mtc2	49.678 KB	609	0	0	0	0

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

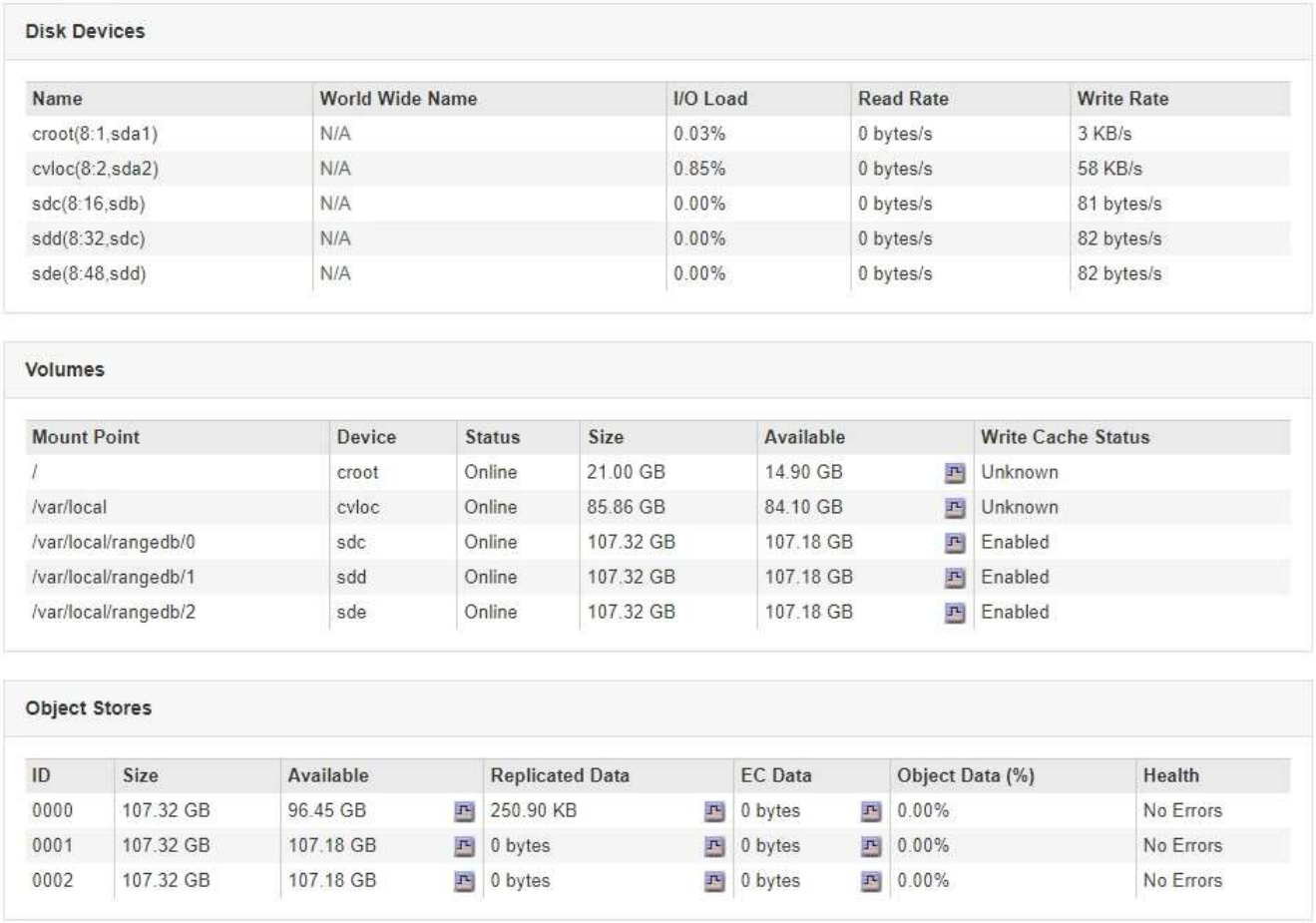




a. Faites défiler vers le bas pour afficher les quantités de stockage disponibles pour chaque volume et magasin d'objets.

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

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



Disk Devices

Name	World Wide Name	I/O Load	Read Rate	Write Rate
croot(8:1,sda1)	N/A	0.03%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.85%	0 bytes/s	58 KB/s
sdc(8:16,sdb)	N/A	0.00%	0 bytes/s	81 bytes/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	14.90 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.10 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.18 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	96.45 GB	250.90 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

Informations associées

"Dispositifs de stockage SG6000"

"Appliances de stockage SG5700"

"Appliances de stockage SG5600"

Affichage de l'onglet SANtricity System Manager

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

L'onglet SANtricity System Manager s'affiche pour les nœuds d'appliance de stockage.

Grâce à 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 CPU du contrôleur de stockage et le débit
- Vérifier l'état des composants matériels
- Réaliser des fonctions de support, comme visualiser les données de diagnostic et configurer le système E-Series AutoSupport

Pour utiliser SANtricity System Manager afin de configurer un proxy pour la baie AutoSupport E-Series, reportez-vous aux instructions du document d'administration deStorageGRID.

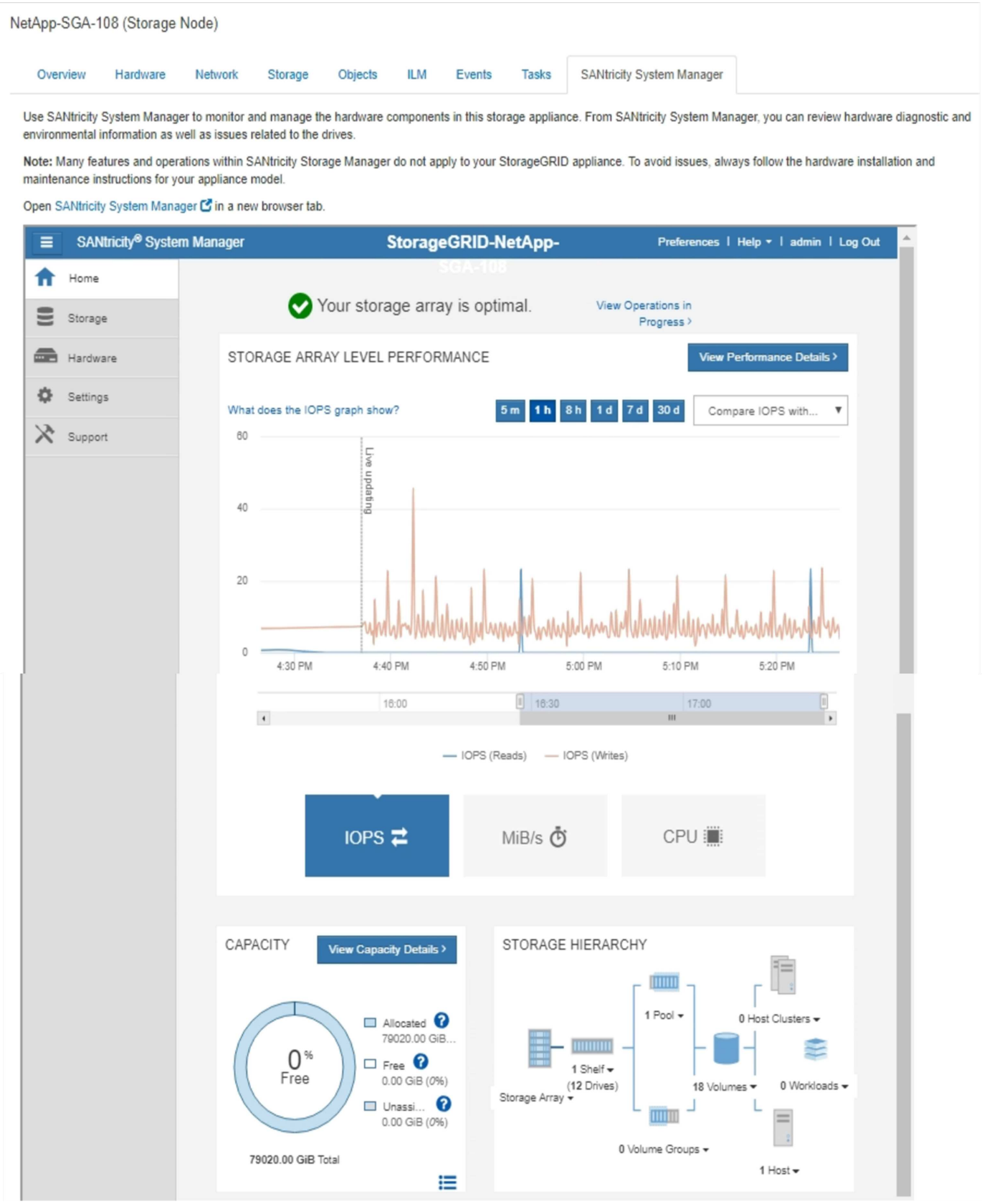
"Administrer StorageGRID"

Pour accéder à SANtricity System Manager via Grid Manager, vous devez disposer de l'autorisation Administrateur de l'appliance de stockage ou de l'autorisation accès racine.

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

L'accès à SANtricity System Manager à partir de Grid Manager se limite généralement à la surveillance du matériel de l'appliance et à la configuration des baies E-Series AutoSupport. De nombreuses fonctionnalités et opérations dans SANtricity System Manager, telles que la mise à niveau du firmware, ne s'appliquent pas à la surveillance de votre appliance StorageGRID. Pour éviter tout problème, suivez toujours les instructions d'installation et de maintenance du matériel de votre appareil.

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



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

Pour obtenir des informations détaillées sur les performances et l'utilisation de la capacité au niveau des baies

de stockage, passez le curseur de la souris sur chaque graphique.

Pour plus de détails sur l'affichage des informations accessibles depuis l'onglet SANtricity System Manager, reportez-vous aux informations du "Centre de documentation des systèmes NetApp E-Series"

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

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

Étapes

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

   Le tableau informations sur le nœud de l'onglet vue d'ensemble affiche l'ID et le nom du nœud, le type de nœud, la version logicielle installée et les adresses IP associées au nœud. La colonne interface contient le nom de l'interface, comme suit :

   - **Adllb** et **adlli** : affiché si la liaison actif/sauvegarde est utilisée pour l'interface réseau d'administration
   - **Eth** : réseau Grid, réseau Admin ou réseau client.
   - **Hic** : un des ports physiques 10, 25 ou 100 GbE de l'appareil. Ces ports peuvent être liés ensemble et connectés au réseau StorageGRID Grid Network (eth0) et au réseau client (eth2).
   - **mtc** : l'un des ports physiques 1 GbE de l'appareil, qui peut être lié ou aliasé et connecté au réseau d'administration StorageGRID
     (eth1).

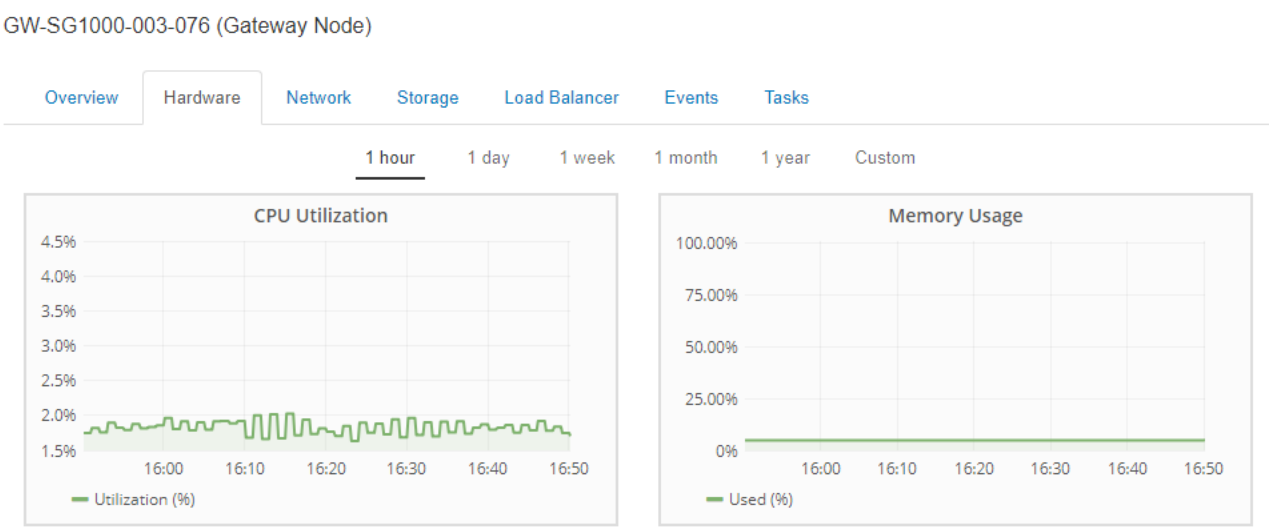
Node Information

ID	46702fe0-2bca-4097-8f61-f3fe6b22ed75
Name	GW-SG1000-003-076
Type	Gateway Node
Software Version	11.3.0 (build 20190708.2304.71ba19a)
IP Addresses	169.254.0.1, 172.16.3.76, 10.224.3.76, 47.47.3.76 Show less

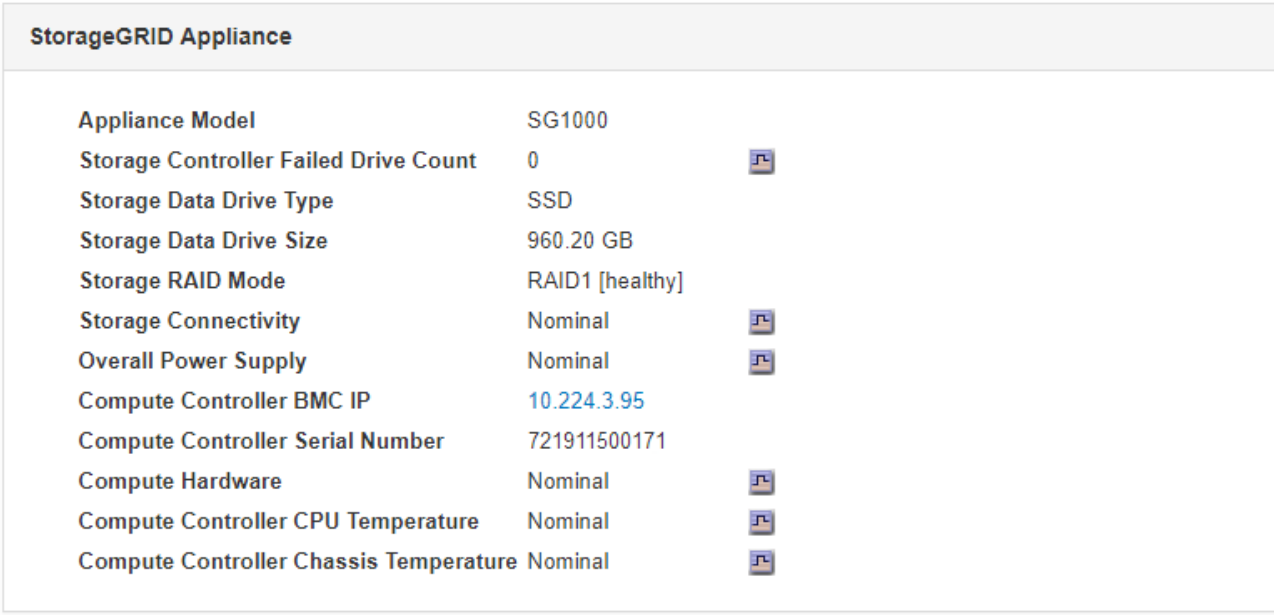
Interface	IP Address
adllb	fe80::c020:17ff:fe59:1cf3
adlli	169.254.0.1
adlli	fd20:327:327:0:408f:84ff:fe80:a9
adlli	fd20:8b1e:b255:8154:408f:84ff:fe80:a9
adlli	fe80::408f:84ff:fe80:a9
eth0	172.16.3.76
eth0	fd20:328:328:0:9a03:9bff:fe98:a272
eth0	fe80::9a03:9bff:fe98:a272
eth1	10.224.3.76
eth1	fd20:327:327:0:b6a9:fcff:fe08:4e49
eth1	fd20:8b1e:b255:8154:b6a9:fcff:fe08:4e49
eth1	fe80::b6a9:fcff:fe08:4e49
eth2	47.47.3.76
eth2	fd20:332:332:0:9a03:9bff:fe98:a272
eth2	fe80::9a03:9bff:fe98:a272
hic1	47.47.3.76
hic2	47.47.3.76
hic3	47.47.3.76
hic4	47.47.3.76
mtc1	10.224.3.76
mtc2	10.224.3.76

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

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



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



Dans la table Appliance	Description
Modèle de type appliance	Numéro de modèle de cette appliance StorageGRID.
Nombre de disques défaillants du contrôleur de stockage	Nombre de disques qui ne sont pas optimaux.
Type de disque de données de stockage	Type de disque dur de l'appliance, par exemple HDD (disque dur) ou SSD (disque SSD).
Taille du disque de données de stockage	Capacité totale comprenant tous les disques de données de l'appliance.

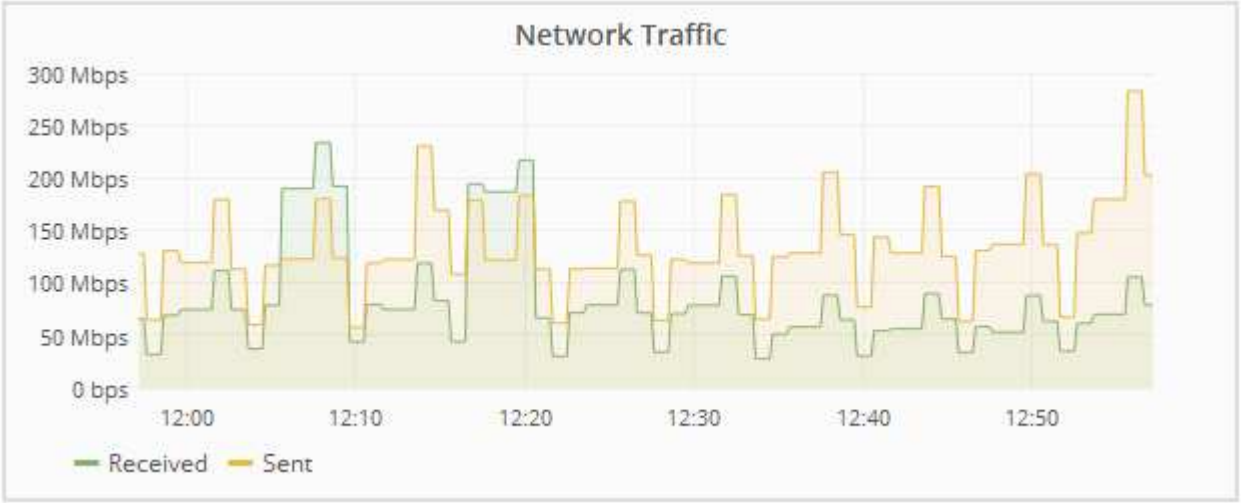
Dans la table Appliance	Description
Mode de stockage RAID	Mode RAID de l'appareil.
Bloc d'alimentation général	L'état de toutes les alimentations de l'appareil.
IP BMC du contrôleur de calcul	Adresse IP du port du contrôleur de gestion de la carte mère (BMC) dans le contrôleur de calcul. Vous pouvez utiliser cette adresse IP pour vous connecter à l'interface BMC afin de surveiller et de diagnostiquer le matériel de l'appliance. Ce champ ne s'affiche pas pour les modèles d'appliance qui ne contiennent pas de BMC.
Numéro de série du contrôleur de calcul	Numéro de série du contrôleur de calcul.
Matériel de calcul	L'état du matériel du contrôleur de calcul.
Température du processeur du contrôleur de calcul	L'état de température de l'UC du contrôleur de calcul.
Température du châssis du contrôleur de calcul	État de température du contrôleur de calcul.

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

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

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

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



a. Consultez la section interfaces réseau.

Network Interfaces

Name	Hardware Address	Speed	Duplex	Auto Negotiate	Link Status
adllb	C2:20:17:59:1C:F3	10 Gigabit	Full	Off	Up
adlli	42:8F:84:80:00:A9	10 Gigabit	Full	Off	Up
eth0	98:03:9B:98:A2:72	400 Gigabit	Full	Off	Up
eth1	B4:A9:FC:08:4E:49	10 Gigabit	Full	Off	Up
eth2	98:03:9B:98:A2:72	400 Gigabit	Full	Off	Up
hic1	98:03:9B:98:A2:72	100 Gigabit	Full	On	Up
hic2	98:03:9B:98:A2:72	100 Gigabit	Full	On	Up
hic3	98:03:9B:98:A2:72	100 Gigabit	Full	On	Up
hic4	98:03:9B:98:A2:72	100 Gigabit	Full	On	Up
mtc1	B4:A9:FC:08:4E:49	Gigabit	Full	On	Up
mtc2	B4:A9:FC:08:4E:49	Gigabit	Full	On	Up

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

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

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

b. Passez en revue la section communication réseau.

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

Network Communication

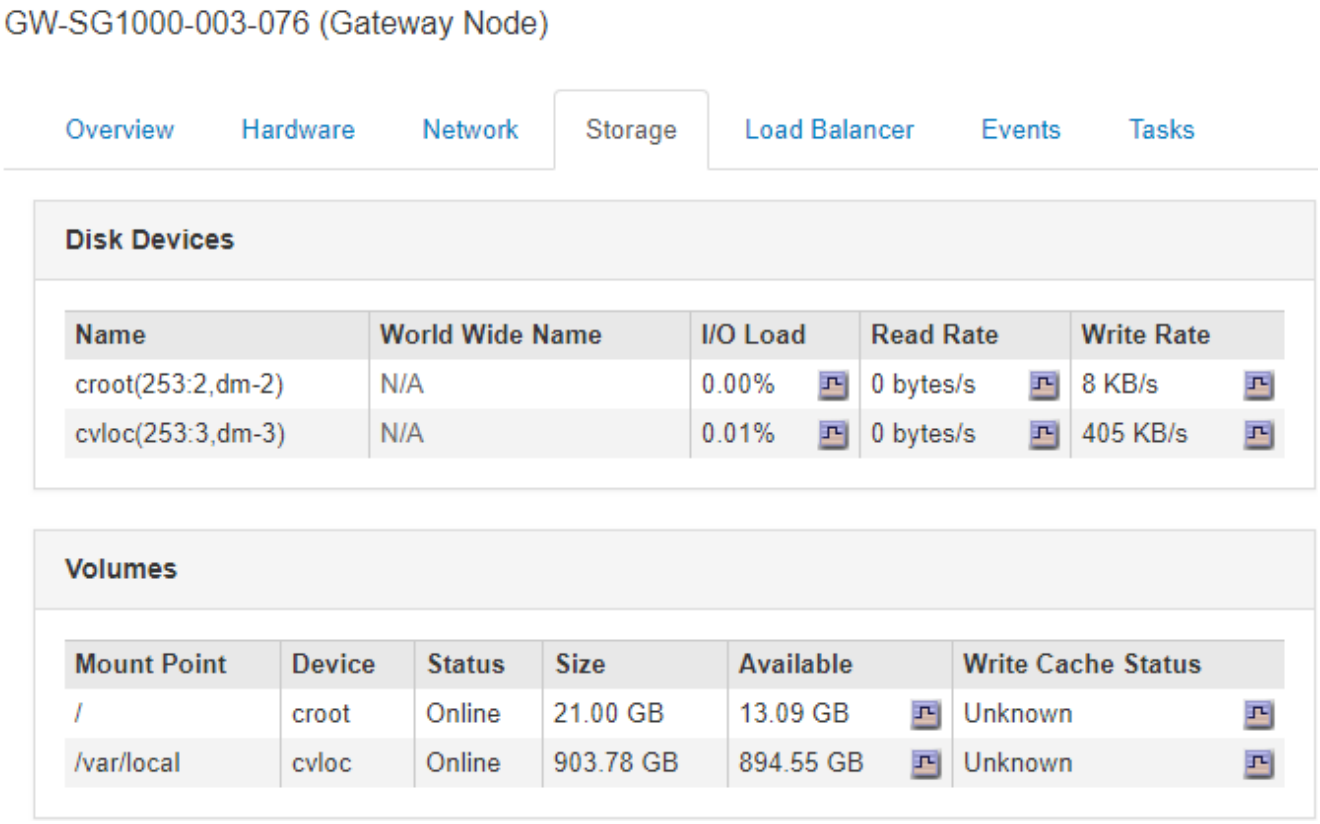
Receive

Interface	Data	Packets	Errors	Dropped	Frame Overruns	Frames
eth0	3.250 TB	5,610,578,144	0	8,327	0	0
eth1	1.205 GB	9,828,095	0	32,049	0	0
eth2	849.829 GB	186,349,407	0	10,269	0	0
hic1	114.864 GB	303,443,393	0	0	0	0
hic2	2.315 TB	5,351,180,956	0	305	0	0
hic3	1.690 TB	1,793,580,230	0	0	0	0
hic4	194.283 GB	331,640,075	0	0	0	0
mtc1	1.205 GB	9,828,096	0	0	0	0
mtc2	1.168 GB	9,564,173	0	32,050	0	0

Transmit

Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	5.759 TB	5,789,638,626	0	0	0	0
eth1	4.563 MB	41,520	0	0	0	0
eth2	855.404 GB	139,975,194	0	0	0	0
hic1	289.248 GB	326,321,151	5	0	0	5
hic2	1.636 TB	2,640,416,419	18	0	0	18
hic3	3.219 TB	4,571,516,003	33	0	0	33
hic4	1.687 TB	1,658,180,262	22	0	0	22
mtc1	4.563 MB	41,520	0	0	0	0
mtc2	49.678 KB	609	0	0	0	0

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



Informations associées

"SG100 etamp ; appareils de services SG1000"

Informations à surveiller régulièrement

StorageGRID est un système de stockage distribué, tolérant aux pannes et conçu pour continuer à fonctionner même en cas d'erreur, ou lorsque des nœuds ou des sites sont indisponibles. Vous devez surveiller de manière proactive l'état du système, les workloads et les statistiques d'utilisation afin de pouvoir prendre les mesures nécessaires pour résoudre les problèmes potentiels avant qu'ils n'affectent l'efficacité ou la disponibilité du réseau.

Un système occupé génère de grandes quantités d'informations. Cette section fournit des conseils sur les informations les plus importantes à surveiller de façon continue. Cette section contient les sous-sections suivantes :

- "Surveillance de l'état du système"
- "Contrôle de la capacité de stockage"
- "Contrôle de la gestion du cycle de vie des informations"
- "Surveillance des performances, de la mise en réseau et des ressources système"
- "Contrôle de l'activité des locataires"
- "Contrôle de la capacité d'archivage"
- "Surveillance des opérations d'équilibrage des charges"

- "Application de correctifs ou mise à niveau des logiciels si nécessaire"

Quoi surveiller	Fréquence
Les données d'état du système qui s'affichent sur le tableau de bord de Grid Manager si quelque chose a changé par rapport à la veille.	Tous les jours
Vitesse de consommation de la capacité des objets et des métadonnées du nœud de stockage	Hebdomadaire
Opérations de gestion du cycle de vie des informations	Hebdomadaire
Performances, mise en réseau et ressources système : • Latence des requêtes • Connectivité et réseau • Ressources au niveau des nœuds	Hebdomadaire
Activité des locataires	Hebdomadaire
Capacité du système de stockage d'archives externe	Hebdomadaire
Opérations d'équilibrage de la charge	Après la configuration initiale et après toute modification de la configuration
Disponibilité des correctifs logiciels et des mises à niveau logicielles	Tous les mois

Surveillance de l'état du système

Il est conseillé de surveiller l'état général de votre système StorageGRID tous les jours.

Le système StorageGRID est tolérant aux pannes et peut continuer à fonctionner même lorsque des parties de la grille sont indisponibles. Le premier signe d'un problème potentiel avec votre système StorageGRID est susceptible d'être une alerte ou une alarme (système hérité) et pas nécessairement un problème de fonctionnement du système. Porter une attention particulière à l'état du système peut vous aider à détecter des problèmes mineurs avant qu'ils n'affectent les opérations ou l'efficacité du réseau.

Le volet Santé du tableau de bord de Grid Manager fournit un récapitulatif des problèmes susceptibles d'affecter votre système. Vous devez examiner tous les problèmes qui apparaissent sur le tableau de bord.

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

1. Connectez-vous au Grid Manager pour afficher le tableau de bord.

2. Passez en revue les informations du panneau Santé.

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

Lien	Indique
Détails de la grille	S'affiche si des nœuds sont déconnectés (état de connexion inconnu ou arrêt administratif). Cliquez sur le lien ou cliquez sur l'icône bleue ou grise pour déterminer le ou les nœuds concernés.
Alertes en cours	S'affiche si des alertes sont actuellement actives. Cliquez sur le lien ou cliquez sur **critique**, **majeur** ou **mineur** pour voir les détails sur la page **alertes** > **courant**.
Alertes récemment résolues	S'affiche si des alertes déclenchées la semaine passée sont à présent résolues. Cliquez sur le lien pour voir les détails sur la page **alertes** > **résolu**.
Alarmes anciennes	S'affiche si des alarmes (système hérité) sont actuellement actives. Cliquez sur le lien pour afficher les détails sur la page **support** > **alarmes (hérité)** > **alarmes actuelles**. **Remarque :** alors que le système d'alarme existant continue d'être pris en charge, le système d'alerte offre des avantages significatifs et est plus facile à utiliser.
Licence	S'affiche en cas de problème avec la licence logicielle de ce système StorageGRID. Cliquez sur le lien pour afficher les détails sur la page **Maintenance** > **système** > **Licence**.

Informations associées

"Administrer StorageGRID"

"Configuration des notifications par e-mail pour les alertes"

"Utilisation de la surveillance SNMP"

Contrôle de l'état de connexion du nœud

Si un ou plusieurs nœuds sont déconnectés de la grille, les opérations StorageGRID stratégiques peuvent être affectées. Vous devez contrôler l'état de connexion des nœuds et résoudre tout problème dans les plus brefs délais.

Ce dont vous avez besoin

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

Description de la tâche

Les nœuds peuvent avoir l'un des trois États de connexion suivants :

- **Non connecté - Inconnu** : Le nœud n'est pas connecté à la grille pour une raison inconnue. Par exemple, la connexion réseau entre les nœuds a été perdue ou l'alimentation est coupée. L'alerte **Impossible de communiquer avec le noeud** peut également être déclenchée. D'autres alertes peuvent également être actives. Cette situation exige une attention immédiate.

  > Un nœud peut apparaître comme inconnu lors des opérations d'arrêt géré. Dans ces cas, vous pouvez ignorer l'état Inconnu.

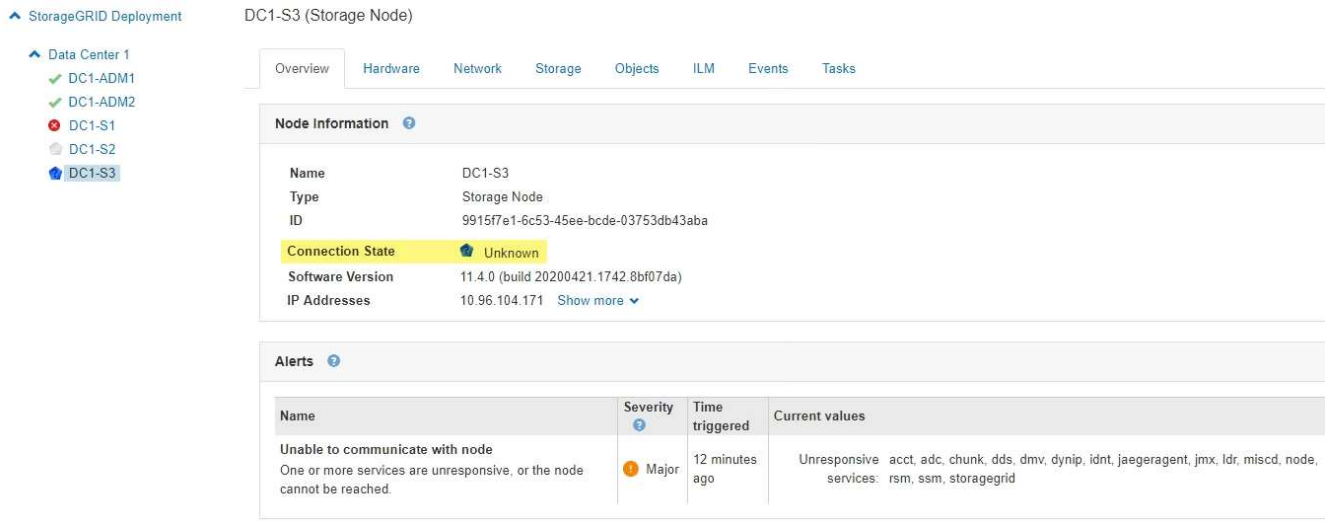
- **Non connecté - Arrêt administratif** : Le nœud n'est pas connecté à la grille pour une raison attendue. Par exemple, le nœud ou les services du nœud ont été normalement arrêtés, le nœud est en cours de redémarrage ou le logiciel est mis à niveau. Une ou plusieurs alertes peuvent également être actives.
- * Connecté* : Le nœud est connecté à la grille.

Étapes

1. Si une icône bleue ou grise apparaît dans le panneau Santé du tableau de bord, cliquez sur l'icône ou sur **Détails de la grille**. (Les icônes bleue ou grise et le lien **Grid details** apparaissent uniquement si au moins un nœud est déconnecté de la grille.)

   La page vue d'ensemble du premier nœud bleu de l'arborescence des nœuds s'affiche. S'il n'y a pas de nœuds bleus, la page vue d'ensemble du premier nœud gris de l'arborescence s'affiche.

   Dans l'exemple, le nœud de stockage nommé DC1-S3 possède une icône bleue. L'état de connexion * du panneau informations sur le nœud est **Inconnu** et l'alerte **Impossible de communiquer avec le noeud** est active. L'alerte indique qu'un ou plusieurs services ne répondent pas ou que le nœud ne peut pas être atteint.



2. Si un nœud dispose d'une icône bleue, effectuez la procédure suivante :
   a. Sélectionnez chaque alerte dans le tableau et suivez les actions recommandées.

      Par exemple, vous devrez peut-être redémarrer un service qui a arrêté ou redémarré l'hôte du nœud.

   b. Si vous ne pouvez pas remettre le nœud en ligne, contactez le support technique.
3. Si un nœud dispose d'une icône grise, effectuez la procédure suivante :

   Les nœuds gris sont attendus lors des procédures de maintenance et peuvent être associés à une ou plusieurs alertes. Selon le problème sous-jacent, ces nœuds « hors service administratif » sont souvent remis en ligne sans intervention.

   a. Passez en revue la section alertes et déterminez si des alertes affectent ce nœud.
   b. Si une ou plusieurs alertes sont actives, sélectionnez chaque alerte dans le tableau et suivez les actions recommandées.
   c. Si vous ne pouvez pas remettre le nœud en ligne, contactez le support technique.

Informations associées

"Référence des alertes"

"Maintenance et récupération"

Affichage des alertes en cours

Lorsqu'une alerte est déclenchée, une icône d'alerte s'affiche sur le tableau de bord. Une icône d'alerte s'affiche également pour le nœud sur la page nœuds. Il est également possible d'envoyer une notification par e-mail, à moins que l'alerte n'ait été neutralisée.

Ce dont vous avez besoin

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

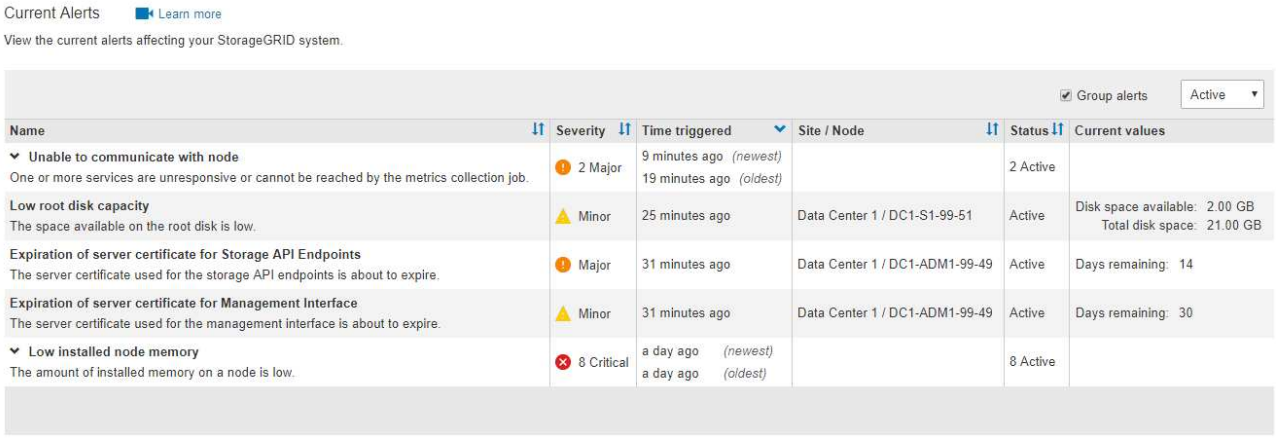
Étapes

1. Si une ou plusieurs alertes sont actives, procédez de l'une des façons suivantes :
   - Dans le panneau Santé du tableau de bord, cliquez sur l'icône d'alerte ou cliquez sur **alertes actuelles**. (Une icône d'alerte et le lien **alertes actuelles** n'apparaissent que si au moins une alerte est

active.)

- Sélectionnez **alertes** > **actuel**.

  La page alertes en cours s'affiche. Il répertorie toutes les alertes qui affectent actuellement votre système StorageGRID.



  Les alertes sont affichées par défaut comme suit :

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

    La page alertes actuelle est actualisée toutes les deux minutes.

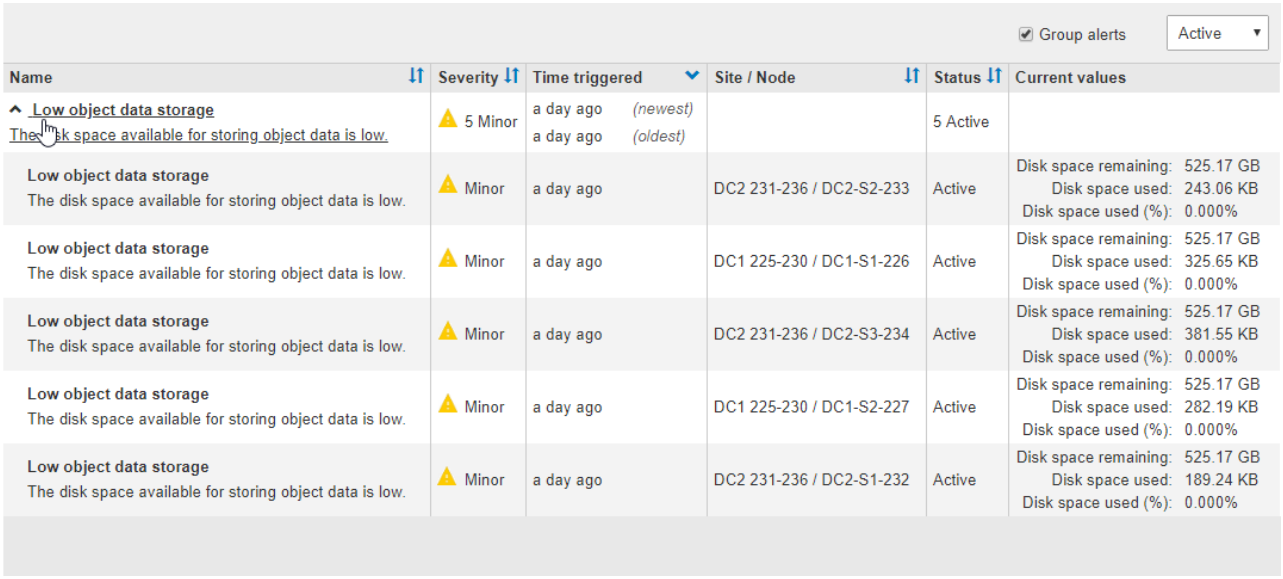
2. Vérifiez les informations du tableau.

En-tête de colonne	Description
Nom	Le nom de l'alerte et sa description.

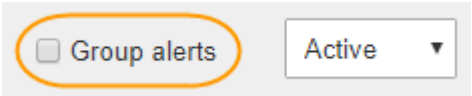
En-tête de colonne	Description
Gravité	Gravité de l'alerte. Si plusieurs alertes sont regroupées, la ligne de titre indique le nombre d'instances de cette alerte à chaque gravité. • **Critique** : Il existe une condition anormale qui a arrêté les opérations normales d'un nœud ou service StorageGRID. Vous devez immédiatement résoudre le problème sous-jacent. Une interruption du service et une perte de données peuvent se produire si le problème n'est pas résolu. • **Majeur** : Il existe une condition anormale affectant les opérations en cours ou approchant le seuil d'une alerte critique. Vous devez examiner les alertes majeures et résoudre tous les problèmes sous-jacents pour vérifier que leur condition anormale n'arrête pas le fonctionnement normal d'un nœud ou d'un service StorageGRID. • **Mineur** : Le système fonctionne normalement, mais il existe une condition anormale qui pourrait affecter la capacité du système à fonctionner s'il continue. Vous devez surveiller et résoudre les alertes mineures qui ne sont pas claires par elles-mêmes pour vous assurer qu'elles n'entraînent pas un problème plus grave.
Temps déclenché	Il y a combien de temps l'alerte a été déclenchée. Si plusieurs alertes sont regroupées, la ligne de titre affiche les heures de l'instance la plus récente de l'alerte (*le plus récent*) et de l'instance la plus ancienne de l'alerte (*le plus ancien*).
Site/nœud	Nom du site et du nœud où l'alerte se produit. Si plusieurs alertes sont regroupées, les noms de site et de nœud ne s'affichent pas dans la ligne de titre.
État	Indique si l'alerte est active ou a été neutralisée. Si plusieurs alertes sont regroupées et que **toutes les alertes** sont sélectionnées dans la liste déroulante, la ligne de titre indique le nombre d'instances de cette alerte actives et le nombre d'instances désactivées.

En-tête de colonne	Description
Valeurs actuelles	Valeur actuelle de la mesure qui a déclenché 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 **stockage de données d'objet bas** comprennent le pourcentage d'espace disque utilisé, la quantité totale d'espace disque et la quantité d'espace disque utilisée. **Remarque :** si plusieurs alertes sont regroupées, les valeurs actuelles ne sont pas affichées dans la ligne de titre.

3. Pour développer et réduire des groupes d'alertes :
   - Pour afficher les alertes individuelles d'un groupe, cliquez sur le point d'arrêt ⌄ dans l'en-tête ou cliquez sur le nom du groupe.
   - Pour masquer les alertes individuelles d'un groupe, cliquez sur le point d'insertion ⌃ dans l'en-tête ou cliquez sur le nom du groupe.



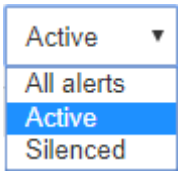
4. Pour afficher des alertes individuelles au lieu de groupes d'alertes, décochez la case **alertes de groupe** en haut du tableau.



5. Pour trier les alertes ou les groupes d'alertes, cliquez sur les flèches haut/bas ⇅ dans chaque en-tête de colonne.
   - Lorsque **alertes de groupe** est sélectionné, les groupes d'alertes et les alertes individuelles de chaque groupe sont triés. Par exemple, vous pouvez trier les alertes d'un groupe par **heure déclenchée** pour trouver l'instance la plus récente d'une alerte spécifique.
   - Lorsque **alertes de groupe** n'est pas sélectionnée, la liste complète des alertes est triée. Par exemple, vous pouvez trier toutes les alertes par **nœud/site** pour voir toutes les alertes affectant un nœud

spécifique.

6. Pour filtrer les alertes par état, utilisez le menu déroulant situé en haut du tableau.



   - Sélectionnez **toutes les alertes** pour afficher toutes les alertes en cours (alertes actives et désactivées).
   - Sélectionnez **actif** pour afficher uniquement les alertes en cours actives.
   - Sélectionnez **silencieux** pour afficher uniquement les alertes en cours qui ont été réduites au silence.

7. Pour afficher les détails d'une alerte spécifique, sélectionnez l'alerte dans le tableau.

   Une boîte de dialogue de l'alerte s'affiche. Reportez-vous aux instructions d'affichage d'une alerte spécifique.

Informations associées

"Affichage d'une alerte spécifique"

"Neutralisation des notifications d'alerte"

Affichage des alertes résolues

Vous pouvez rechercher et afficher l'historique des alertes qui ont été résolues.

Ce dont vous avez besoin

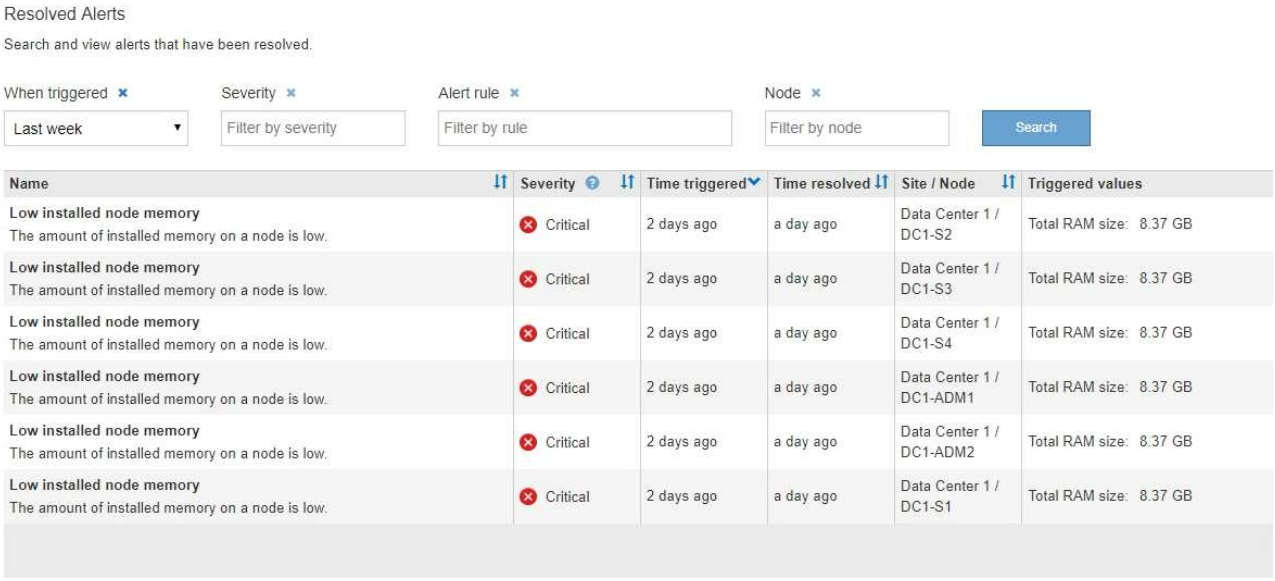
- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.

Étapes

1. Pour afficher les alertes résolues, effectuez l'une des opérations suivantes :
   - Dans le panneau Santé du tableau de bord, cliquez sur **alertes récemment résolues**.

     Le lien **alertes récemment résolues** n'apparaît que si une ou plusieurs alertes ont été déclenchées au cours de la semaine dernière et sont maintenant résolues.

   - Sélectionnez **alertes** > **résolu**. La page alertes résolues s'affiche. Par défaut, les alertes résolues déclenchées au cours de la dernière semaine sont affichées, les alertes déclenchées les plus récemment étant affichées en premier. Les alertes de cette page étaient précédemment affichées sur la page alertes en cours ou dans un e-mail de notification.



2. Vérifiez les informations du tableau.

En-tête de colonne	Description
Nom	Le nom de l'alerte et sa description.
Gravité	Gravité de l'alerte. • **Critique** : Il existe une condition anormale qui a arrêté les opérations normales d'un nœud ou service StorageGRID. Vous devez immédiatement résoudre le problème sous-jacent. Une interruption du service et une perte de données peuvent se produire si le problème n'est pas résolu. • **Majeur** : Il existe une condition anormale affectant les opérations en cours ou approchant le seuil d'une alerte critique. Vous devez examiner les alertes majeures et résoudre tous les problèmes sous-jacents pour vérifier que leur condition anormale n'arrête pas le fonctionnement normal d'un nœud ou d'un service StorageGRID. • **Mineur** : Le système fonctionne normalement, mais il existe une condition anormale qui pourrait affecter la capacité du système à fonctionner s'il continue. Vous devez surveiller et résoudre les alertes mineures qui ne sont pas claires par elles-mêmes pour vous assurer qu'elles n'entraînent pas un problème plus grave.
Temps déclenché	Il y a combien de temps l'alerte a été déclenchée.

En-tête de colonne	Description
Heure de résolution	Il y a combien de temps l'alerte a été résolue.
Site/nœud	Nom du site et du nœud sur lequel l'alerte s'est produite.
Valeurs déclenchées	Valeur de la mesure à l'origine du déclenchement de l'alerte. Pour certaines alertes, des valeurs supplémentaires sont affichées pour vous aider à comprendre et à examiner l'alerte. Par exemple, les valeurs affichées pour une alerte **stockage de données d'objet bas** comprennent le pourcentage d'espace disque utilisé, la quantité totale d'espace disque et la quantité d'espace disque utilisée.

3. Pour trier la liste complète des alertes résolues, cliquez sur les flèches haut/bas ⇅ dans chaque en-tête de colonne.

   Par exemple, vous pouvez trier les alertes résolues par **site/nœud** pour voir les alertes qui ont affecté un nœud spécifique.

4. Vous pouvez également filtrer la liste des alertes résolues à l'aide des menus déroulants situés en haut du tableau.
   a. Sélectionnez une période dans le menu déroulant **déclenché** pour afficher les alertes résolues en fonction de la durée de déclenchement.

      Vous pouvez rechercher des alertes qui ont été déclenchées dans les périodes suivantes :

      - Dernière heure
      - Dernier jour
      - Dernière semaine (vue par défaut)
      - Le mois dernier
      - Tout temps
      - Personnalisé (vous permet de spécifier la date de début et la date de fin de la période)

   b. Sélectionnez un ou plusieurs niveaux de gravité dans le menu déroulant **gravité** pour filtrer les alertes résolues d'une gravité spécifique.
   c. Sélectionnez une ou plusieurs règles d'alerte par défaut ou personnalisées dans le menu déroulant **règle d'alerte** pour filtrer les alertes résolues associées à une règle d'alerte spécifique.
   d. Sélectionnez un ou plusieurs nœuds dans le menu déroulant **Node** pour filtrer les alertes résolues liées à un nœud spécifique.
   e. Cliquez sur **Rechercher**.
5. Pour afficher les détails d'une alerte résolue spécifique, sélectionnez l'alerte dans le tableau.

   Une boîte de dialogue de l'alerte s'affiche. Reportez-vous aux instructions d'affichage d'une alerte spécifique.

Informations associées

"Affichage d'une alerte spécifique"

Affichage d'une alerte spécifique

Vous pouvez afficher des informations détaillées sur une alerte qui affecte actuellement votre système StorageGRID ou une alerte qui a été résolue. Ces informations incluent les actions correctives recommandées, l'heure à laquelle l'alerte a été déclenchée et la valeur actuelle des mesures associées à cette alerte. Vous pouvez éventuellement désactiver une alerte en cours ou mettre à jour la règle d'alerte.

Ce dont vous avez besoin

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

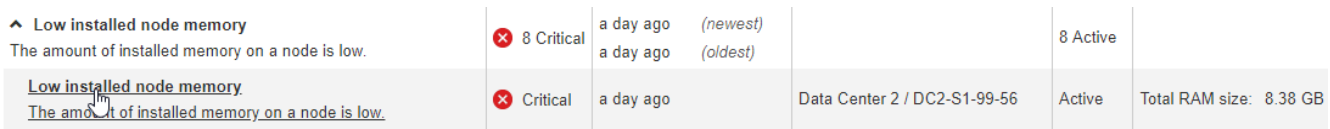
Étapes

1. Effectuez l'une des opérations suivantes, selon que vous souhaitez afficher une alerte en cours ou résolue :

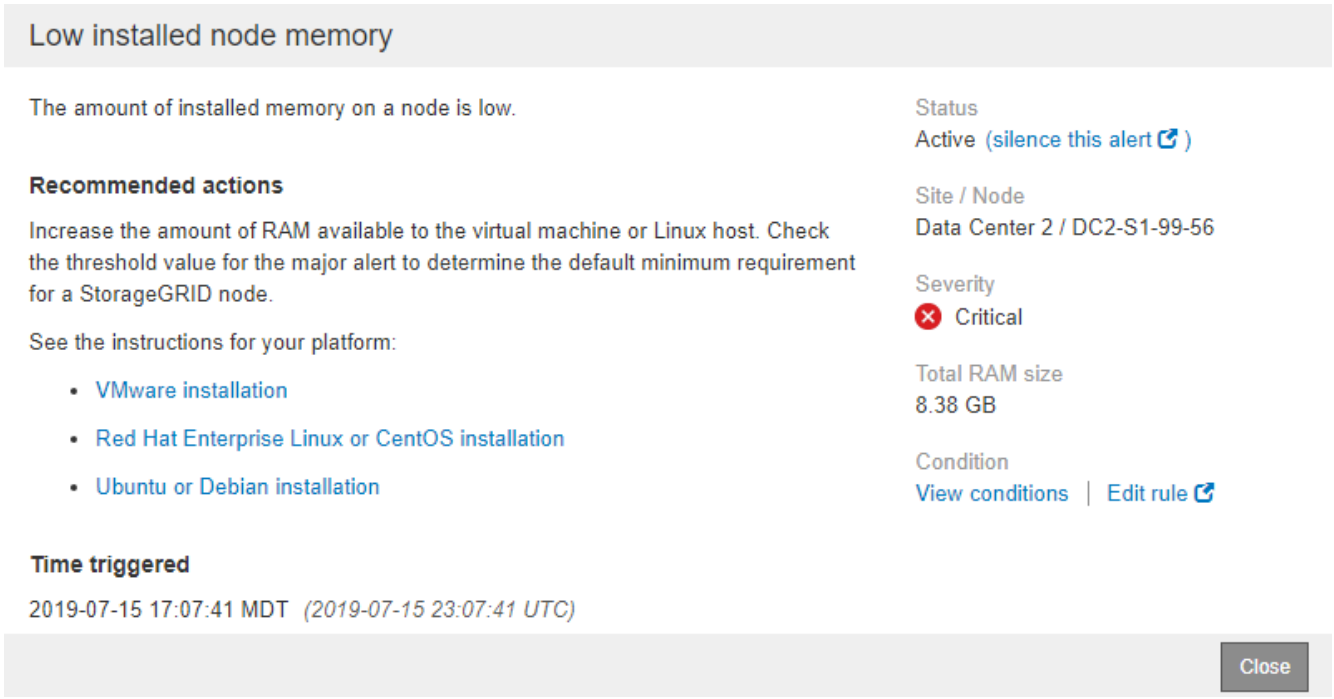
En-tête de colonne	Description
Alerte actuelle	• Dans le panneau Santé du tableau de bord, cliquez sur le lien **alertes actuelles**. Ce lien n'apparaît que si au moins une alerte est active. Ce lien est masqué s'il n'y a pas d'alerte en cours ou si toutes les alertes en cours ont été désactivées. • Sélectionnez **alertes** > **actuel**. • Dans la page **noeuds**, sélectionnez l'onglet **vue d'ensemble** pour un noeud doté d'une icône d'alerte. Cliquez ensuite sur le nom de l'alerte dans la section alertes.
Alerte résolue	• Dans le panneau Santé du tableau de bord, cliquez sur le lien **alertes récemment résolues**. (Ce lien apparaît uniquement si une ou plusieurs alertes ont été déclenchées au cours de la semaine passée et sont maintenant résolues. Ce lien est masqué si aucune alerte n'a été déclenchée et résolue au cours de la semaine dernière.) • Sélectionnez **alertes** > **résolu**.

2. Si nécessaire, développez un groupe d'alertes, puis sélectionnez l'alerte que vous souhaitez afficher.

Sélectionnez l'alerte, et non l'en-tête d'un groupe d'alertes.



Une boîte de dialogue s'affiche et fournit des détails sur l'alerte sélectionnée.



3. Vérifiez les détails de l'alerte.

Informations	Description
titre	Nom de l'alerte.
premier paragraphe	Description de l'alerte.
Actions recommandées	Actions recommandées pour cette alerte.
Temps déclenché	Date et heure de déclenchement de l'alerte à l'heure locale et à l'heure UTC.
Heure de résolution	Pour les alertes résolues uniquement, la date et l'heure auxquelles l'alerte a été résolue dans votre heure locale et dans UTC.
État	État de l'alerte : actif, silencieux ou résolu.
Site/nœud	Nom du site et du nœud affectés par l'alerte.

Informations	Description
Gravité	Gravité de l'alerte. • **Critique** : Il existe une condition anormale qui a arrêté les opérations normales d'un nœud ou service StorageGRID. Vous devez immédiatement résoudre le problème sous-jacent. Une interruption du service et une perte de données peuvent se produire si le problème n'est pas résolu. • **Majeur** : Il existe une condition anormale affectant les opérations en cours ou approchant le seuil d'une alerte critique. Vous devez examiner les alertes majeures et résoudre tous les problèmes sous-jacents pour vérifier que leur condition anormale n'arrête pas le fonctionnement normal d'un nœud ou d'un service StorageGRID. • **Mineur** : Le système fonctionne normalement, mais il existe une condition anormale qui pourrait affecter la capacité du système à fonctionner s'il continue. Vous devez surveiller et résoudre les alertes mineures qui ne sont pas claires par elles-mêmes pour vous assurer qu'elles n'entraînent pas un problème plus grave.
valeurs de données	Valeur actuelle de la mesure pour cette 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 **stockage de métadonnées faible** incluent le pourcentage d'espace disque utilisé, la quantité totale d'espace disque et la quantité d'espace disque utilisée.

4. Vous pouvez également cliquer sur **neutraliser cette alerte** pour désactiver la règle d'alerte qui a déclenché cette alerte.

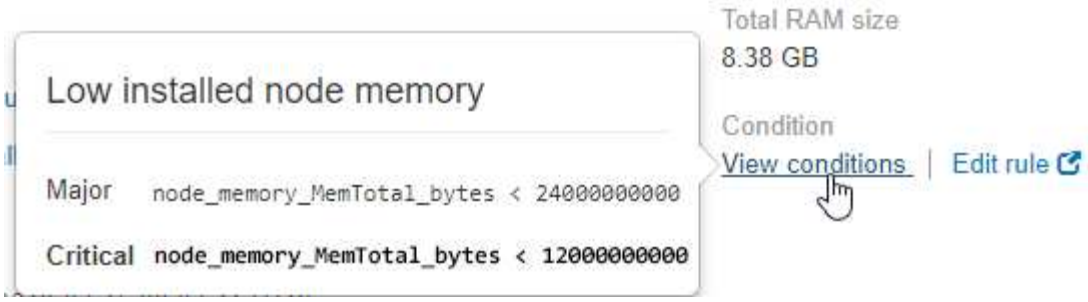
   Vous devez disposer de l'autorisation gérer les alertes ou l'accès racine pour désactiver une règle d'alerte.

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

5. Pour afficher les conditions actuelles de la règle d'alerte :

   a. Dans les détails de l'alerte, cliquez sur **Voir conditions**.

      Une fenêtre contextuelle s'affiche, répertoriant l'expression Prometheus pour chaque gravité définie.



a. Pour fermer la fenêtre contextuelle, cliquez n'importe où en dehors de la fenêtre contextuelle.

6. Si vous le souhaitez, cliquez sur **Modifier la règle** pour modifier la règle d'alerte qui a déclenché cette alerte :

   Vous devez disposer de l'autorisation gérer les alertes ou l'accès racine pour modifier une règle d'alerte.

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

7. Pour fermer les détails de l'alerte, cliquez sur **Fermer**.

Informations associées

"Neutralisation des notifications d'alerte"

"Modification d'une règle d'alerte"

Affichage des anciennes alarmes

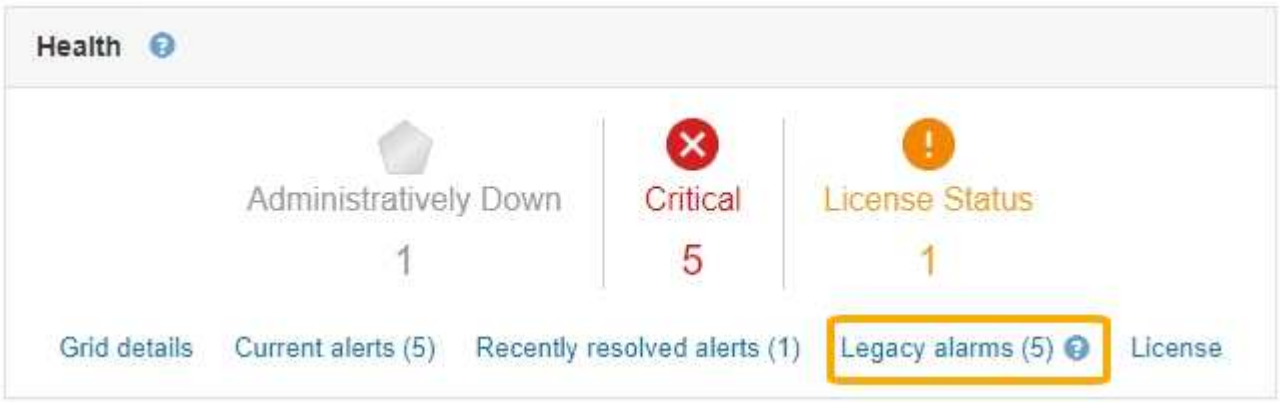
Les alarmes (système hérité) sont déclenchées lorsque les attributs système atteignent les valeurs de seuil d'alarme. Vous pouvez afficher les alarmes actives à partir du tableau de bord ou de la page alarmes en cours.

Ce dont vous avez besoin

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

Description de la tâche

Si une ou plusieurs des alarmes héritées sont actuellement actives, le panneau Santé du tableau de bord inclut un lien **Legacy Alarms**. Le nombre entre parenthèses indique le nombre d'alarmes actuellement actives.



Le nombre d'alarmes * héritées* sur le tableau de bord est incrémenté chaque fois qu'une alarme héritée est déclenchée. Ce nombre est incrémenté même si vous avez désactivé les notifications par e-mail d'alarme. Vous pouvez généralement ignorer ce numéro (puisque les alertes offrent une meilleure vue du système) ou afficher les alarmes actives.

Bien que le système d'alarme existant continue d'être pris en charge, le système d'alerte offre des avantages significatifs et est plus facile à utiliser.

Étapes

1. Pour afficher les anciennes alarmes actuellement actives, effectuez l'une des opérations suivantes :
   - Dans le panneau Santé du tableau de bord, cliquez sur **Legacy alarmes**. Ce lien n'apparaît que si au moins une alarme est active.
   - Sélectionnez **support** > **alarmes (hérité)** > **alarmes actuelles**. La page alarmes en cours s'affiche.

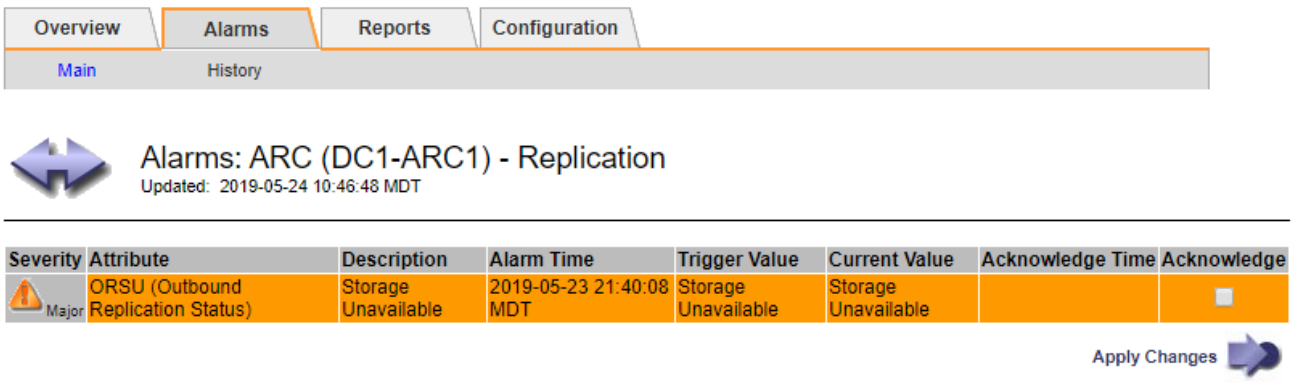
L'icône d'alarme indique la gravité de chaque alarme, comme suit :

Icône	Couleur	Gravité de l'alarme	Signification
	Jaune	Avertissement	Le nœud est connecté à la grille, mais il existe une condition inhabituelle qui n'affecte pas les opérations normales.
	Orange clair	Mineur	Le nœud est connecté à la grille, mais il existe une condition anormale qui pourrait affecter son fonctionnement à l'avenir. Vous devez étudier pour éviter la remontée des problèmes.

Icône	Couleur	Gravité de l'alarme	Signification
	Orange foncé	Majeur	Le nœud est connecté à la grille, mais il existe une condition anormale qui affecte actuellement le fonctionnement. Cela nécessite une attention particulière afin d'éviter la remontée des problèmes.
	Rouge	Primordial	Le nœud est connecté à la grille, mais il existe une condition anormale qui a arrêté des opérations normales. Vous devez résoudre le problème immédiatement.

1. Pour en savoir plus sur l'attribut à l'origine du déclenchement de l'alarme, cliquez avec le bouton droit de la souris sur le nom de l'attribut dans le tableau.
2. Pour afficher des détails supplémentaires sur une alarme, cliquez sur le nom du service dans le tableau.

   L'onglet alarmes du service sélectionné apparaît (**support** > **Outils** > **topologie de grille** > ***Grid Node*** > ***Service*** > **alarmes**).



3. Si vous souhaitez effacer le nombre d'alarmes en cours, vous pouvez, en option, procéder comme suit :
   - Accuser réception de l'alarme. Une alarme acquittée n'est plus incluse dans le nombre d'alarmes héritées à moins qu'elle ne soit déclenchée au niveau de gravité suivant ou qu'elle ne soit résolue et se déclenche à nouveau.
   - Désactivez une alarme par défaut particulière ou une alarme personnalisée globale pour l'ensemble du système afin d'éviter qu'elle ne se déclenche à nouveau.

Informations associées

"Référence des alarmes (système hérité)"

"Confirmation des alarmes actuelles (système hérité)"

"Désactivation des alarmes (système hérité)"

Contrôle de la capacité de stockage

Vous devez contrôler l'espace total disponible sur les nœuds de stockage pour vérifier que l'espace de stockage disponible sur le système StorageGRID n'est pas insuffisant pour les objets ou les métadonnées d'objet.

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

Vous pouvez afficher les informations de capacité de stockage pour l'ensemble de la grille, pour chaque site et pour chaque nœud de stockage de votre système StorageGRID.

Informations associées

"Affichage de l'onglet stockage"

Surveillance de la capacité de stockage pour l'ensemble de la grille

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

Ce dont vous avez besoin

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

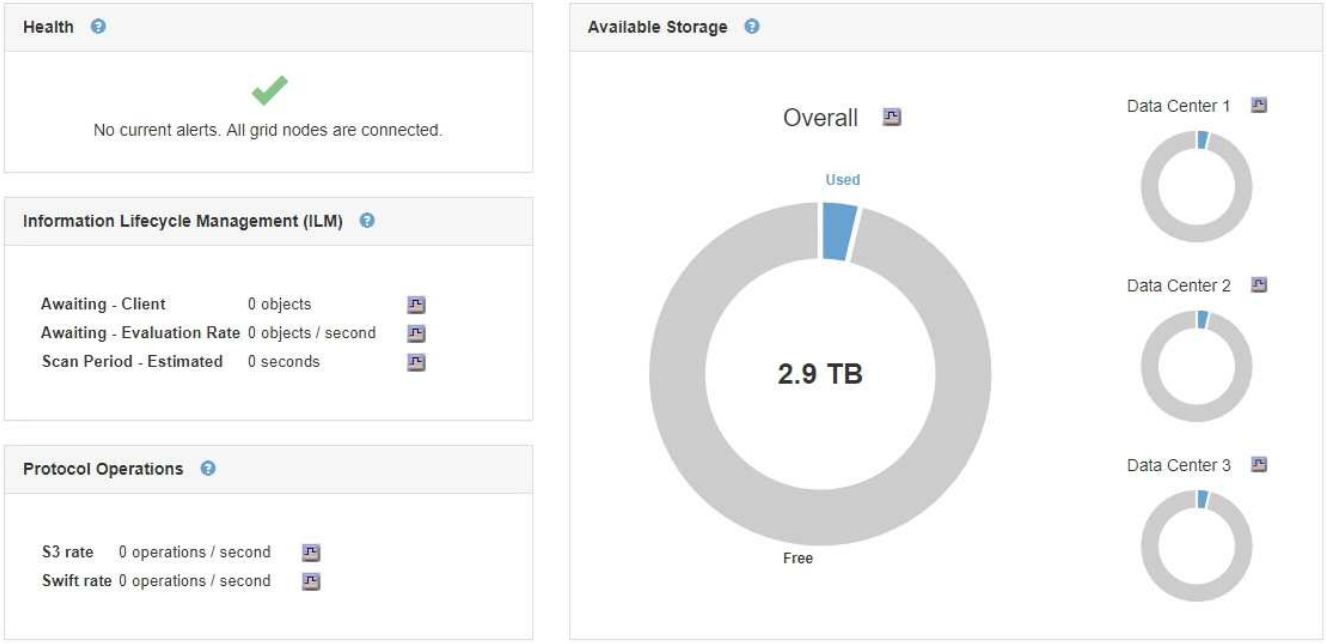
Description de la tâche

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

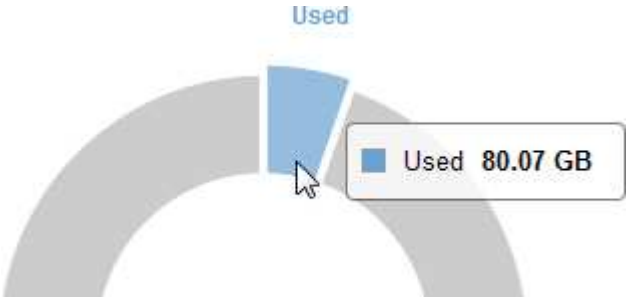
Étapes

1. Évaluez la quantité de stockage disponible pour l'ensemble du grid et pour chaque data Center.
   a. Sélectionnez **Tableau de bord**.
   b. Dans le panneau stockage disponible, notez le récapitulatif général de la capacité de stockage disponible et utilisée.

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



a. Placez votre curseur sur les sections capacité libre ou utilisée du graphique pour voir exactement la quantité d'espace libre ou utilisé.



b. Pour les grilles multisites, consultez le tableau de chaque data Center.

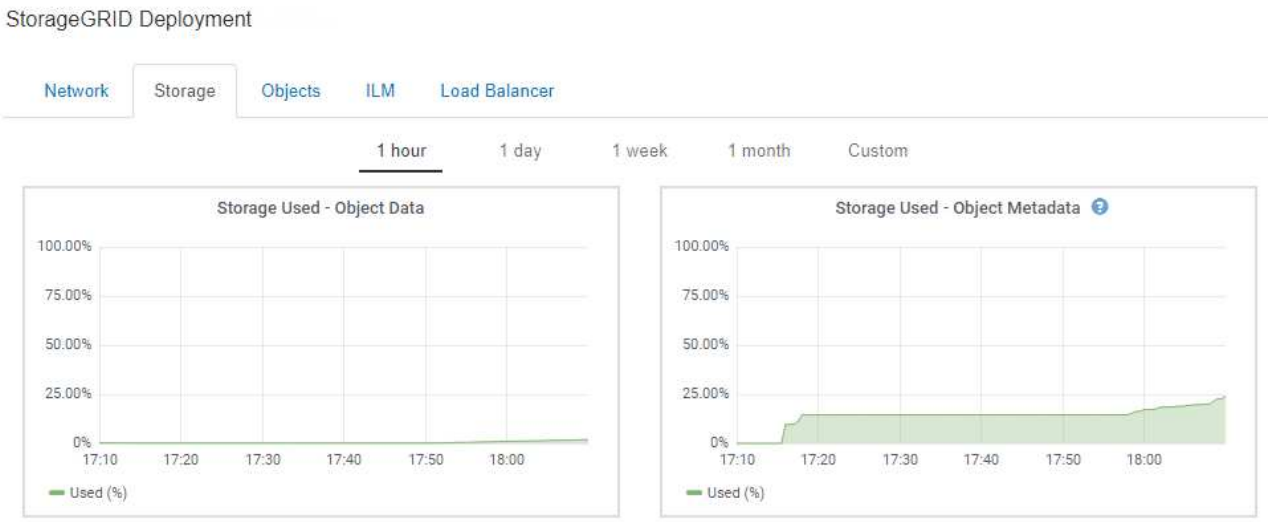
c. Cliquez sur l'icône du graphique pour le graphique global ou pour un centre de données individuel, afficher un graphique indiquant l'utilisation de la capacité dans le temps.

   Graphique montrant un pourcentage de capacité de stockage utilisée (%) par rapport L'heure s'affiche.

2. Déterminez la quantité de stockage utilisée et la quantité de stockage disponible pour les données d'objet et les métadonnées d'objet.

   a. Sélectionnez **noeuds**.

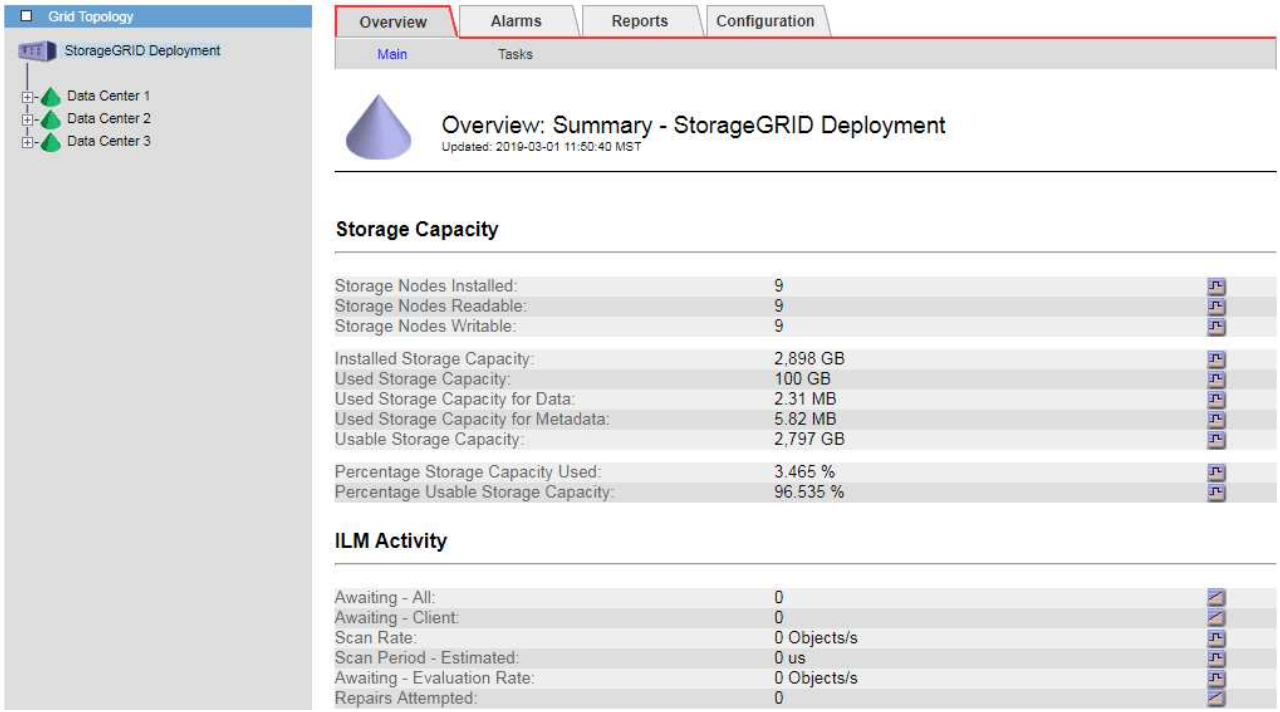
   b. Sélectionnez ***GRID*** > **stockage**.



c. Placez le curseur de la souris sur le champ stockage utilisé - données d'objet et diagrammes de métadonnées de l'objet utilisé pour connaître la quantité de stockage de métadonnées d'objet et du stockage de métadonnées disponible pour l'ensemble de la grille, ainsi que la quantité utilisée au fil du temps.

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

3. Comme indiqué par le support technique, consultez les informations supplémentaires sur la capacité de stockage de votre grid.
   a. Sélectionnez **support** > **Outils** > **topologie de grille**.
   b. Sélectionnez ***GRID*** > **Présentation** > **main**.



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

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

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

Pour plus d'informations sur la planification d'une extension du stockage, consultez les instructions d'extension d'StorageGRID.

Informations associées

"Développez votre grille"

Contrôle de la capacité de stockage pour chaque nœud de stockage

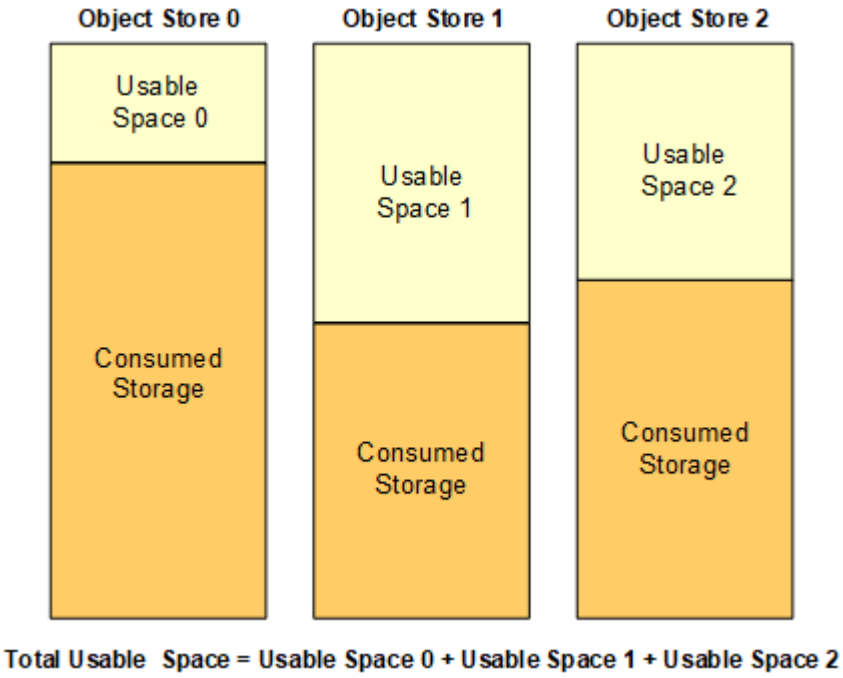
Vous devez contrôler l'espace total utilisable pour chaque nœud de stockage pour vous assurer que le nœud dispose d'un espace suffisant pour les nouvelles données d'objet.

Ce dont vous avez besoin

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

Description de la tâche

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



Étapes

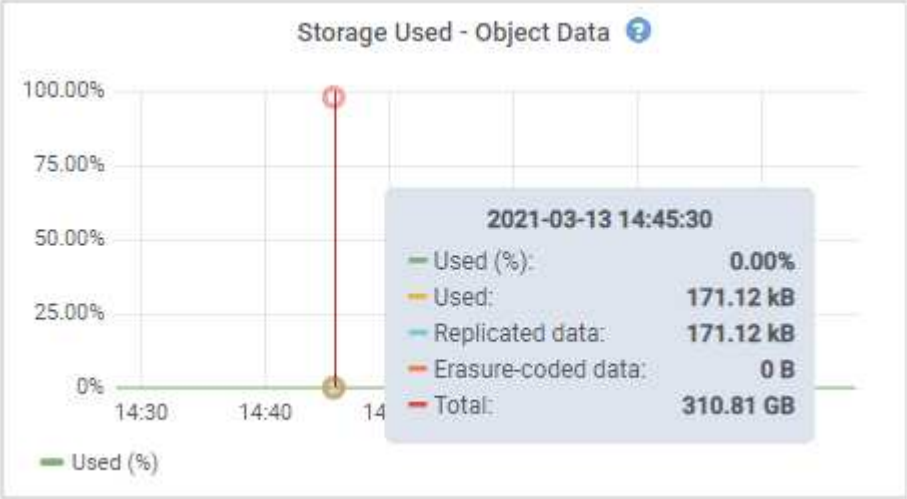
1. Sélectionnez **Nodes** > ***Storage Node*** > **Storage**.

   Les graphiques et les tableaux du nœud apparaissent.

2. Placez le curseur de la souris sur le graphique stockage utilisé - données d'objet.

   Les valeurs suivantes sont affichées :

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



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

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

Disk Devices

Name	World Wide Name	I/O Load	Read Rate	Write Rate
croot(8:1,sda1)	N/A	0.03%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.85%	0 bytes/s	58 KB/s
sdc(8:16,sdb)	N/A	0.00%	0 bytes/s	81 bytes/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	14.90 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.10 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.18 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	96.45 GB	250.90 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 dans le temps pour estimer le taux de consommation de l'espace de stockage utilisable.
5. Pour préserver le fonctionnement normal du système, ajoutez des nœuds de stockage, ajoutez des volumes de stockage ou archivez les données d'objet avant de consommer l'espace utilisable.

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

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

   Pour plus d'informations sur la planification d'une extension du stockage, consultez les instructions d'extension d'StorageGRID.

   L'alerte **stockage de données d'objet bas** et l'alarme État de stockage hérité (SSTS) sont déclenchées lorsque l'espace restant insuffisant pour stocker des données d'objet sur un noeud de stockage.

Informations associées

"Administrer StorageGRID"

"Dépannage de l'alerte de stockage de données d'objet faible"

"Développez votre grille"

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

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

Ce dont vous avez besoin

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

Description de la tâche

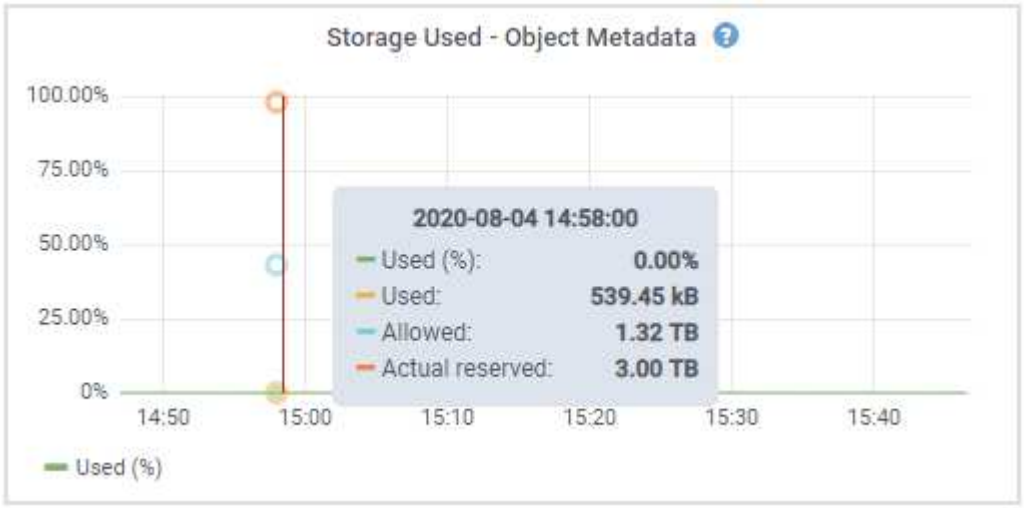
StorageGRID conserve trois copies des métadonnées d'objet sur chaque site pour assurer la redondance et protéger les métadonnées d'objet contre la perte. Les trois copies sont réparties de manière homogène sur tous les nœuds de stockage de chaque site, en utilisant l'espace réservé aux métadonnées sur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

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

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

Étapes

1. Sélectionnez **Nodes** > ***Storage Node*** > **Storage**.
2. Placez le curseur de la souris sur le graphique Storage Used - Object Metadata pour afficher les valeurs d'une heure spécifique.



Valeur	Description	Metrics Prometheus
Utilisé (%)	Pourcentage de l'espace de métadonnées autorisé utilisé sur ce nœud de stockage.	`storagegrid_storage_utilization_metadata_bytes/ storagegrid_storage_utilization_metadata_allowed_bytes`
Utilisé	Les octets de l'espace de métadonnées autorisé qui ont été utilisés sur ce nœud de stockage.	`storagegrid_storage_utilization_metadata_bytes`
Autorisé	Espace autorisé pour les métadonnées d'objet sur ce nœud de stockage. Pour savoir comment cette valeur est définie pour chaque nœud de stockage, reportez-vous aux instructions d'administration de StorageGRID.	`storagegrid_storage_utilization_metadata_allowed_bytes`
Réservé réelle	Espace réel réservé aux métadonnées sur ce nœud de stockage. Inclut l'espace autorisé et l'espace requis pour les opérations essentielles sur les métadonnées. Pour savoir comment cette valeur est calculée pour chaque nœud de stockage, reportez-vous aux instructions d'administration de StorageGRID.	`storagegrid_storage_utilization_metadata_reserved_bytes`

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

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

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

Lorsque vous ajoutez des nœuds, le système rééquilibre automatiquement les métadonnées d'objet sur tous les nœuds de stockage du site. Voir les instructions d'extension d'un système StorageGRID.

Informations associées

"Dépannage de l'alerte de stockage de métadonnées faible"

"Administrer StorageGRID"

"Développez votre grille"

Contrôle de la gestion du cycle de vie des informations

Le système de gestion du cycle de vie des informations (ILM) assure la gestion des données de tous les objets stockés sur la grille. Vous devez surveiller les opérations ILM pour déterminer si la grille peut traiter la charge actuelle ou si d'autres ressources sont requises.

Ce dont vous avez besoin

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

Description de la tâche

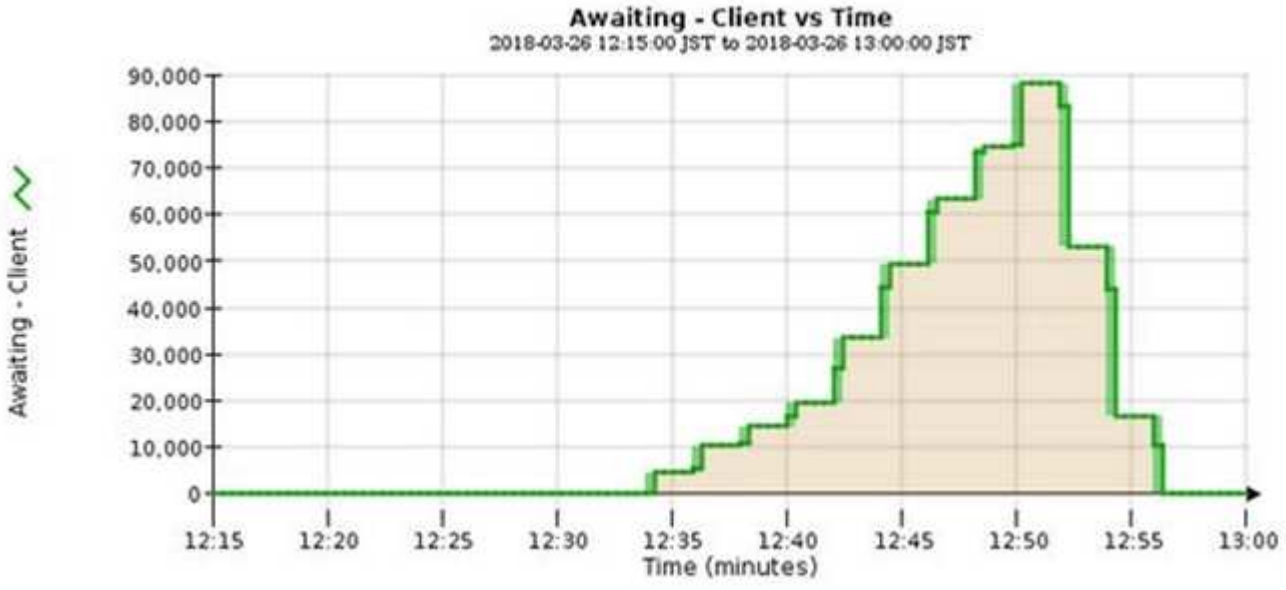
Le système StorageGRID gère les objets en appliquant la règle ILM active. La politique ILM et les règles ILM associées déterminent le nombre de copies, le type de copies créées, le lieu où les copies sont placées, ainsi que la durée de conservation de chaque copie.

L'ingestion d'objets et d'autres activités liées aux objets peuvent dépasser le taux d'évaluation de la ILM par StorageGRID. Le système file d'attente des objets dont les instructions de placement ILM ne peuvent pas être exécutées en temps quasi réel. Vous pouvez contrôler si StorageGRID maintient les actions du client en transcritant l'attribut attente - client.

Pour tracer cet attribut :

1. Connectez-vous au Grid Manager.
2. Dans le tableau de bord, recherchez l'entrée **attente - client** dans le panneau gestion du cycle de vie des informations (ILM).
3. Cliquez sur l'icône du graphique .

Le graphique illustre une situation dans laquelle le nombre d'objets en attente d'évaluation ILM a temporairement augmenté de façon non viable, puis a finalement diminué. Une telle tendance indique que la gestion du cycle de vie des informations (ILM) n'a été temporairement pas respectée en temps réel.



Des pics temporaires dans le graphique d'attente - client doivent être attendus. Si la valeur affichée sur le graphique continue d'augmenter et ne diminue jamais, la grille nécessite davantage de ressources pour fonctionner efficacement : plus de nœuds de stockage ou, si la règle ILM place les objets à distance, plus de

bande passante réseau.

Vous pouvez approfondir l'analyse des files d'attente ILM à l'aide de la page **Nodes**.

Étapes

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

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

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

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

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

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

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

Surveillance des performances, de la mise en réseau et des ressources système

Vous devez surveiller les performances, la mise en réseau et les ressources système pour déterminer si StorageGRID peut gérer sa charge actuelle et s'assurer que les performances des clients ne se dégradent pas au fil du temps.

Contrôle de la latence des requêtes

Les actions client, telles que le stockage, la récupération ou la suppression d'objets, créent des requêtes vers la base de données distribuée de métadonnées d'objet de la

grille. Vous devez surveiller les tendances de la latence des requêtes pour vous assurer que les ressources de la grille sont adaptées à la charge actuelle.

Ce dont vous avez besoin

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

Description de la tâche

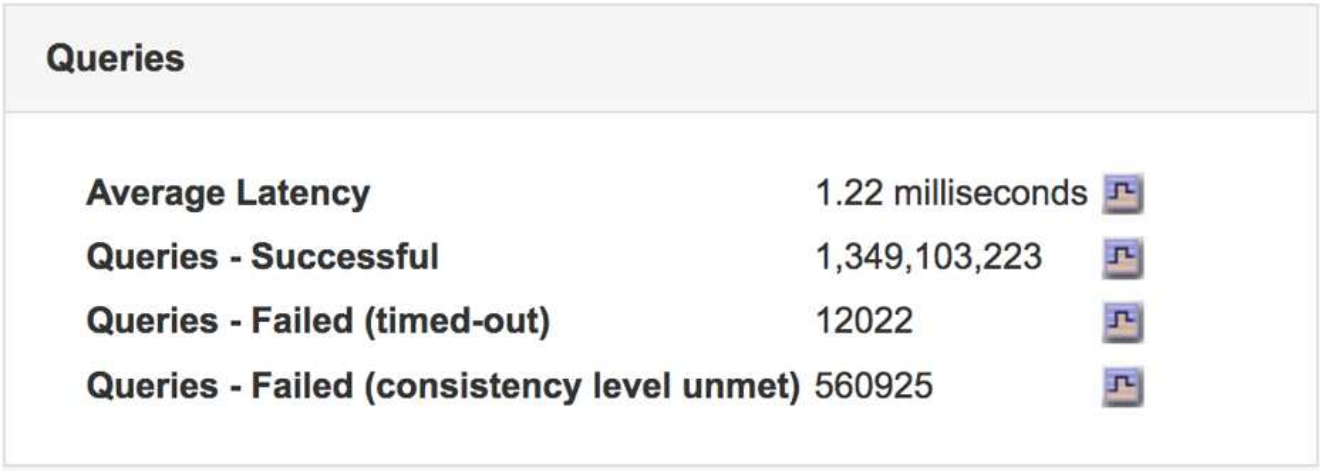
Les augmentations temporaires de la latence des requêtes sont normales et peuvent être dues à une augmentation soudaine des demandes d'entrée. Les requêtes en échec sont également normales et peuvent entraîner des problèmes de réseau transitoire ou des nœuds temporairement non disponibles. Cependant, si le temps moyen d'exécution d'une requête augmente, les performances globales de la grille diminuent.

Si vous remarquez que la latence des requêtes augmente au fil du temps, il est recommandé d'ajouter des nœuds de stockage supplémentaires dans une procédure d'extension afin de répondre aux futures charges de travail.

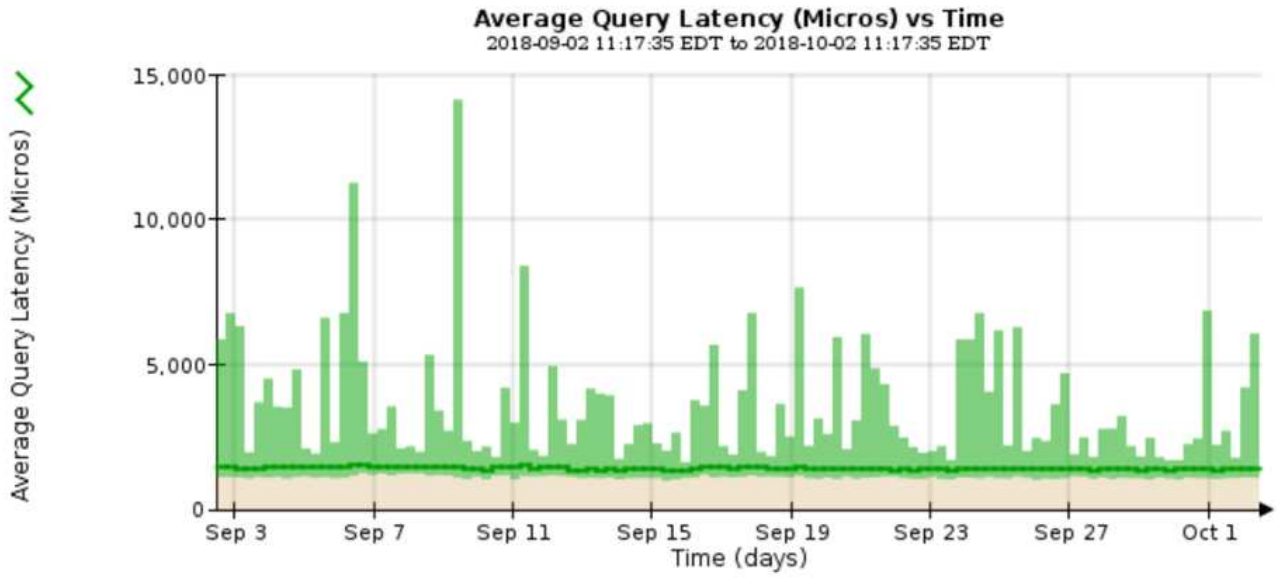
L'alerte **latence élevée pour les requêtes de métadonnées** est déclenchée si la durée moyenne des requêtes est trop longue.

Étapes

1. Sélectionnez **Nodes** > ***Storage Node*** > **objets**.
2. Faites défiler jusqu'au tableau requêtes et affichez la valeur de latence moyenne.



3. Cliquez sur l'icône du graphique pour tracer la valeur dans le temps.



L'exemple de graphique montre les pics de latence d'une requête pendant le fonctionnement normal de la grille.

Informations associées

"Développez votre grille"

Contrôle des connexions réseau et des performances

Les nœuds de la grille doivent pouvoir communiquer les uns avec les autres pour permettre le fonctionnement de la grille. L'intégrité du réseau entre les nœuds et les sites, et la bande passante réseau entre les sites, sont essentielles à l'efficacité des opérations.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

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

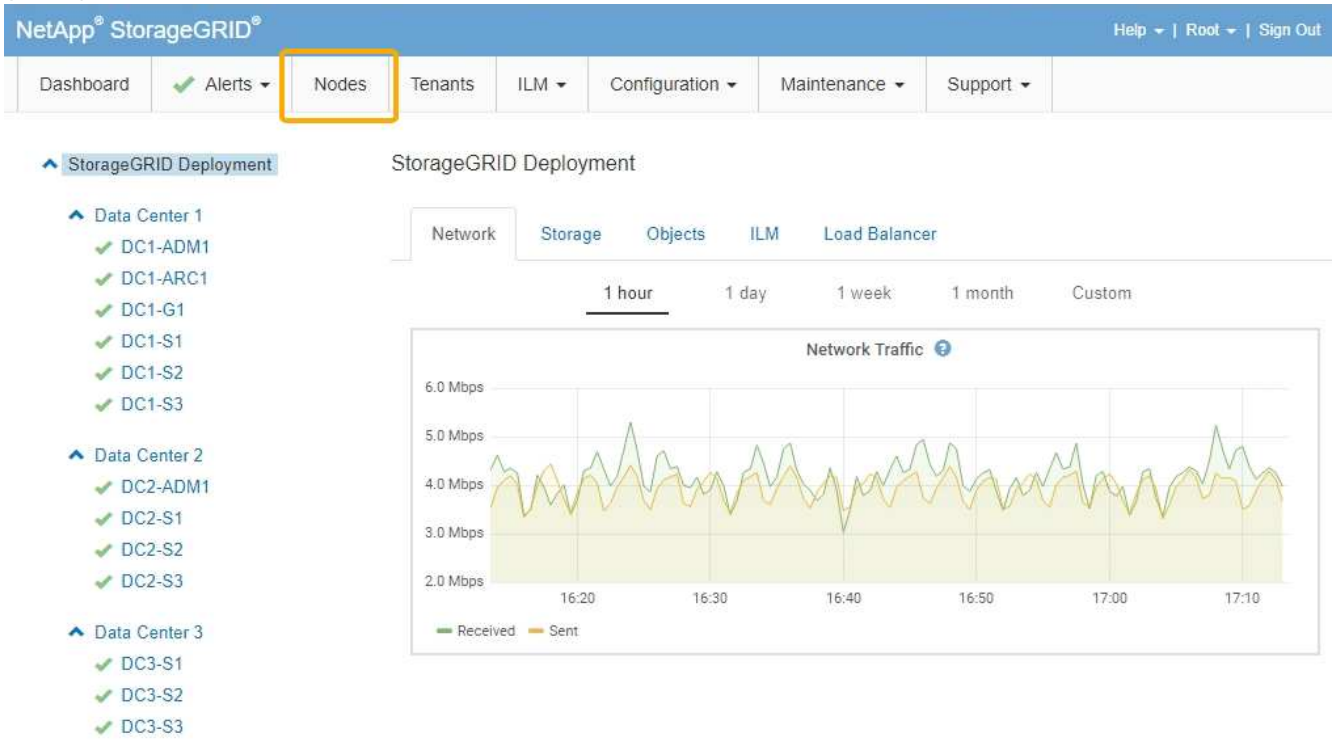
Grid Manager surveille la connectivité et les performances du réseau afin de résoudre tous les problèmes rapidement.

Envisagez également de créer des règles de classification du trafic réseau pour fournir des fonctionnalités de surveillance et de limitation du trafic lié à des locataires, des compartiments, des sous-réseaux ou des terminaux d'équilibrage de la charge spécifiques. Voir les instructions d'administration de StorageGRID.

Étapes

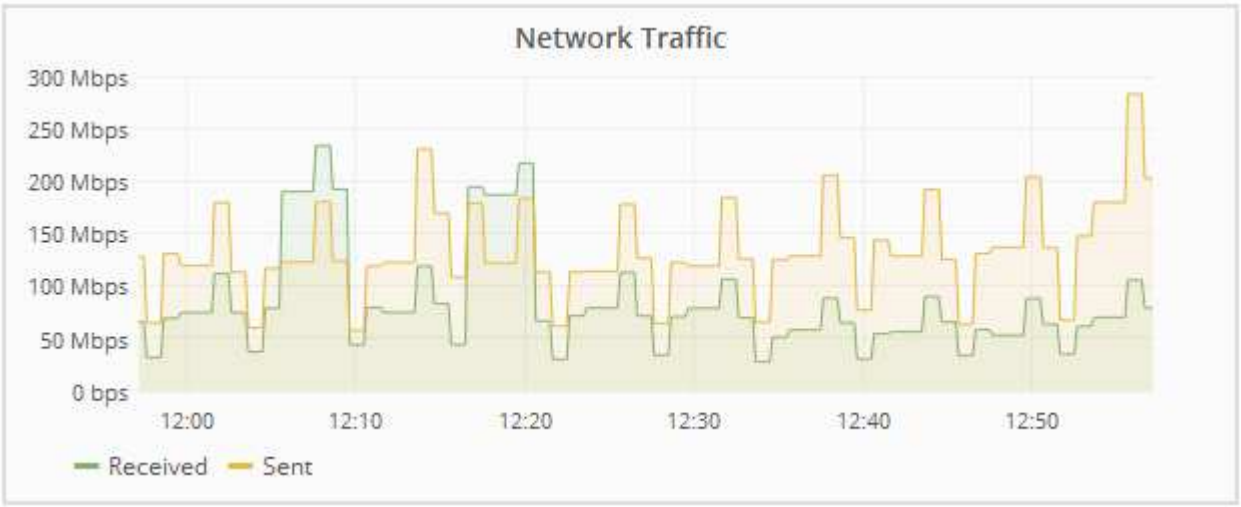
1. Sélectionnez **noeuds**.

La page nœuds s'affiche. Les icônes de nœud indiquent en un coup d'œil quels nœuds sont connectés (icône de coche verte) et quels nœuds sont déconnectés (icônes bleues ou grises).



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

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



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

Network Interfaces

Name	Hardware Address	Speed	Duplex	Auto Negotiate	Link Status
eth0	50:6B:4B:42:D7:11	100 Gigabit	Full	Off	Up
eth1	D8:C4:97:2A:E4:9E	Gigabit	Full	Off	Up
eth2	50:6B:4B:42:D7:11	100 Gigabit	Full	Off	Up
hic1	50:6B:4B:42:D7:11	25 Gigabit	Full	Off	Up
hic2	50:6B:4B:42:D7:11	25 Gigabit	Full	Off	Up
hic3	50:6B:4B:42:D7:11	25 Gigabit	Full	Off	Up
hic4	50:6B:4B:42:D7:11	25 Gigabit	Full	Off	Up
mtc1	D8:C4:97:2A:E4:9E	Gigabit	Full	On	Up
mtc2	D8:C4:97:2A:E4:9F	Gigabit	Full	On	Up

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

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

Network Communication

Receive

Interface	Data	Packets	Errors	Dropped	Frame Overruns	Frames
eth0	3.250 TB	5,610,578,144	0	8,327	0	0
eth1	1.205 GB	9,828,095	0	32,049	0	0
eth2	849.829 GB	186,349,407	0	10,269	0	0
hic1	114.864 GB	303,443,393	0	0	0	0
hic2	2.315 TB	5,351,180,956	0	305	0	0
hic3	1.690 TB	1,793,580,230	0	0	0	0
hic4	194.283 GB	331,640,075	0	0	0	0
mtc1	1.205 GB	9,828,096	0	0	0	0
mtc2	1.168 GB	9,564,173	0	32,050	0	0

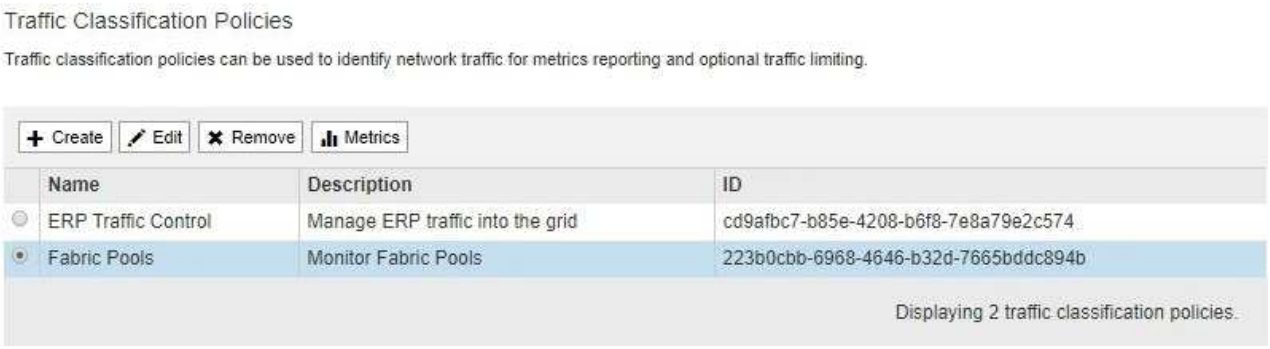
Transmit

Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	5.759 TB	5,789,638,626	0	0	0	0
eth1	4.563 MB	41,520	0	0	0	0
eth2	855.404 GB	139,975,194	0	0	0	0
hic1	289.248 GB	326,321,151	5	0	0	5
hic2	1.636 TB	2,640,416,419	18	0	0	18
hic3	3.219 TB	4,571,516,003	33	0	0	33
hic4	1.687 TB	1,658,180,262	22	0	0	22
mtc1	4.563 MB	41,520	0	0	0	0
mtc2	49.678 KB	609	0	0	0	0

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

   a. Sélectionnez **Configuration** > **Paramètres réseau** > **Classification du trafic**.

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



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

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

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

Pour créer, modifier ou supprimer des stratégies de classification de trafic, reportez-vous aux instructions d'administration de StorageGRID.

Informations associées

"Affichage de l'onglet réseau"

"Contrôle de l'état de connexion du nœud"

"Administrer StorageGRID"

Contrôle des ressources au niveau des nœuds

Vous devez surveiller chaque nœud de la grille pour vérifier ses niveaux d'utilisation des ressources.

Ce dont vous avez besoin

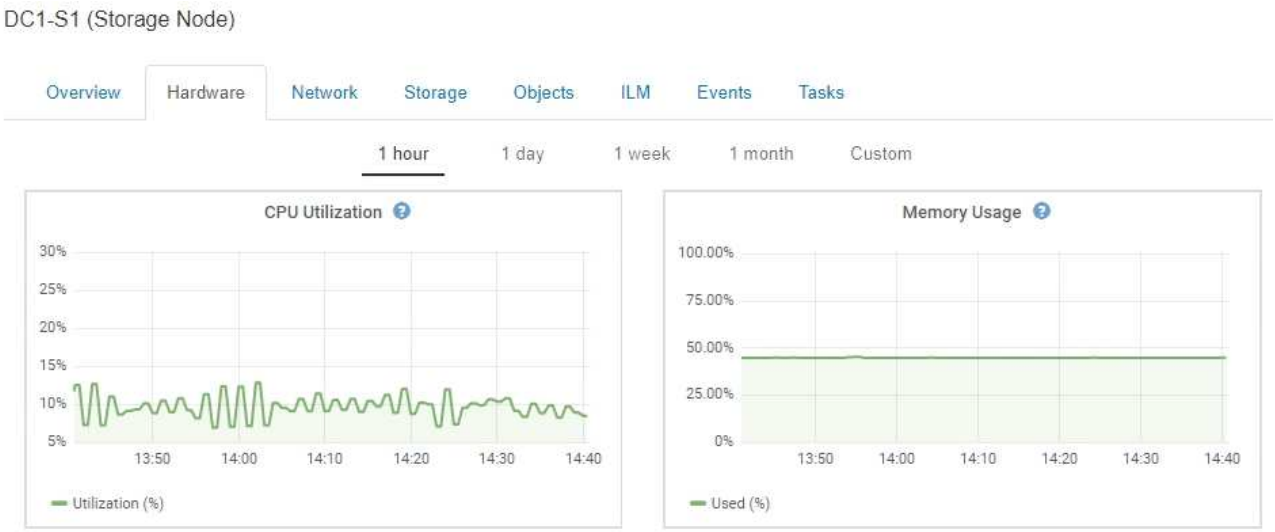
- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.

Description de la tâche

Si les nœuds sont constamment surchargés, un nombre plus élevé de nœuds peut être requis pour une efficacité optimale des opérations.

Étapes

1. Pour afficher des informations sur l'utilisation matérielle d'un nœud de grid :
   a. Dans la page **noeuds**, sélectionnez le noeud.
   b. Sélectionnez l'onglet **matériel** pour afficher les graphiques de l'utilisation de l'UC et de la mémoire.



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

d. Si le nœud est hébergé sur une appliance de stockage ou sur une appliance de services, faites défiler la page vers le bas pour afficher les tableaux des composants. L'état de tous les composants doit être « nominal ». Rechercher les composants ayant un autre état.

Informations associées

"Affichage des informations sur les nœuds de stockage de l'appliance"

"Affichage des informations sur les nœuds d'administration de l'appliance et les nœuds de passerelle"

Contrôle de l'activité des locataires

Toute l'activité client est associée à un compte de locataire. Vous pouvez utiliser Grid Manager pour surveiller l'utilisation du stockage ou du trafic réseau d'un locataire, ou encore utiliser le journal d'audit ou les tableaux de bord Grafana pour obtenir des informations plus détaillées sur l'utilisation de StorageGRID par les locataires.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer de l'autorisation accès racine ou Administrateur.

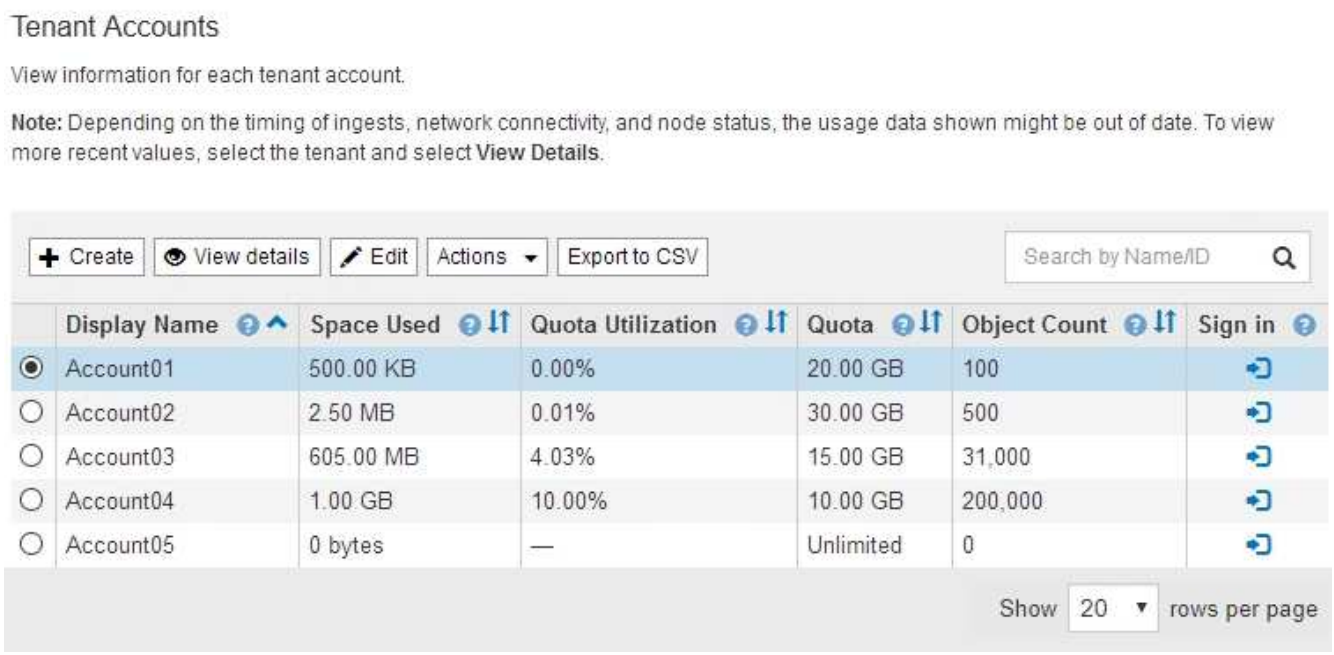
Description de la tâche

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

Étapes

1. Sélectionnez **locataires** pour examiner la quantité de stockage utilisée par tous les locataires.

   Les champs espace utilisé, quota Utilization, quota et Object Count sont répertoriés pour chaque locataire. Si un quota n'est pas défini pour un locataire, le champ quota Utilization contient un tiret (--) et le champ quota indique « Unlimited ».



Si votre système comprend plus de 20 éléments, vous pouvez spécifier le nombre de lignes affichées simultanément sur chaque page. Utilisez la zone de recherche pour rechercher un compte de tenant par nom d'affichage ou ID de tenant.

Vous pouvez vous connecter à un compte locataire en sélectionnant le lien dans la colonne **connexion** de la table.

2. Vous pouvez également sélectionner **Exporter au format CSV** pour afficher et exporter un fichier .csv contenant les valeurs d'utilisation de tous les locataires.

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

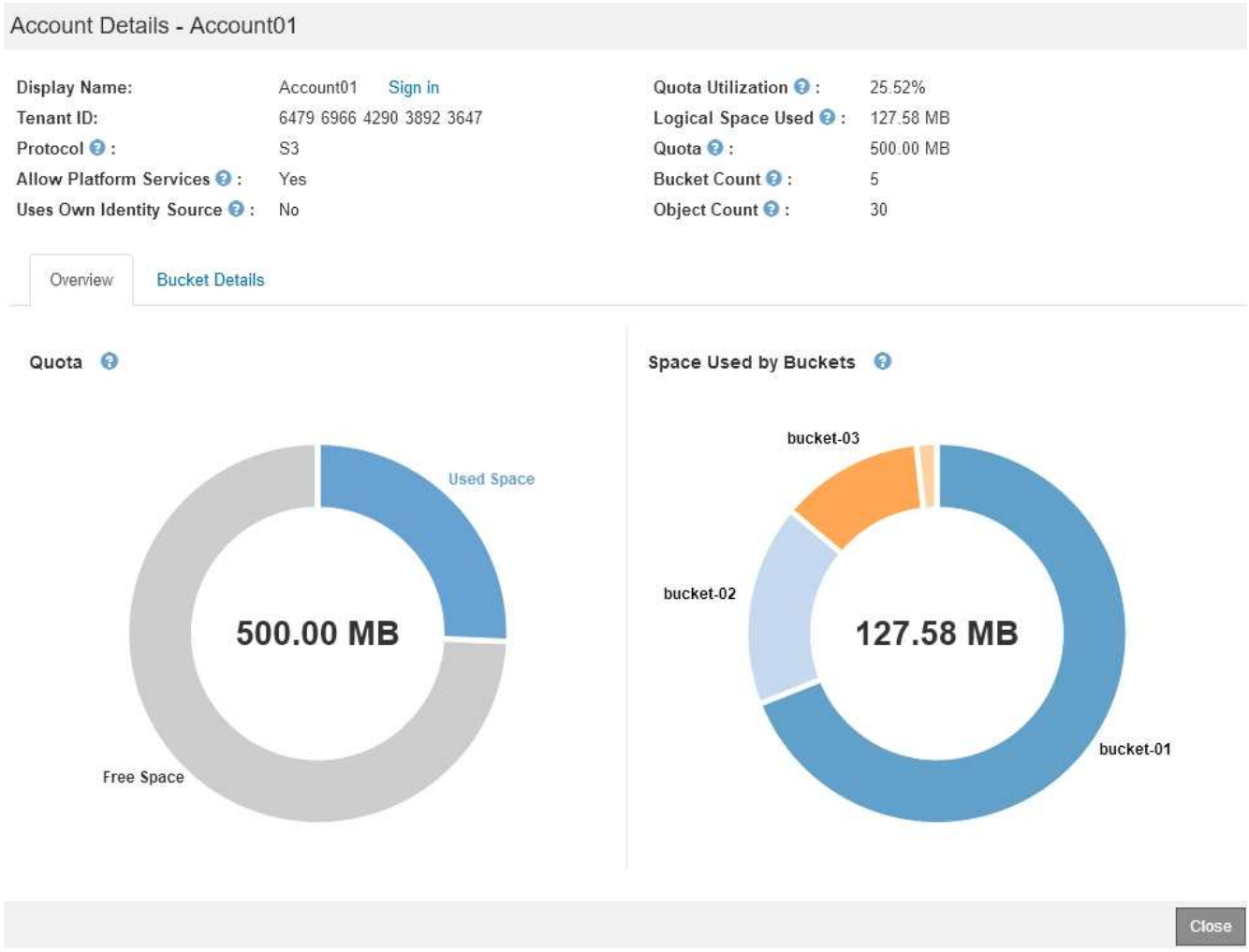
   Le contenu d'un fichier .csv ressemble à l'exemple suivant :

Tenant ID	Display Name	Space Used (Bytes)	Quota utilization (%)	Quota (Bytes)	Object Count	Protocol
56243391454153665591	Account01	500000	0	20000000000	100	S3
82457136581801590515	Account02	2500000	0.01	30000000000	500	S3
04489086912300179118	Account03	605000000	4.03	15000000000	31000	S3
26417581662098345719	Account04	1000000000	10	10000000000	200000	S3
78472447501213318575	Account05	0			0	S3

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

3. Pour afficher les détails d'un locataire spécifique, y compris les graphiques d'utilisation, sélectionnez le compte de tenant dans la page comptes de tenant, puis sélectionnez **Afficher les détails**.

   La page Détails du compte s'affiche et affiche des informations récapitulatives, un tableau représentant la quantité de quota utilisé et restant, ainsi qu'un graphique représentant la quantité de données d'objet dans des compartiments (S3) ou des conteneurs (Swift).



- **Quota**

  Si un quota a été fixé pour ce locataire, le graphique **quota** indique la quantité de ce quota utilisée par ce locataire et la quantité disponible. Si aucun quota n'a été défini, le locataire dispose d'un quota illimité et un message d'information s'affiche. Si le locataire a dépassé le quota de stockage de plus de 1 % et d'au moins 1 Go, le graphique indique le quota total et le montant de l'excès.

  Vous pouvez placer le curseur sur le segment espace utilisé pour afficher le nombre d'objets stockés et le nombre total d'octets utilisés. Vous pouvez placer votre curseur sur le segment espace libre pour voir le nombre d'octets de quota de stockage disponibles.

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

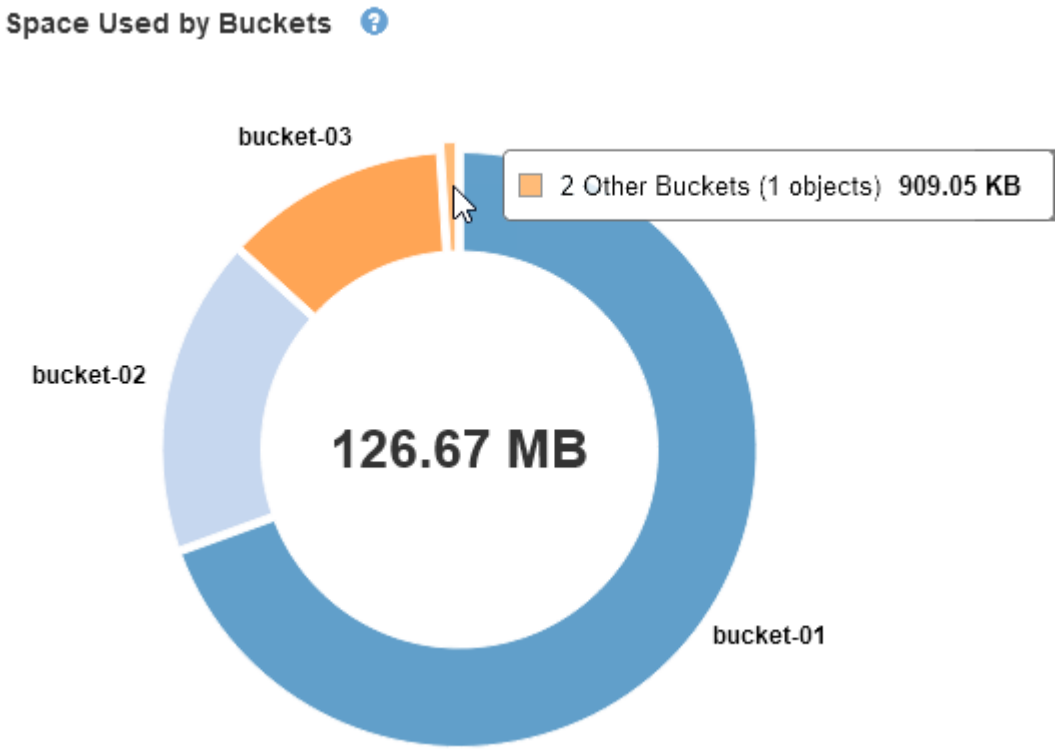
L'utilisation des quotas d'un locataire indique la quantité totale des données d'objet que le locataire a téléchargées sur StorageGRID (taille logique). L'utilisation du quota ne représente pas l'espace utilisé pour stocker les copies de ces objets et de leurs métadonnées (taille physique).

Vous pouvez activer l'alerte **tenant quota usage high** pour déterminer si les locataires consomment leurs quotas. Si elle est activée, cette alerte est déclenchée lorsqu'un locataire a utilisé 90 % de son quota. Pour plus d'informations, reportez-vous à la référence des alertes.

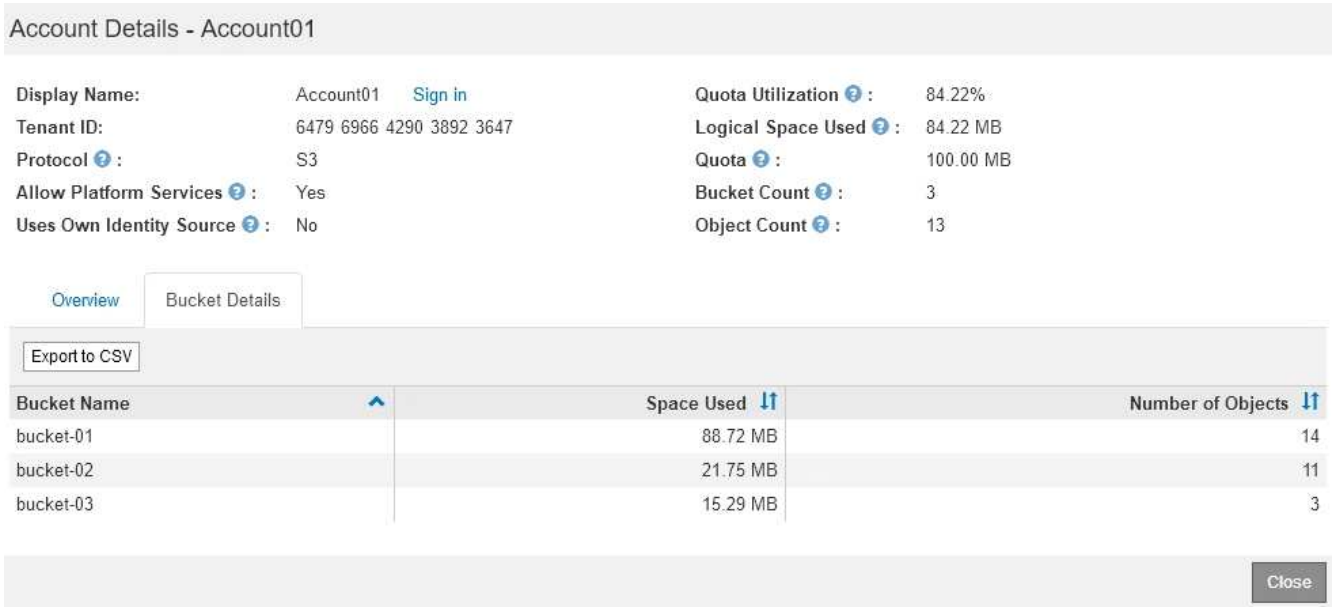
- **Espace utilisé**

  Le graphique **espace utilisé par les compartiments** (S3) ou **espace utilisé par les conteneurs** (Swift) montre les plus grands compartiments pour le locataire. L'espace utilisé correspond à la quantité totale de données d'objet dans le compartiment. Cette valeur ne représente pas l'espace de stockage requis pour les copies ILM et les métadonnées d'objet.

  Si le locataire possède plus de neuf compartiments ou conteneurs, ils sont combinés dans un segment appelé autre. Certains segments de graphique peuvent être trop petits pour inclure une étiquette. Vous pouvez placer votre curseur sur n'importe quel segment pour afficher le libellé et obtenir plus d'informations, notamment le nombre d'objets stockés et le nombre total d'octets pour chaque compartiment ou conteneur.



4. Sélectionnez **Détails du compartiment** (S3) ou **Détails du conteneur** (Swift) pour afficher la liste des objets espacés utilisés et du nombre d'objets pour chacun des compartiments ou conteneurs du locataire.



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

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

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

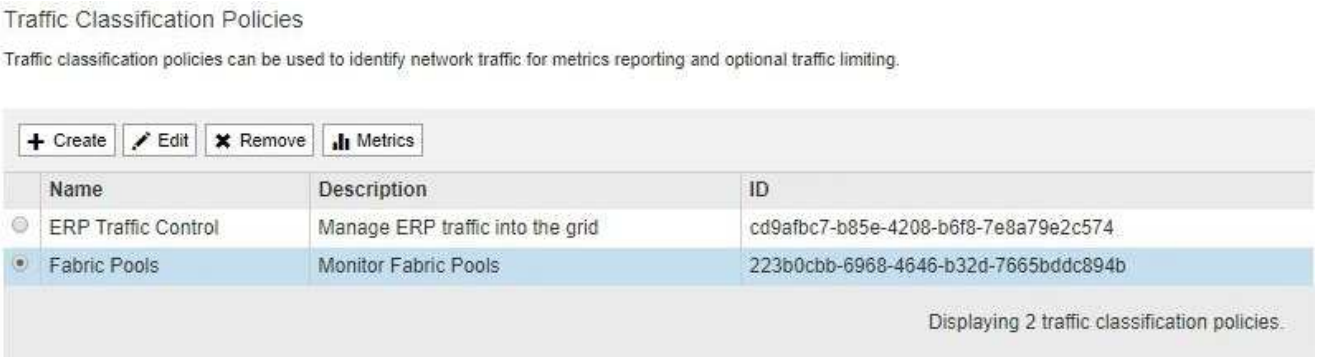
Tenant ID	Bucket Name	Space Used (Bytes)	Number of Objects
64796966429038923647	bucket-01	88717711	14
64796966429038923647	bucket-02	21747507	11
64796966429038923647	bucket-03	15294070	3

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

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

   a. Sélectionnez **Configuration** > **Paramètres réseau** > **Classification du trafic**.

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



   a. Consultez la liste des politiques pour identifier celles qui s'appliquent à un locataire spécifique.

   b. Pour afficher les mesures associées à une stratégie, sélectionnez le bouton radio à gauche de la

stratégie, puis cliquez sur **métriques**.

c. Analysez les graphiques pour déterminer à quelle fréquence la stratégie limite le trafic et si vous devez ajuster la stratégie.

   Pour créer, modifier ou supprimer des stratégies de classification de trafic, reportez-vous aux instructions d'administration de StorageGRID.

7. Vous pouvez également utiliser le journal d'audit pour un contrôle plus granulaire des activités d'un locataire.

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

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

   Les journaux d'audit sont écrits dans des fichiers texte que vous pouvez analyser à l'aide de l'outil d'analyse des journaux de votre choix. Vous pouvez ainsi mieux comprendre les activités des clients ou implémenter des modèles de facturation et de refacturation sophistiqués. Pour plus d'informations, reportez-vous aux instructions relatives à la compréhension des messages d'audit.

8. Vous pouvez également utiliser des metrics Prometheus pour fournir des rapports sur l'activité des locataires :
   - Dans le Gestionnaire de grille, sélectionnez **support** > **Outils** > **métriques**. Vous pouvez utiliser les tableaux de bord existants, tels que S3 Overview, pour examiner les activités des clients.

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

   - Sélectionnez **aide** > **Documentation API**. Vous pouvez utiliser les mesures de la section Metrics de l'API de gestion du grid pour créer des règles d'alerte et des tableaux de bord personnalisés pour l'activité des locataires.

Informations associées

"Référence des alertes"

"Examiner les journaux d'audit"

"Administrer StorageGRID"

"L'examen des metrics de support"

Contrôle de la capacité d'archivage

Vous ne pouvez pas surveiller directement la capacité d'un système de stockage d'archives externe par le biais du système StorageGRID. Vous pouvez toutefois contrôler si le nœud d'archivage peut toujours envoyer des données d'objet à la destination d'archivage, ce qui peut indiquer qu'une extension de support d'archivage est nécessaire.

Ce dont vous avez besoin

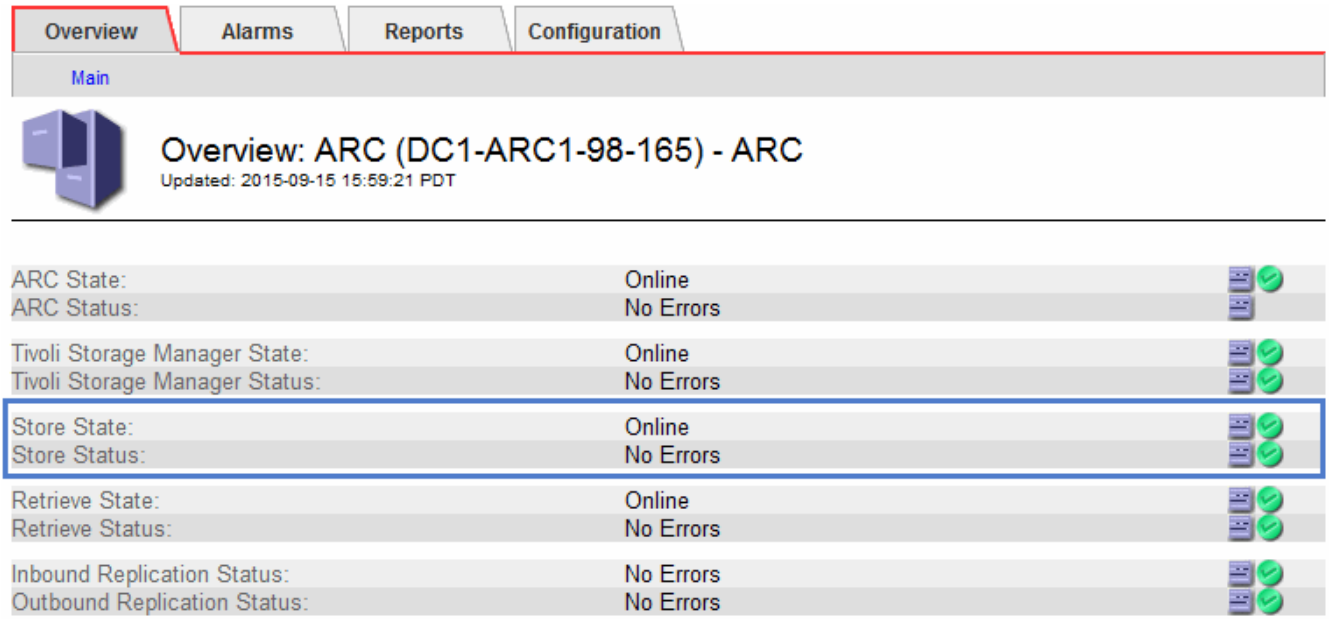
- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

Vous pouvez surveiller le composant de stockage pour vérifier si le nœud d'archivage peut toujours envoyer des données d'objet au système de stockage d'archives ciblé. L'alarme Store Failures (ARVF) peut également indiquer que le système de stockage d'archives ciblé a atteint sa capacité et qu'il ne peut plus accepter les données d'objet.

Étapes

1. Sélectionnez **support** > **Outils** > **topologie de grille**.
2. Sélectionnez ***Archive Node*** > **ARC> vue d'ensemble> main**.
3. Vérifiez les attributs Etat du magasin et Etat du magasin pour confirmer que le composant Store est en ligne sans erreur.



Un composant de stockage hors ligne ou un composant contenant des erreurs peut indiquer que le système de stockage d'archivage ciblé ne peut plus accepter les données d'objet en raison de sa capacité atteinte.

Informations associées

"Administrer StorageGRID"

Surveillance des opérations d'équilibrage des charges

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

Ce dont vous avez besoin

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

- Vous devez disposer d’autorisations d’accès spécifiques.

Description de la tâche

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

Le service CLB est obsolète.

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

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

Reportez-vous à la section sur la configuration des connexions client dans les instructions d’administration de StorageGRID.

Étapes

1. Si les clients S3 ou Swift se connectent à l’aide du service Load Balancer, vérifiez que les nœuds d’administration ou les nœuds de passerelle distribuent le trafic activement, comme indiqué :
   a. Sélectionnez **noeuds**.
   b. Sélectionnez un nœud de passerelle ou un nœud d’administration.
   c. Dans l’onglet **Présentation**, vérifiez si une interface de nœud se trouve dans un groupe HA et si l’interface de nœud a le rôle maître.

      Les nœuds ayant le rôle Master et les nœuds qui ne se trouvent pas dans un groupe haute disponibilité doivent être activement répartis les demandes vers les clients.

   d. Pour chaque nœud qui doit distribuer activement les demandes client, sélectionnez l’onglet **Load Balancer**.
   e. Consultez le graphique du trafic des demandes d’équilibrage de charge pour la dernière semaine afin de vous assurer que le nœud distribue activement les demandes.

      Les nœuds d’un groupe haute disponibilité à sauvegarde active peuvent parfois prendre le rôle de sauvegarde. Pendant ce temps, les nœuds ne distribuent pas les requêtes client.

   f. Consultez le graphique du taux de demande entrant de Load Balancer pour la dernière semaine afin de vérifier le débit d’objet du nœud.
   g. Répétez cette procédure pour chaque nœud d’administration ou de passerelle du système StorageGRID.
   h. Vous pouvez également utiliser les stratégies de classification du trafic pour afficher une ventilation plus détaillée du trafic servi par le service Load Balancer.
2. Si les clients S3 ou Swift se connectent à l’aide du service CLB (obsolète), effectuez les vérifications suivantes :
   a. Sélectionnez **noeuds**.
   b. Sélectionnez un nœud de passerelle.

c. Dans l'onglet **Présentation**, vérifiez si une interface de nœud se trouve dans un groupe HA et si l'interface de nœud a le rôle Master.

   Les nœuds ayant le rôle Master et les nœuds qui ne se trouvent pas dans un groupe haute disponibilité doivent être activement répartis les demandes vers les clients.

d. Pour chaque noeud de passerelle qui doit être en train de distribuer activement les demandes client, sélectionnez **support** > **Outils** > **topologie de grille**.

e. Sélectionnez ***Gateway Node*** > **CLB** > **HTTP** > **Présentation** > **main**.

f. Vérifiez le nombre de **sessions entrantes - établies** pour vérifier que le nœud de passerelle a traité activement les demandes.

3. Vérifiez que ces demandes sont réparties de manière homogène vers les nœuds de stockage.

   a. Sélectionnez ***Storage Node*** > **LDR** > **HTTP**.

   b. Examiner le nombre de **sessions entrantes actuellement établies**.

   c. Répétez l'opération pour chaque nœud de stockage de la grille.

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

Informations associées

"Administrer StorageGRID"

"Affichage de l'onglet Load Balancer"

Application de correctifs ou mise à niveau des logiciels si nécessaire

Si un correctif ou une nouvelle version du logiciel StorageGRID est disponible, vous devez déterminer si la mise à jour est adaptée à votre système et l'installer si nécessaire.

Description de la tâche

Les correctifs StorageGRID contiennent des modifications logicielles qui sont disponibles en dehors d'une version de fonctionnalité ou de correctif. Les mêmes modifications seront incluses dans une prochaine version.

Étapes

1. Accédez à la page de téléchargements NetApp pour StorageGRID.

   "Téléchargement NetApp : StorageGRID"

2. Sélectionnez la flèche vers le bas du champ **Type/Sélectionner version** pour afficher la liste des mises à jour disponibles au téléchargement :

   - **Versions du logiciel StorageGRID** : 11.*x.y*
   - **Correctifs StorageGRID**: 11.*x. .yz*

3. Vérifiez les modifications qui sont incluses dans la mise à jour :

   a. Sélectionnez la version dans le menu déroulant et cliquez sur **Go**.

   b. Connectez-vous en utilisant le nom d'utilisateur et le mot de passe de votre compte NetApp.

   c. Lisez le contrat de licence de l'utilisateur final, cochez la case, puis sélectionnez **accepter et continuer**.

      La page des téléchargements de la version sélectionnée s'affiche.

4. Découvrez les changements inclus dans la version du logiciel ou le correctif.
    - Pour une nouvelle version du logiciel, consultez la rubrique « Nouveautés » dans les instructions de mise à niveau de StorageGRID.
    - Pour un correctif, téléchargez le fichier README pour un résumé des modifications incluses dans le correctif.
5. Si vous décidez qu'une mise à jour logicielle est nécessaire, suivez les instructions avant de continuer.
    - Pour obtenir une nouvelle version du logiciel, suivez attentivement les instructions de mise à niveau de StorageGRID.
    - Pour un correctif, recherchez la procédure de correctif dans les instructions de récupération et de maintenance

Informations connexes

"Mise à niveau du logiciel"

"Maintenance et récupération"

Gestion des alertes et des alarmes

Le système d'alerte StorageGRID est conçu pour vous informer des problèmes opérationnels qui requièrent votre attention. Si nécessaire, vous pouvez également utiliser l'ancien système d'alarme pour surveiller votre système. Cette section contient les sous-sections suivantes :

- "Comparaison des alertes et des alarmes"
- "Gestion des alertes"
- "Gestion des alarmes (système hérité)"

StorageGRID intègre deux systèmes pour vous informer des problèmes.

Système d'alerte

Le système d'alerte est conçu pour être votre outil principal de surveillance des problèmes susceptibles de survenir dans votre système StorageGRID. Le système d'alerte offre une interface facile à utiliser pour détecter, évaluer et résoudre les problèmes.

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

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

Système d'alarme existant

Le système d'alarme est pris en charge, mais est considéré comme un système hérité. Comme les alertes, les alarmes sont déclenchées à des niveaux de gravité spécifiques lorsque les attributs atteignent des valeurs de seuil définies. Toutefois, contrairement aux alertes, de nombreuses alarmes sont déclenchées pour les événements que vous pouvez ignorer en toute sécurité, ce qui peut entraîner un nombre excessif de notifications par e-mail ou SNMP.

Lorsqu'une alarme est déclenchée, les actions suivantes se produisent :

- Le nombre d'alarmes héritées sur le tableau de bord est incrémenté.
- L'alarme apparaît sur la page **support** > **alarmes (hérité)** > **alarmes actuelles**.
- Une notification par e-mail est envoyée, en supposant que vous avez configuré un serveur SMTP et configuré une ou plusieurs listes de diffusion.
- Une notification SNMP peut être envoyée, en supposant que vous avez configuré l'agent SNMP StorageGRID. (Les notifications SNMP ne sont pas envoyées pour toutes les alarmes ou tous les niveaux d'alarme.)

Comparaison des alertes et des alarmes

Il existe un certain nombre de similitudes entre le système d'alerte et le système d'alarme existant, mais le système d'alerte offre des avantages significatifs et est plus facile à utiliser.

Reportez-vous au tableau suivant pour savoir comment effectuer des opérations similaires.

	Alertes	Alarmes (système hérité)
Comment puis-je voir quelles alertes ou alarmes sont actives ?	• Cliquez sur le lien **alertes actuelles** dans le tableau de bord. • Cliquez sur l'alerte sur la page **noeuds** > **Présentation**. • Sélectionnez **alertes** > **actuel**. "Affichage des alertes en cours"	• Cliquez sur le lien **alarmes héritées** dans le tableau de bord. • Sélectionnez **support** > **alarmes (hérité)** > **alarmes actuelles**. "Affichage des anciennes alarmes"
Quelle est la cause du déclenchement d'une alerte ou d'une alerte ?	Les alertes sont déclenchées lorsqu'une expression Prometheus dans une règle d'alerte est évaluée comme TRUE pour une condition de déclenchement et une durée spécifiques. "Affichage des règles d'alerte"	Les alarmes sont déclenchées lorsqu'un attribut StorageGRID atteint une valeur de seuil. "Logique de déclenchement d'alarme (système hérité)"

	Alertes	Alarmes (système hérité)
Si une alerte ou une alarme est déclenchée, comment résoudre le problème sous-jacent ?	Les actions recommandées pour une alerte sont incluses dans les notifications par e-mail et sont disponibles dans les pages alertes du Gestionnaire de grille. Si nécessaire, des informations supplémentaires sont fournies dans la documentation StorageGRID. "Référence des alertes"	Pour en savoir plus sur une alarme, cliquez sur le nom de l'attribut ou recherchez un code d'alarme dans la documentation StorageGRID. "Référence des alarmes (système hérité)"
Où puis-je voir une liste d'alertes ou d'alarmes qui ont été résolues ?	• Cliquez sur le lien **alertes récemment résolues** dans le tableau de bord. • Sélectionnez **alertes** > **résolu**. "Affichage des alertes résolues"	Sélectionnez **support** > **alarmes (hérité)** > **alarmes historiques**. "Vérification des alarmes historiques et de la fréquence des alarmes (système hérité)"
Où puis-je gérer les paramètres ?	Sélectionnez **alertes**. Utilisez ensuite les options du menu alertes. "Gestion des alertes"	Sélectionnez **support**. Utilisez ensuite les options de la section **alarmes (hérité)** du menu. "Gestion des alarmes (système hérité)"
Quelles autorisations de groupe d'utilisateurs ai-je besoin ?	• Toute personne qui peut se connecter au Grid Manager peut afficher les alertes actuelles et résolues. • Vous devez disposer de l'autorisation gérer les alertes pour gérer les silences, les notifications d'alerte et les règles d'alerte. "Administrer StorageGRID"	• Toute personne qui peut se connecter à Grid Manager peut afficher les alarmes héritées. • Vous devez disposer de l'autorisation accuser réception d'alarmes pour accuser réception d'alarmes. • Vous devez disposer d'autorisations Grid Topology page Configuration et d'autres autorisations Grid Configuration pour gérer les alarmes globales et les notifications par e-mail. "Administrer StorageGRID"

	Alertes	Alarmes (système hérité)
Comment puis-je gérer les notifications par e-mail ?	Sélectionnez **alertes** > **Configuration email**. **Remarque :** puisque les alarmes et les alertes sont des systèmes indépendants, la configuration des e-mails utilisée pour les notifications d'alarme et de AutoSupport n'est pas utilisée pour les notifications d'alerte. Cependant, vous pouvez utiliser le même serveur de messagerie pour toutes les notifications. "Gestion des notifications d'alertes"	Sélectionnez **support** > **alarmes (hérité)** > **Configuration des e-mails existants**. "Configuration des notifications pour les alarmes (système hérité)"
Comment gérer les notifications SNMP ?	Sélectionnez **Configuration** > **surveillance** > **agent SNMP**. "Utilisation de la surveillance SNMP"	Sélectionnez **Configuration** > **surveillance** > **agent SNMP**. "Utilisation de la surveillance SNMP" **Remarque** : les notifications SNMP ne sont pas envoyées pour chaque gravité d'alarme ou d'alarme. "Alarmes générant des notifications SNMP (système hérité)"
Comment puis-je contrôler qui reçoit les notifications ?	1. Sélectionnez **alertes** > **Configuration email**. 2. Dans la section **destinataires**, entrez une adresse e-mail pour chaque liste d'e-mails ou personne qui doit recevoir un e-mail lorsqu'une alerte se produit. "Configuration des notifications par e-mail pour les alertes"	1. Sélectionnez **support** > **alarmes (hérité)** > **Configuration des e-mails existants**. 2. Création d'une liste de diffusion. 3. Sélectionnez **Notifications**. 4. Sélectionnez la liste de diffusion. "Création de listes de diffusion pour les notifications d'alarme (système hérité)" "Configuration des notifications par e-mail pour les alarmes (système hérité)"

	Alertes	Alarmes (système hérité)
Quels nœuds d'administration envoient des notifications ?	Un seul nœud d'administration (l'« expéditeur préféré »). "Administrer StorageGRID"	Un seul nœud d'administration (l'« expéditeur préféré »). "Administrer StorageGRID"
Comment supprimer certaines notifications ?	1. Sélectionnez **alertes** > **silences**. 2. Sélectionnez la règle d'alerte que vous souhaitez désactiver. 3. Spécifiez une durée pour le silence. 4. Sélectionnez la gravité de l'alerte que vous souhaitez désactiver. 5. Sélectionnez cette option pour appliquer le silence à la grille entière, à un seul site ou à un seul nœud. **Remarque** : si vous avez activé l'agent SNMP, les silences suppriment également les interruptions SNMP et informe. "Neutralisation des notifications d'alerte"	1. Sélectionnez **support** > **alarmes (hérité)** > **Configuration des e-mails existants**. 2. Sélectionnez **Notifications**. 3. Sélectionnez une liste de diffusion et sélectionnez **Supprimer**. "Suppression des notifications d'alarme pour une liste de diffusion (système existant)"
Comment supprimer toutes les notifications ?	Sélectionnez **alertes** > **silences**.sélectionnez alors **toutes les règles**. **Remarque** : si vous avez activé l'agent SNMP, les silences suppriment également les interruptions SNMP et informe. "Neutralisation des notifications d'alerte"	1. Sélectionnez **Configuration** > **Paramètres système** > **Options d'affichage**. 2. Cochez la case **notification Supprimer tout**. **Remarque** : la suppression des notifications par e-mail dans tout le système supprime également les e-mails AutoSupport déclenchés par des événements. "Suppression des notifications par e-mail à l'échelle du système"

	Alertes	Alarmes (système hérité)
Comment personnaliser les conditions et les déclencheurs ?	1. Sélectionnez **alertes** > **règles d'alerte**. 2. Sélectionnez une règle par défaut à modifier ou sélectionnez **Créer une règle personnalisée**. "Modification d'une règle d'alerte" "Création de règles d'alerte personnalisées"	1. Sélectionnez **support** > **alarmes (hérité)** > **alarmes globales**. 2. Créez une alarme personnalisée globale pour remplacer une alarme par défaut ou pour surveiller un attribut qui n'a pas d'alarme par défaut. "Création d'alarmes personnalisées globales (système hérité)"
Comment désactiver une alerte ou une alarme individuelle ?	1. Sélectionnez **alertes** > **règles d'alerte**. 2. Sélectionnez la règle et cliquez sur **Modifier la règle**. 3. Décochez la case **Enabled**. "Désactivation d'une règle d'alerte"	1. Sélectionnez **support** > **alarmes (hérité)** > **alarmes globales**. 2. Sélectionnez la règle et cliquez sur l'icône Modifier. 3. Décochez la case **Enabled**. "Désactivation d'une alarme par défaut (système hérité)" "Désactivation des alarmes personnalisées globales (système hérité)"

Gestion des alertes

Les alertes vous permettent de surveiller différents événements et conditions au sein de votre système StorageGRID. Vous pouvez gérer les alertes en créant des alertes personnalisées, en modifiant ou en désactivant les alertes par défaut, en configurant des notifications par e-mail pour les alertes et en désactivant les notifications d'alertes.

Informations associées

"Affichage des alertes en cours"

"Affichage des alertes résolues"

"Affichage d'une alerte spécifique"

"Référence des alertes"

Quelles sont les alertes

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

- Le système d'alerte est axé sur des problèmes exploitables dans le système. Contrairement à certaines

alarmes du système hérité, des alertes sont déclenchées pour les événements nécessitant votre attention immédiate, et non pour les événements qui peuvent être ignorés en toute sécurité.

- La page alertes en cours fournit une interface conviviale permettant d'afficher les problèmes actuels. Vous pouvez trier la liste par alerte individuelle et par groupe d'alertes. Par exemple, il peut être nécessaire de trier toutes les alertes par nœud/site pour afficher les alertes qui affectent un nœud spécifique. Vous pouvez également trier les alertes d'un groupe par heure déclenchée pour trouver l'instance la plus récente d'une alerte spécifique.
- La page alertes résolues fournit des informations similaires à celles de la page alertes en cours, mais elle vous permet de rechercher et d'afficher l'historique des alertes qui ont été résolues, notamment lorsque l'alerte a été déclenchée et quand elle a été résolue.
- Plusieurs alertes du même type sont regroupées en un seul e-mail afin de réduire le nombre de notifications. De plus, plusieurs alertes du même type sont affichées sous forme de groupe sur la page alertes. Vous pouvez développer et réduire les groupes d'alertes pour afficher ou masquer les alertes individuelles. Par exemple, si plusieurs nœuds indiquent l'alerte **Impossible de communiquer avec le nœud** en même temps, un seul e-mail est envoyé et l'alerte est affichée comme un groupe sur la page alertes.
- Les alertes utilisent des noms et des descriptions intuitifs pour vous aider à comprendre rapidement le problème. Les notifications d'alerte incluent des informations détaillées sur le nœud et le site concernés, la gravité de l'alerte, le moment où la règle d'alerte a été déclenchée et la valeur actuelle des mesures relatives à l'alerte.
- Les notifications par e-mail d'alerte et les listes d'alertes figurant sur les pages alertes en cours et alertes résolues fournissent des actions recommandées pour résoudre une alerte. Ces actions recommandées incluent souvent des liens directs vers le centre de documentation StorageGRID pour faciliter l'accès aux procédures de dépannage plus détaillées.
- Si vous avez besoin de supprimer temporairement les notifications pour une alerte à un ou plusieurs niveaux de sévérité, vous pouvez facilement désactiver une règle d'alerte spécifique pendant une durée spécifiée et pour la grille dans son ensemble, un seul site ou un seul nœud. Vous pouvez également désactiver toutes les règles d'alerte, par exemple, lors d'une procédure de maintenance planifiée telle qu'une mise à niveau logicielle.
- Vous pouvez modifier les règles d'alerte par défaut si nécessaire. Vous pouvez désactiver complètement une règle d'alerte ou modifier ses conditions et sa durée de déclenchement.
- Vous pouvez créer des règles d'alerte personnalisées afin de cibler les conditions spécifiques qui sont pertinentes pour votre situation et de proposer vos propres actions recommandées. Pour définir les conditions d'une alerte personnalisée, vous créez des expressions à l'aide des metrics Prometheus disponibles dans la section Metrics de l'API de gestion du grid.

Gestion des règles d'alerte

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

Affichage des règles d'alerte

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

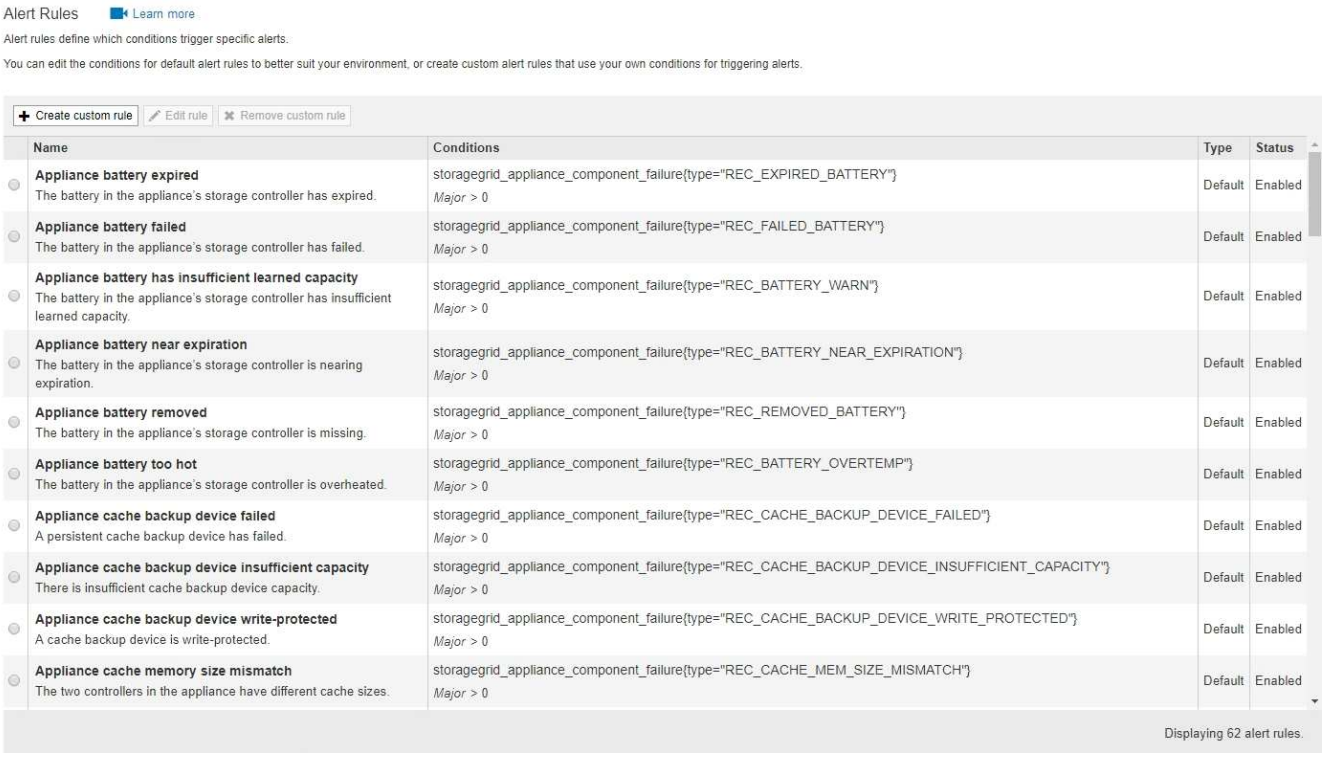
Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer de l'autorisation gérer les alertes ou accès racine.

Étapes

1. Sélectionnez **alertes** > **règles d'alerte**.

   La page règles d'alerte s'affiche.



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

En-tête de colonne	Description
Nom	Nom et description uniques de la règle d'alerte. Les règles d'alerte personnalisées sont répertoriées en premier, suivies des règles d'alerte par défaut. Le nom de la règle d'alerte est l'objet des notifications par e-mail.

En-tête de colonne	Description
Conditions	Expressions Prometheus qui déterminent le moment où cette alerte est déclenchée. Une alerte peut être déclenchée à un ou plusieurs des niveaux de sévérité suivants, mais une condition pour chaque gravité n'est pas requise. • **Critique** : Il existe une condition anormale qui a arrêté les opérations normales d'un nœud ou service StorageGRID. Vous devez immédiatement résoudre le problème sous-jacent. Une interruption du service et une perte de données peuvent se produire si le problème n'est pas résolu. • **Majeur** : Il existe une condition anormale affectant les opérations en cours ou approchant le seuil d'une alerte critique. Vous devez examiner les alertes majeures et résoudre tous les problèmes sous-jacents pour vérifier que leur condition anormale n'arrête pas le fonctionnement normal d'un nœud ou d'un service StorageGRID. • **Mineur** : Le système fonctionne normalement, mais il existe une condition anormale qui pourrait affecter la capacité du système à fonctionner s'il continue. Vous devez surveiller et résoudre les alertes mineures qui ne sont pas claires par elles-mêmes pour vous assurer qu'elles n'entraînent pas un problème plus grave.
Type	Type de règle d'alerte : • **Default** : 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*** : règle d'alerte par défaut qui inclut une condition ou une durée modifiée. Si nécessaire, vous pouvez facilement rétablir une condition modifiée par défaut. • **Custom** : une règle d'alerte que vous avez créée. Vous pouvez désactiver, modifier et supprimer des règles d'alerte personnalisées.
État	Si cette règle d'alerte est actuellement activée ou désactivée. Les conditions des règles d'alerte désactivées ne sont pas évaluées. Aucune alerte n'est donc déclenchée.

Informations associées

"Référence des alertes"

Création de règles d'alerte personnalisées

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

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer de l'autorisation gérer les alertes ou accès racine.

Description de la tâche

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

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

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

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

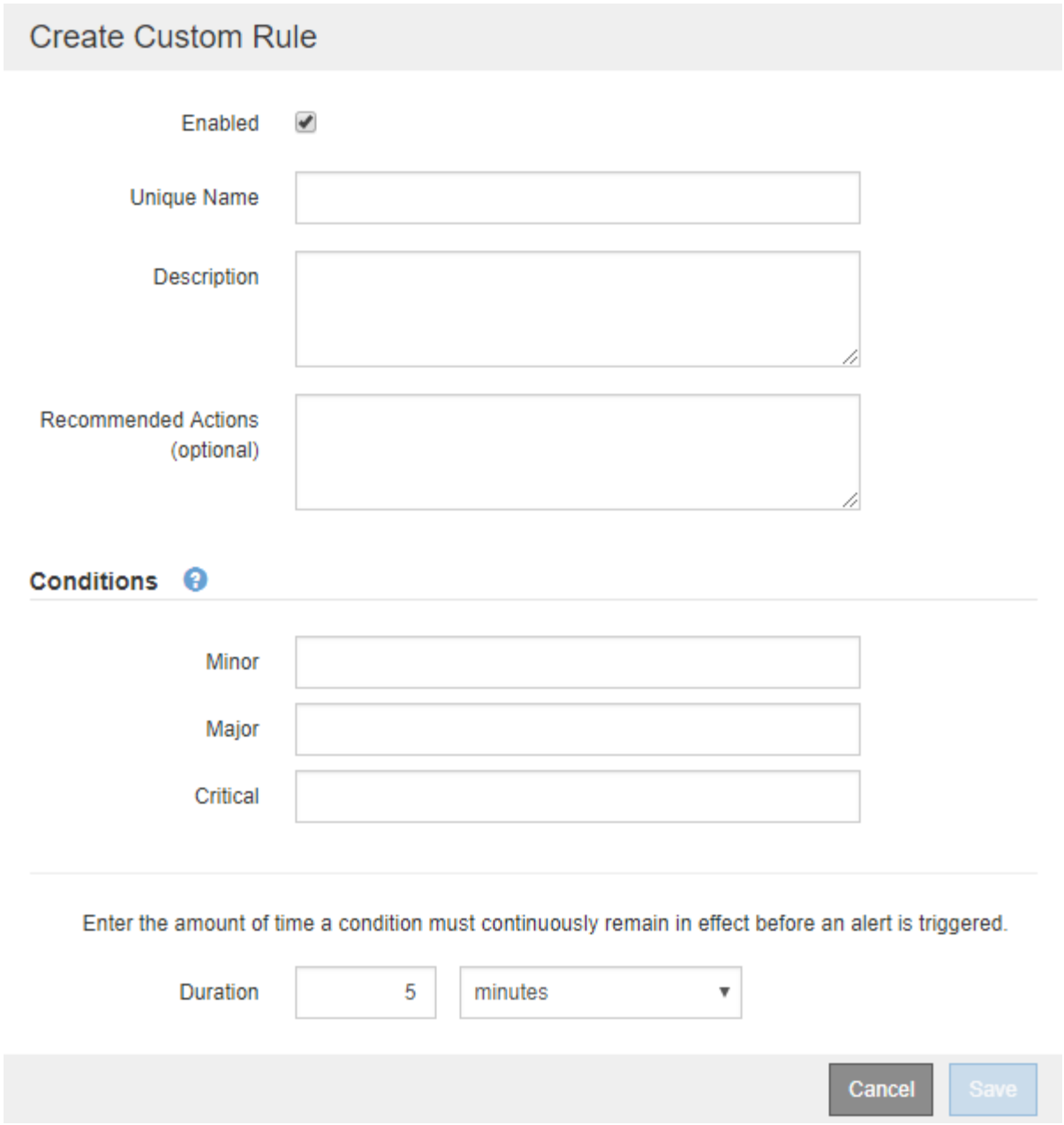
Étapes

1. Sélectionnez **alertes** > **règles d'alerte**.

   La page règles d'alerte s'affiche.

2. Sélectionnez **Créer règle personnalisée**.

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



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

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

4. Saisissez les informations suivantes :

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

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

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

   Une expression de base est généralement de la forme :

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

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

   Pour afficher les metrics disponibles et tester les expressions Prometheus, cliquez sur l'icône d'aide Et suivez le lien vers la section Metrics de l'API de gestion du grid.

   Pour en savoir plus sur l'utilisation de l'API de gestion de grille, reportez-vous aux instructions d'administration de StorageGRID. Pour plus d'informations sur la syntaxe des requêtes Prometheus, consultez la documentation Prometheus.

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

   ```
   node_memory_MemTotal_bytes < 24000000000
   ```

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

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

   La valeur par défaut est 5 minutes.

7. Cliquez sur **Enregistrer**.

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

Informations associées

"Administrer StorageGRID"

"Metrics Prometheus couramment utilisés"

"Prometheus : notions de base sur les requêtes"

Modification d'une règle d'alerte

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

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer de l'autorisation gérer les alertes ou accès racine.

Description de la tâche

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

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

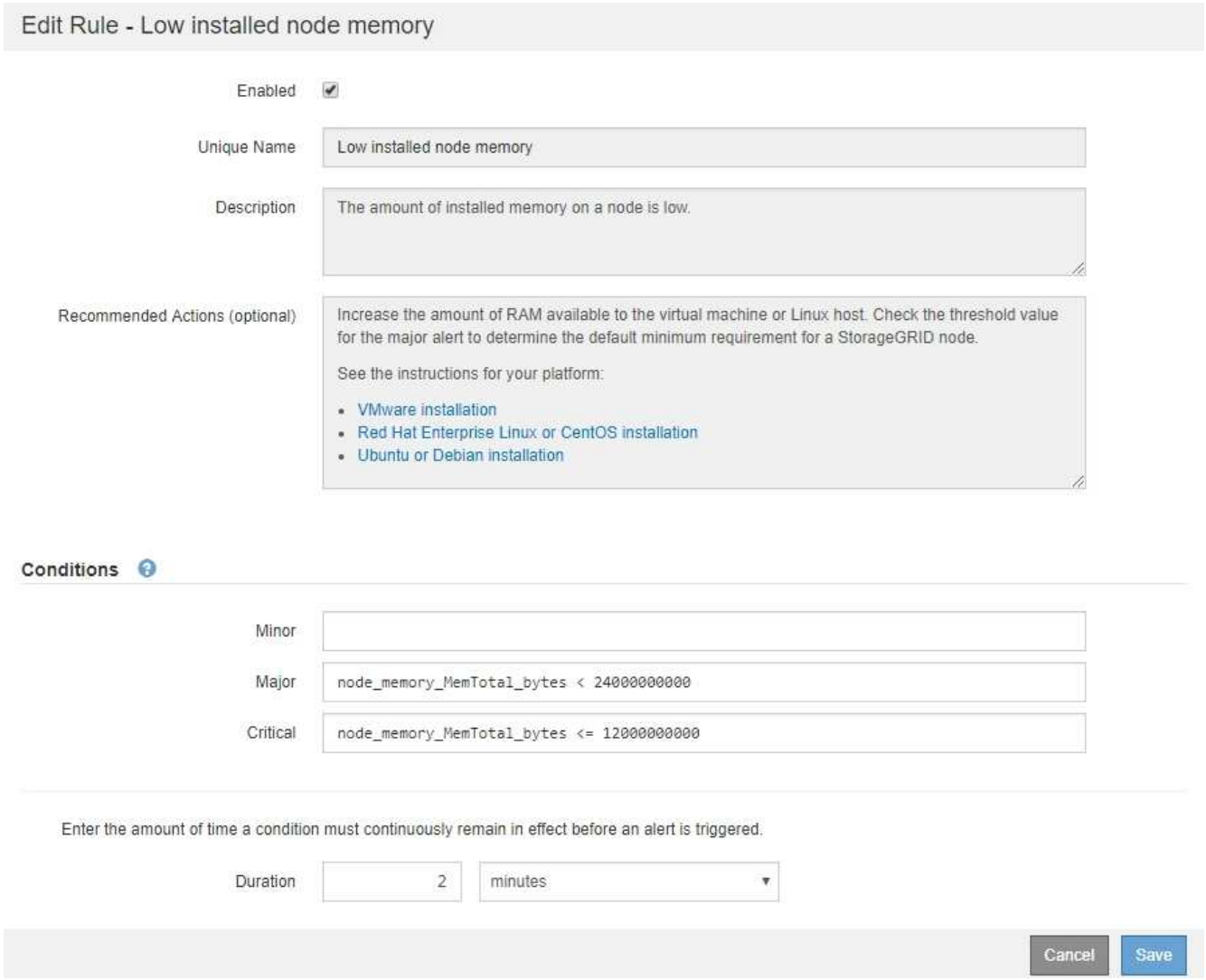
Étapes

1. Sélectionnez **alertes** > **règles d'alerte**.

   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 désélectionnez la case **Enabled** pour déterminer si cette règle d'alerte est actuellement activée.

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

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

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

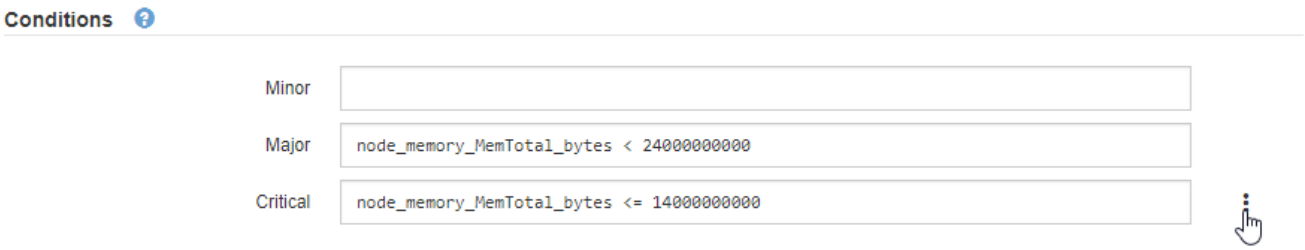
5. Pour les règles d'alerte personnalisées, mettez à jour les informations suivantes si nécessaire.

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

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

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

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



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

Une expression de base est généralement de la forme :

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

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

Pour afficher les metrics disponibles et tester les expressions Prometheus, cliquez sur l'icône d'aide Et suivez le lien vers la section Metrics de l'API de gestion du grid.

Pour en savoir plus sur l'utilisation de l'API de gestion de grille, reportez-vous aux instructions d'administration de StorageGRID. Pour plus d'informations sur la syntaxe des requêtes Prometheus, consultez la documentation Prometheus.

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

```
node_memory_MemTotal_bytes < 24000000000
```

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

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

   La valeur par défaut est 5 minutes.

8. Cliquez sur **Enregistrer**.

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

Informations associées

"Administrer StorageGRID"

"Metrics Prometheus couramment utilisés"

"Prometheus : notions de base sur les requêtes"

Désactivation d'une règle d'alerte

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

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer de l'autorisation gérer les alertes ou accès racine.

Description de la tâche

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

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

Étapes

1. Sélectionnez **alertes** > **règles d'alerte**.

   La page règles d'alerte s'affiche.

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

3. Sélectionnez **Modifier la règle**.

   La boîte de dialogue Modifier la règle s'affiche.

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

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

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

5. Cliquez sur **Enregistrer**.

   Disabled apparaît dans la colonne **Status**.

Suppression d'une règle d'alerte personnalisée

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

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer de l'autorisation gérer les alertes ou accès racine.

Étapes

1. Sélectionnez **alertes** > **règles d'alerte**.

   La page règles d'alerte s'affiche.

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

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

3. Cliquez sur **Supprimer la règle personnalisée**.

   Une boîte de dialogue de confirmation s'affiche.

4. Cliquez sur **OK** pour supprimer la règle d'alerte.

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

Gestion des notifications d'alertes

Lorsqu'une alerte est déclenchée, StorageGRID peut envoyer des notifications par e-mail et des notifications SNMP (simple Network Management Protocol) (traps).

Configuration des 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.

Description de la tâche

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

Pour savoir comment configurer l'agent SNMP, reportez-vous à la section utilisation de la surveillance SNMP.

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

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

Des notifications d'interruption et d'information sont envoyées lorsqu'une alerte par défaut ou personnalisée est déclenchée à n'importe quel niveau de gravité. Pour supprimer les notifications SNMP pour une alerte, vous devez configurer un silence pour l'alerte. Les notifications d'alerte sont envoyées par n'importe quel nœud d'administration configuré pour être l'expéditeur préféré. Par défaut, le nœud d'administration principal est sélectionné. Pour plus de détails, reportez-vous aux instructions d'administration de StorageGRID.

> Des notifications de déroutement et d'information sont également envoyées lorsque certaines alarmes (système hérité) sont déclenchées à des niveaux de gravité spécifiés ou supérieurs ; cependant, les notifications SNMP ne sont pas envoyées pour chaque alarme ou chaque gravité d'alarme.

Informations associées

"Utilisation de la surveillance SNMP"

"Neutralisation des notifications d'alerte"

"Administrer StorageGRID"

"Alarmes générant des notifications SNMP (système hérité)"

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

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer de l'autorisation gérer les alertes ou accès racine.

Ce dont vous avez besoin

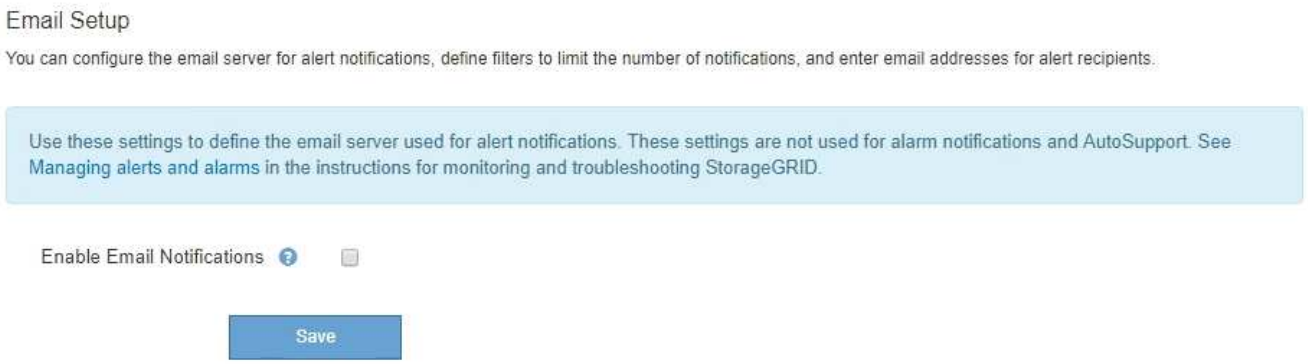
Comme les alarmes et les alertes sont des systèmes indépendants, la configuration des e-mails utilisée pour les notifications d'alerte n'est pas utilisée pour les notifications d'alarme et les messages AutoSupport. Cependant, vous pouvez utiliser le même serveur de messagerie pour toutes les notifications.

Si votre déploiement StorageGRID inclut plusieurs nœuds d'administration, vous pouvez sélectionner le nœud d'administration qui doit être l'expéditeur préféré des notifications d'alerte. Le même « expéditeur privilégié » est également utilisé pour les notifications d'alarme et les messages AutoSupport. Par défaut, le nœud d'administration principal est sélectionné. Pour plus de détails, reportez-vous aux instructions d'administration de StorageGRID.

Étapes

1. Sélectionnez **alertes** > **Configuration email**.

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



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

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

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

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

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

4. Dans la section adresses e-mail, entrez les adresses e-mail de l'expéditeur et de chaque destinataire.

   a. Pour l'adresse électronique **expéditeur**, spécifiez une adresse e-mail valide à utiliser comme adresse de pour les notifications d'alerte.

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

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

      Cliquez sur l'icône plus ✚ pour ajouter des destinataires.

5. Dans la section transport Layer Security (TLS), cochez la case **exiger TLS** si transport Layer Security (TLS) est requis pour les communications avec le serveur SMTP.

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

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

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

   b. Cochez la case **Envoyer certificat client** si votre serveur de messagerie SMTP nécessite des expéditeurs de messagerie pour fournir des certificats client pour l'authentification.

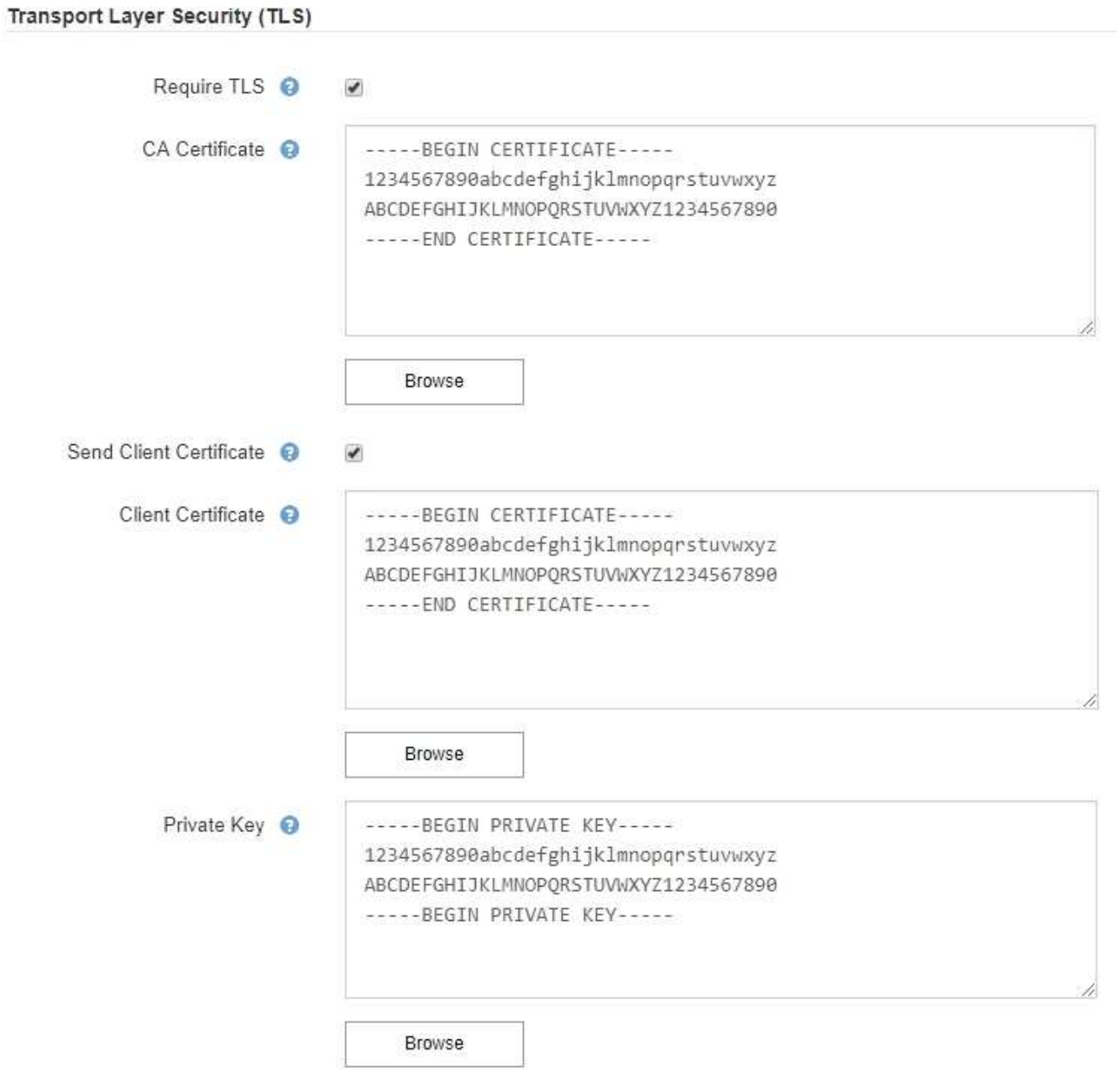
   c. Dans le champ **certificat client**, fournissez le certificat client codé PEM à envoyer au serveur SMTP.

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

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

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

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



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

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

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

7. Lorsque vous êtes prêt à tester vos paramètres de messagerie, procédez comme suit :
   a. Cliquez sur **Envoyer un e-mail de test**.

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

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

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

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

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

8. Cliquez sur **Enregistrer**.

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

   Les paramètres de messagerie sont enregistrés.

Informations associées

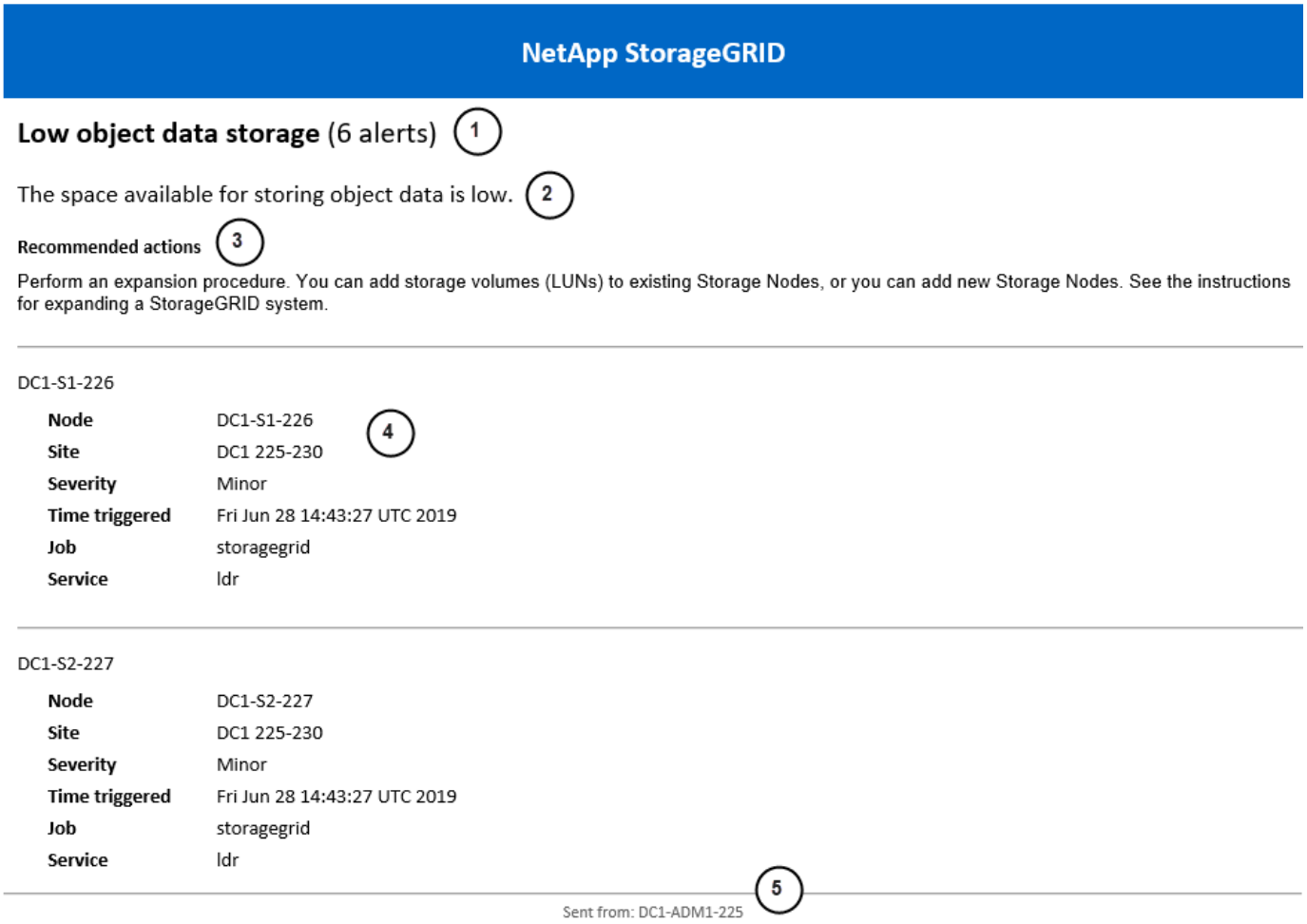
"Dépannage des notifications par e-mail d'alerte"

"Maintenance et récupération"

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

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

Les notifications par e-mail incluent les informations suivantes :



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

Informations associées

"Neutralisation des notifications d'alerte"

Comment StorageGRID groupe les alertes dans les notifications par e-mail

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

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

Comportement	Exemple
Chaque notification d'alerte s'applique uniquement aux alertes portant le même nom. Si deux alertes avec des noms différents sont déclenchées en même temps, deux notifications par e-mail sont envoyées.	• L'alerte A est déclenchée en même temps sur deux nœuds. Une seule notification est envoyée. • L'alerte A est déclenchée sur le nœud 1 et l'alerte B est déclenchée simultanément sur le nœud 2. Deux notifications sont envoyées : une pour chaque alerte.
Pour une alerte spécifique sur un nœud spécifique, si les seuils sont atteints pour plus d'un degré de sévérité, une notification est envoyée uniquement pour l'alerte la plus grave.	• L'alerte A est déclenchée et le seuil d'alerte secondaire, majeur et critique est atteint. 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 du même nom sont déclenchées pendant ce temps, StorageGRID regroupe toutes les alertes de la notification initiale.	1. L'alerte A est déclenchée sur le nœud 1 à 08:00. Aucune notification n'a été envoyée. 2. L'alerte A est déclenchée sur le nœud 2 à 08:01. Aucune notification n'a été envoyée. 3. À 08 h 02, une notification est envoyée pour signaler les deux instances de l'alerte.
Si une autre alerte du même nom est déclenchée, StorageGRID attend 10 minutes avant d'envoyer une nouvelle notification. La nouvelle notification signale toutes les alertes actives (alertes en cours qui n'ont pas été désactivées), même si elles ont été signalées précédemment.	1. L'alerte A est déclenchée sur le nœud 1 à 08:00. Une notification est envoyée à 08:02. 2. L'alerte A est déclenchée sur le nœud 2 à 08:05. Une seconde notification est envoyée à 08:15 (10 minutes plus tard). Les deux nœuds sont signalés.
Si plusieurs alertes en cours portent le même nom et que l'une de ces alertes est résolue, une nouvelle notification n'est pas envoyée si l'alerte se reproduit sur le nœud pour lequel l'alerte a été résolue.	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 seconde 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.

Comportement	Exemple
StorageGRID continue à envoyer des notifications par e-mail tous les 7 jours jusqu'à ce que toutes les instances de l'alerte soient résolues ou que la règle d'alerte soit désactivée.	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 arrêtée. Des notifications supplémentaires sont envoyées le 15 mars, le 22 mars, le 29 mars, etc.

Dépannage des notifications par e-mail d'alerte

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

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer de l'autorisation gérer les alertes ou accès racine.

Étapes

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

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

Informations associées

"Collecte des fichiers journaux et des données système"

Neutralisation des notifications d'alerte

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

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer de l'autorisation gérer les alertes ou accès racine.

Description de la tâche

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

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

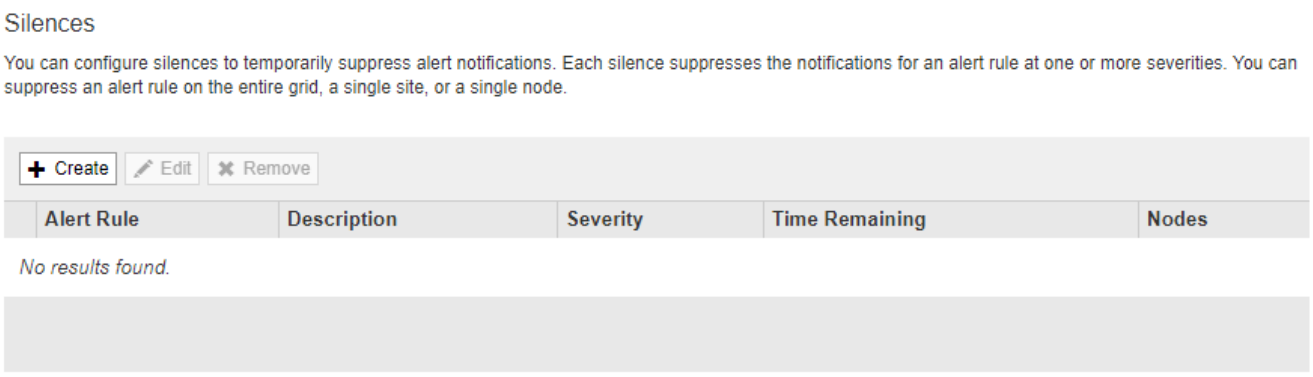
> Soyez prudent lorsque vous décidez de désactiver une règle d'alerte. Si vous neutralisez une alerte, il est possible que vous ne détectez pas un problème sous-jacent tant qu'elle n'empêche pas l'exécution d'une opération critique.

> Les alarmes et les alertes étant des systèmes indépendants, vous ne pouvez pas utiliser cette fonctionnalité pour supprimer les notifications d'alarme.

Étapes

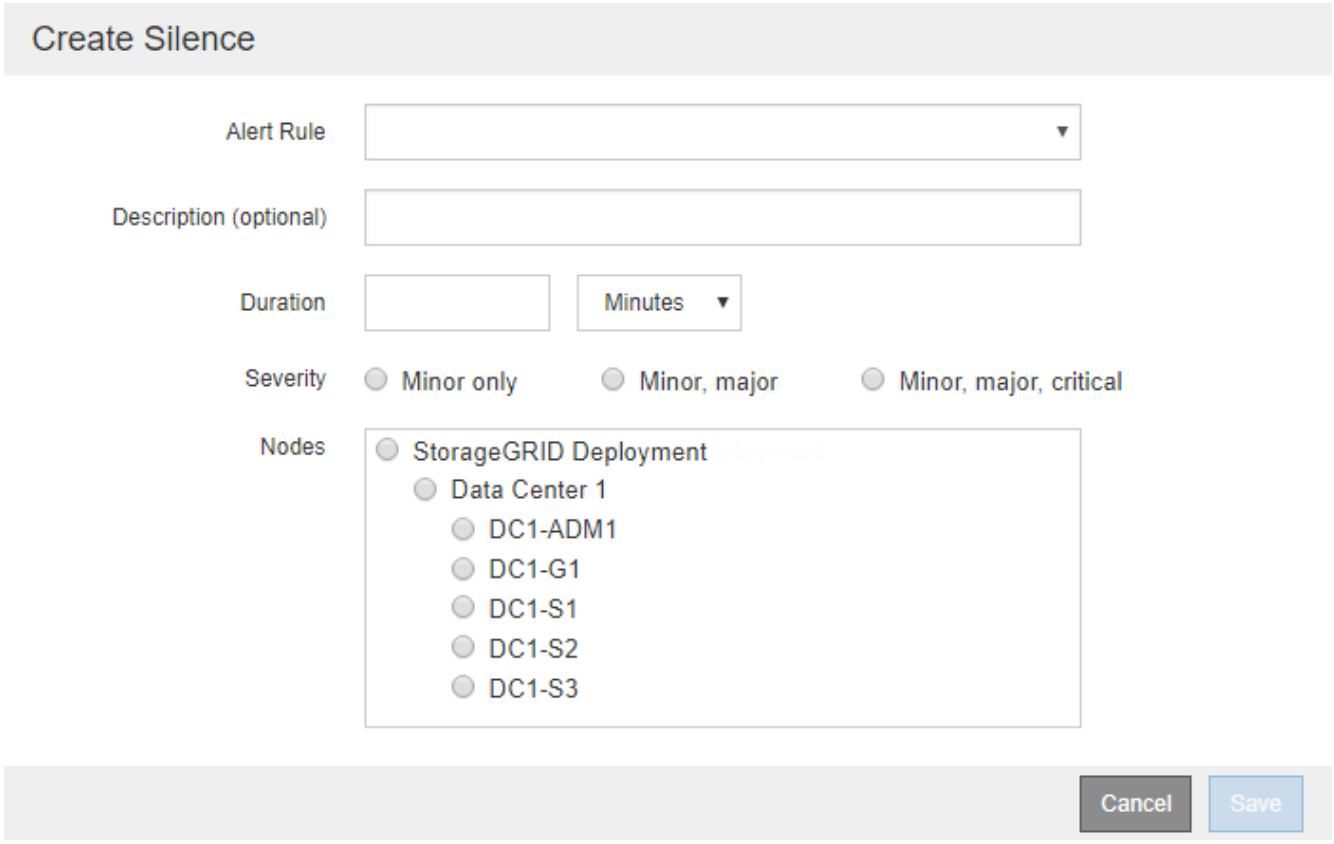
1. Sélectionnez **alertes** > **silences**.

   La page silences s'affiche.



2. Sélectionnez **Créer**.

   La boîte de dialogue Créer une Silence s'affiche.



3. Sélectionnez ou entrez 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 voulez désactiver toutes les règles d'alerte en utilisant les critères spécifiés dans cette boîte de dialogue.
Description	Éventuellement, une description du silence. Par exemple, décrivez le but de ce silence.
Durée	Combien de temps vous voulez que ce silence reste en vigueur, en minutes, heures ou jours. Un silence peut être en vigueur de 5 minutes à 1,825 jours (5 ans). **Remarque:** vous ne devez pas désactiver une règle d'alerte pour une durée prolongée. Si une règle d'alerte est mise en mode silencieux, il est possible que vous ne détectiez pas un problème sous-jacent tant qu'elle n'empêche pas l'exécution d'une opération critique. Cependant, vous devrez peut-être utiliser un silence étendu si une alerte est déclenchée par une configuration intentionnelle spécifique, par exemple pour les alertes **liaison appliance Services Down** et les alertes **liaison appliance Storage Down**.

Champ	Description
Gravité	Quelle alerte de gravité ou de gravité doit être neutralisée. Si l'alerte est déclenchée à l'un des niveaux de gravité sélectionnés, aucune notification n'est envoyée.
Nœuds	À quel nœud ou nœud vous souhaitez que ce silence s'applique. Vous pouvez supprimer une règle d'alerte ou toutes les règles de la grille dans son ensemble, un seul site ou un seul nœud. Si vous sélectionnez l'ensemble de la grille, le silence s'applique à tous les sites et à tous les nœuds. Si vous sélectionnez un site, le silence s'applique uniquement aux nœuds de ce site. **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. Cliquez sur **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. Cliquez sur **Modifier**. d. Modifiez la description, le temps restant, les niveaux de gravité sélectionnés ou le nœud affecté. e. Cliquez sur **Enregistrer**.
Supprimer un silence	a. Sélectionnez **alertes** > **silences**. b. Dans le tableau, sélectionnez le bouton radio correspondant au silence que vous souhaitez supprimer. c. Cliquez sur **Supprimer**. d. Cliquez sur **OK** pour confirmer que vous souhaitez supprimer ce silence. **Remarque** : les notifications sont maintenant envoyées lorsque cette alerte est déclenchée (sauf si elle est supprimée par un autre silence). Si cette alerte est déclenchée, l'envoi de notifications par e-mail ou SNMP peut prendre quelques minutes et la mise à jour de la page alertes.

Informations associées

"Configuration de l'agent SNMP"

Gestion des alarmes (système hérité)

Le système d'alarme StorageGRID est l'ancien système utilisé pour identifier les points de défaillance qui se produisent parfois pendant le fonctionnement normal.

> Bien que le système d'alarme existant continue d'être pris en charge, le système d'alerte offre des avantages significatifs et est plus facile à utiliser.

Informations associées

"Référence des alarmes (système hérité)"

"Affichage des anciennes alarmes"

"Administrer StorageGRID"

Classes d'alarme (système hérité)

Une alarme héritée peut appartenir à l'une des deux classes d'alarme mutuellement exclusives.

Alarmes par défaut

Les alarmes par défaut sont fournies avec chaque système StorageGRID et ne peuvent pas être modifiées. Vous pouvez cependant désactiver les alarmes par défaut ou les remplacer en définissant les alarmes personnalisées globales.

Alarmes personnalisées globales

Les alarmes personnalisées globales contrôlent l'état de tous les services d'un type donné dans le système StorageGRID. Vous pouvez créer une alarme personnalisée globale pour remplacer une alarme par défaut. Vous pouvez également créer une nouvelle alarme personnalisée globale. Cela peut être utile pour la surveillance de toutes les conditions personnalisées de votre système StorageGRID.

Informations associées

"Affichage des alarmes par défaut (système hérité)"

"Désactivation d'une alarme par défaut (système hérité)"

"Création d'alarmes personnalisées globales (système hérité)"

"Désactivation des alarmes personnalisées globales (système hérité)"

Logique de déclenchement d'alarme (système hérité)

Une alarme héritée est déclenchée lorsqu'un attribut StorageGRID atteint une valeur de seuil qui évalue à TRUE par rapport à une combinaison de classe d'alarme (personnalisée par défaut ou personnalisé global) et de niveau de gravité d'alarme.

Icône	Couleur	Gravité de l'alarme	Signification
	Jaune	Avertissement	Le nœud est connecté à la grille, mais il existe une condition inhabituelle qui n'affecte pas les opérations normales.
	Orange clair	Mineur	Le nœud est connecté à la grille, mais il existe une condition anormale qui pourrait affecter son fonctionnement à l'avenir. Vous devez étudier pour éviter la remontée des problèmes.
	Orange foncé	Majeur	Le nœud est connecté à la grille, mais il existe une condition anormale qui affecte actuellement le fonctionnement. Cela nécessite une attention particulière afin d'éviter la remontée des problèmes.
	Rouge	Primordial	Le nœud est connecté à la grille, mais il existe une condition anormale qui a arrêté des opérations normales. Vous devez résoudre le problème immédiatement.

La gravité de l'alarme et la valeur de seuil correspondante peuvent être définies pour chaque attribut numérique. Le service NMS sur chaque noeud d'administration surveille en permanence les valeurs d'attribut actuelles par rapport aux seuils configurés. Lorsqu'une alarme est déclenchée, une notification est envoyée à tout le personnel désigné.

Notez qu'un niveau de gravité Normal ne déclenche pas d'alarme.

Les valeurs d'attribut sont évaluées par rapport à la liste des alarmes activées définies pour cet attribut. La liste des alarmes est vérifiée dans l'ordre suivant pour trouver la première classe d'alarme avec une alarme définie et activée pour l'attribut :

1. Alarmes personnalisées globales avec niveaux de gravité d'alarme allant de critique à avertissement.
2. Alarmes par défaut avec niveaux de gravité d'alarme de critique à avertissement.

Une fois qu'une alarme activée pour un attribut est détectée dans la classe d'alarme supérieure, le service NMS ne s'évalue qu'au sein de cette classe. Le service NMS ne s'évalue pas par rapport aux autres catégories de priorité inférieure. En d'autres termes, si une alarme personnalisée globale est activée pour un attribut, le service NMS évalue uniquement la valeur de l'attribut par rapport aux alarmes personnalisées

globales. Les alarmes par défaut ne sont pas évaluées. Ainsi, une alarme par défaut activée pour un attribut peut répondre aux critères requis pour déclencher une alarme, mais elle ne sera pas déclenchée car une alarme personnalisée globale (qui ne répond pas aux critères spécifiés) pour le même attribut est activée. Aucune alarme n'est déclenchée et aucune notification n'est envoyée.

Exemple de déclenchement d'alarme

Cet exemple permet de comprendre comment les alarmes personnalisées globales et les alarmes par défaut sont déclenchées.

Pour l'exemple suivant, un attribut possède une alarme personnalisée globale et une alarme par défaut définie et activée, comme indiqué dans le tableau suivant.

	Seuil d'alarme personnalisé global (activé)	**Seuil d'alarme par défaut (activé)**
Avertissement	>= 1500	>= 1000
Mineur	>= 15,000	>= 1000
Majeur	>=150,000	>= 250,000

Si l'attribut est évalué lorsque sa valeur est 1000, aucune alarme n'est déclenchée et aucune notification n'est envoyée.

L'alarme personnalisée globale est prioritaire sur l'alarme par défaut. Une valeur de 1000 n'atteint pas la valeur seuil d'un niveau de gravité quelconque pour l'alarme personnalisée globale. Par conséquent, le niveau d'alarme est évalué à Normal.

Après le scénario ci-dessus, si l'alarme personnalisée globale est désactivée, rien ne change. La valeur de l'attribut doit être réévaluée avant qu'un nouveau niveau d'alarme ne soit déclenché.

Lorsque l'alarme personnalisée globale est désactivée, lorsque la valeur de l'attribut est réévaluée, la valeur de l'attribut est évaluée par rapport aux valeurs de seuil de l'alarme par défaut. Le niveau d'alarme déclenche une alarme de niveau d'avertissement et une notification par e-mail est envoyée au personnel désigné.

Alarmes de même gravité

Si deux alarmes personnalisées globales pour le même attribut ont la même gravité, les alarmes sont évaluées par une priorité « top down ».

Par exemple, si UMEM tombe à 50 Mo, la première alarme est déclenchée (= 50000000), mais pas celle en dessous (<=100000000).

Global Alarms
Updated: 2016-03-17 16:05:31 PDT

Global Custom Alarms (0 Result(s))

Enabled	Service	Attribute	Severity	Message	Operator	Value	Additional Recipients	Actions
☑	SSM	UMEM (Available Memory)	Minor	Under 50	=	5000		
☑	SSM	UMEM (Available Memory)	Minor	under10	<=	1000		

Si l'ordre est inversé, lorsque UMEM tombe à 100 Mo, la première alarme (<=100000000) est déclenchée, mais pas celle en dessous (= 50000000).

Global Alarms
Updated: 2016-03-17 16:05:31 PDT

Global Custom Alarms (0 Result(s))

Enabled	Service	Attribute	Severity	Message	Operator	Value	Additional Recipients	Actions
☑	SSM	UMEM (Available Memory)	Minor	under10	<=	1000		
☑	SSM	UMEM (Available Memory)	Minor	Under 50	=	5000		

Default Alarms

Filter by Disabled Defaults

0 Result(s)

Enabled	Service	Attribute	Severity	Message	Operator	Value	Actions

Apply Changes

Notifications

Une notification signale l'occurrence d'une alarme ou le changement d'état d'un service. Les notifications d'alarme peuvent être envoyées par e-mail ou via SNMP.

Pour éviter l'envoi de plusieurs alarmes et notifications lorsqu'une valeur de seuil d'alarme est atteinte, la gravité de l'alarme est vérifiée par rapport à la gravité actuelle de l'alarme pour l'attribut. S'il n'y a pas de changement, aucune autre action n'est entreprise. Cela signifie que, lorsque le service NMS continue à surveiller le système, il déclenche une alarme et envoie des notifications la première fois qu'il remarque une condition d'alarme pour un attribut. Si un nouveau seuil de valeur pour l'attribut est atteint et détecté, la gravité de l'alarme change et une nouvelle notification est envoyée. Les alarmes sont effacées lorsque les conditions reviennent au niveau Normal.

La valeur de déclenchement indiquée dans la notification d'un état d'alarme est arrondie à trois décimales. Par conséquent, une valeur d'attribut de 1.9999 déclenche une alarme dont le seuil est inférieur à (<) 2.0, bien que

la notification d'alarme indique la valeur de déclenchement comme 2.0.

Nouveaux services

Lorsque de nouveaux services sont ajoutés par l'ajout de nouveaux nœuds ou sites de grille, ils héritent des alarmes par défaut et des alarmes personnalisées globales.

Alarmes et tableaux

Les attributs d'alarme affichés dans les tableaux peuvent être désactivés au niveau du système. Les alarmes ne peuvent pas être désactivées pour les lignes individuelles d'une table.

Par exemple, le tableau suivant montre deux entrées critiques disponibles (VMFI) alarmes. (Sélectionnez **support** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***Storage Node*** > **SSM** > **Resources**.)

Vous pouvez désactiver l'alarme VMFI de sorte que l'alarme de niveau critique VMFI ne soit pas déclenchée (les deux alarmes critiques actuelles apparaîtront dans le tableau en vert) ; Cependant, vous ne pouvez pas désactiver une seule alarme dans une rangée de table de sorte qu'une alarme VMFI s'affiche comme une alarme de niveau critique alors que l'autre demeure verte.

Volumes

Mount Point	Device	Status	Size	Space Available	Total Entries	Entries Available	Write Cache
/	sda1	Online	10.6 GB	7.46 GB	655,360	559,263	Enabled
/var/local	sda3	Online	63.4 GB	59.4 GB	3,932,160	3,931,842	Unknown
/var/local/rangedb/0	sdb	Online	53.4 GB	53.4 GB	52,428,800	52,427,856	Enabled
/var/local/rangedb/1	sdc	Online	53.4 GB	53.4 GB	52,428,800	52,427,848	Enabled
/var/local/rangedb/2	sdd	Online	53.4 GB	53.4 GB	52,428,800	52,427,856	Enabled

Confirmation des alarmes actuelles (système hérité)

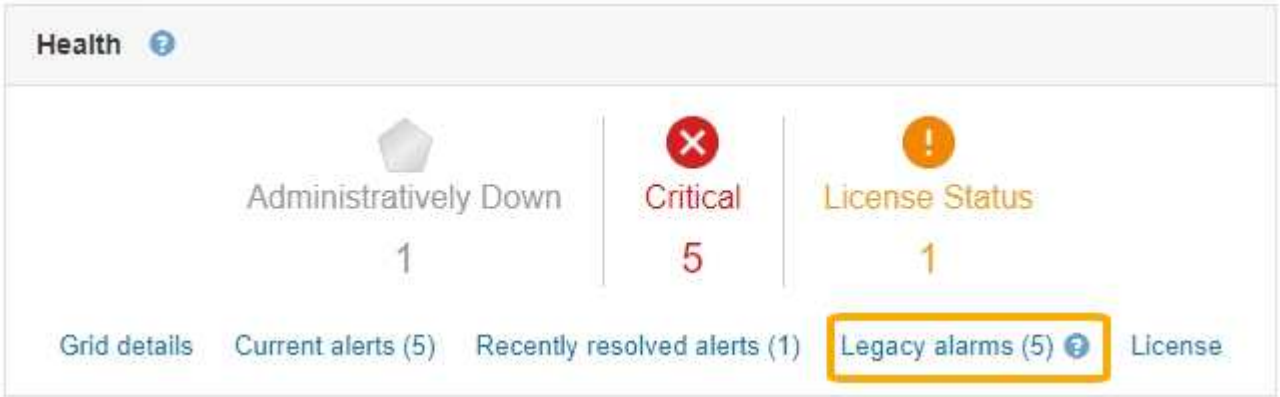
Les alarmes héritées sont déclenchées lorsque les attributs système atteignent les valeurs de seuil d'alarme. Si vous souhaitez réduire ou effacer le nombre d'alarmes héritées sur le tableau de bord, vous pouvez accuser réception des alarmes.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer de l'autorisation accuser réception d'alarmes.

Description de la tâche

Si une alarme du système hérité est actuellement active, le panneau Santé du tableau de bord inclut un lien **Legacy Alarms**. Le nombre entre parenthèses indique le nombre d'alarmes héritées actuellement actives.



Comme le système d'alarme hérité continue d'être pris en charge, le nombre d'alarmes héritées affichées sur le tableau de bord est incrémenté chaque fois qu'une nouvelle alarme se déclenche. Ce nombre est incrémenté même si les notifications par e-mail ne sont plus envoyées pour les alarmes. Vous pouvez généralement ignorer ce numéro (les alertes étant donné qu'elles offrent une meilleure vue du système), ou bien accuser réception des alarmes.

> En option, lorsque vous avez effectué une transition complète vers le système d'alerte, vous pouvez désactiver chaque alarme existante pour l'empêcher d'être déclenchée et ajoutée au nombre d'alarmes existantes.

Lorsque vous reconnaissez une alarme, elle n'est plus incluse dans le nombre d'alarmes héritées, sauf si l'alarme est déclenchée au niveau de gravité suivant ou si elle est résolue et se déclenche à nouveau.

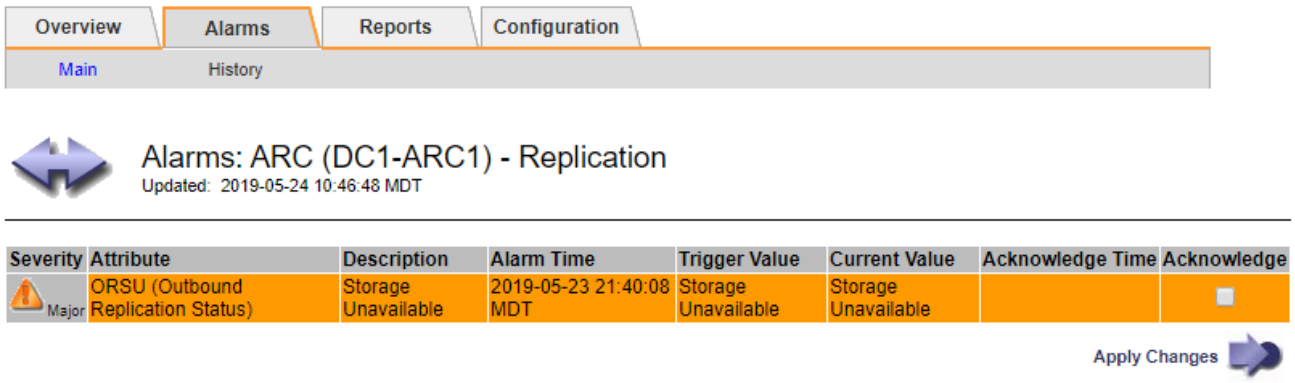
> Bien que le système d'alarme existant continue d'être pris en charge, le système d'alerte offre des avantages significatifs et est plus facile à utiliser.

Étapes

1. Pour afficher l'alarme, effectuez l'une des opérations suivantes :
   - Dans le panneau Santé du tableau de bord, cliquez sur **Legacy alarmes**. Ce lien n'apparaît que si au moins une alarme est active.
   - Sélectionnez **support** > **alarmes (hérité)** > **alarmes actuelles**. La page alarmes en cours s'affiche.

2. Cliquez sur le nom du service dans le tableau.

   L'onglet alarmes du service sélectionné apparaît (**support** > **Outils** > **topologie de grille** > ***Grid Node*** > ***Service*** > **alarmes**).



3. Cochez la case **Acknowledge** pour l'alarme, puis cliquez sur **appliquer les modifications**.

   L'alarme n'apparaît plus sur le tableau de bord ou sur la page alarmes en cours.

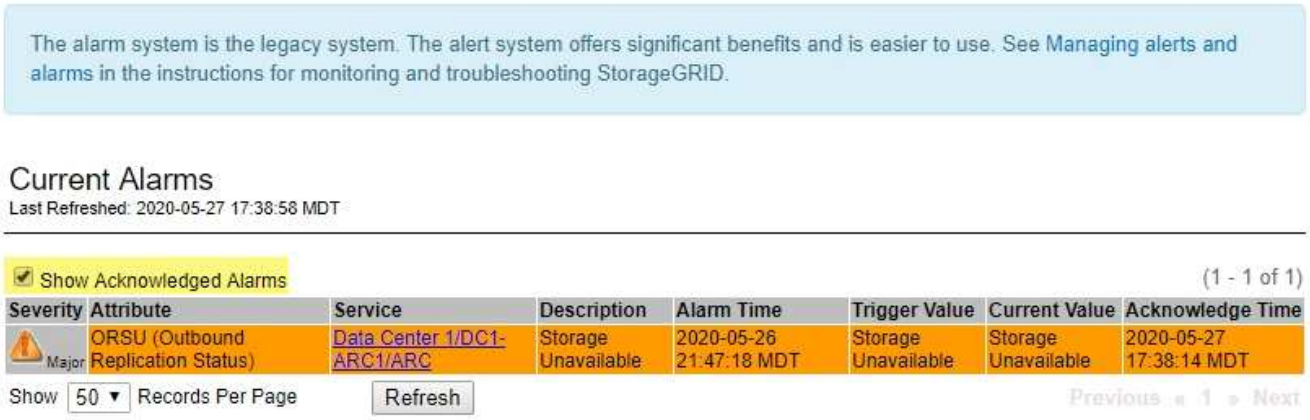
   > Lorsque vous reconnaissez une alarme, l'accusé de réception n'est pas copié sur d'autres nœuds d'administration. Par conséquent, si vous affichez le tableau de bord à partir d'un autre nœud d'administration, vous pouvez continuer à voir l'alarme active.

4. Si nécessaire, affichez les alarmes acquittées.

   a. Sélectionnez **support** > **alarmes (hérité)** > **alarmes actuelles**.

   b. Sélectionnez **Afficher les alarmes acquittées**.

      Toutes les alarmes acquittées sont affichées.



Informations associées

"Référence des alarmes (système hérité)"

Affichage des alarmes par défaut (système hérité)

Vous pouvez afficher la liste de toutes les alarmes héritées par défaut.

Ce dont vous avez besoin

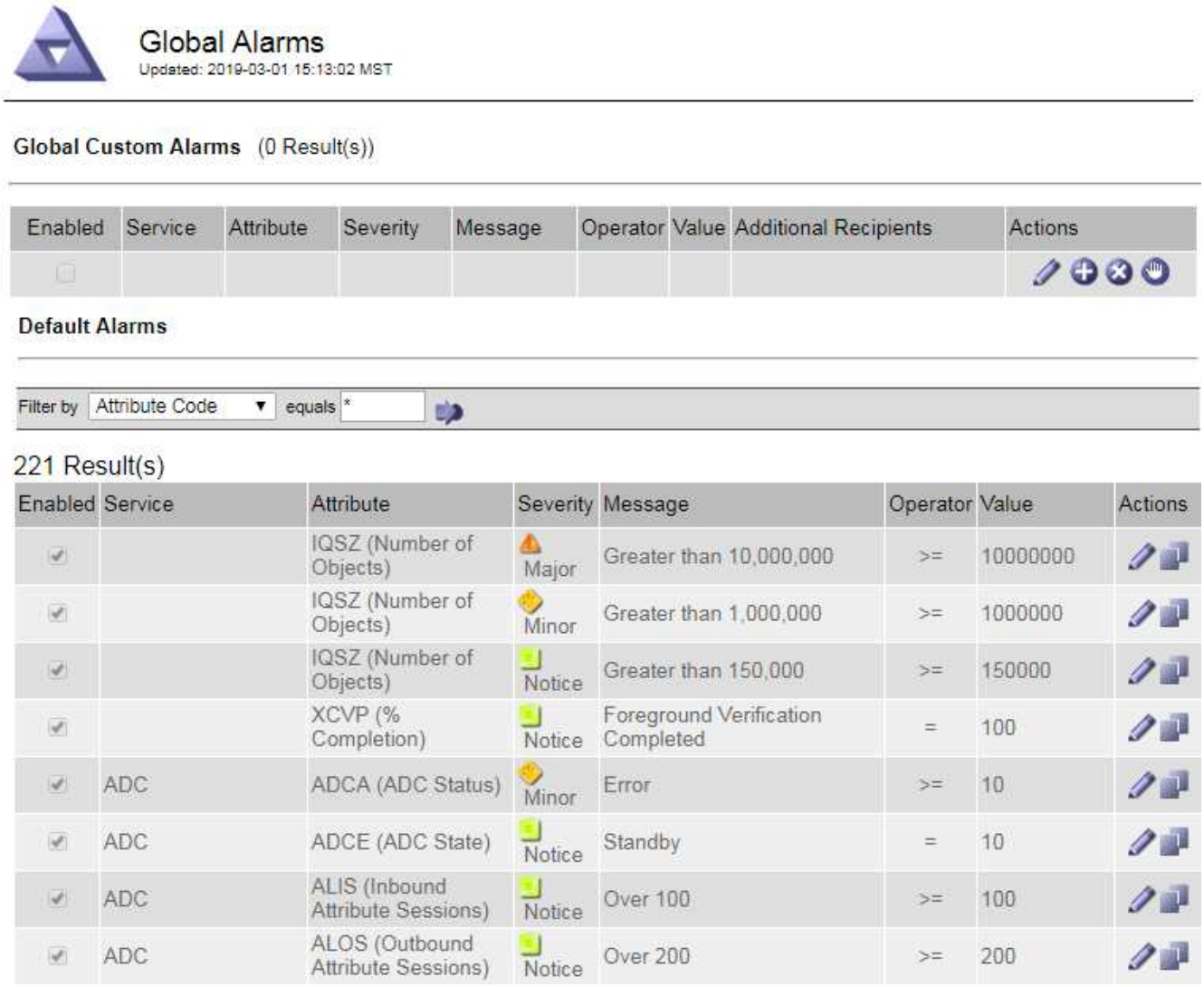
- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

> Bien que le système d'alarme existant continue d'être pris en charge, le système d'alerte offre des avantages significatifs et est plus facile à utiliser.

Étapes

1. Sélectionnez **support** > **alarmes (hérité)** > **alarmes globales**.
2. Pour Filtrer par, sélectionnez **Code d'attribut** ou **Nom d'attribut**.
3. Pour Egal, entrez un astérisque : *
4. Cliquez sur la flèche Ou appuyez sur **entrée**.

   Toutes les alarmes par défaut sont répertoriées.



Vérification des alarmes historiques et de la fréquence des alarmes (système hérité)

Lors du dépannage d'un problème, vous pouvez vérifier la fréquence à laquelle une alarme héritée a été déclenchée par le passé.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

> Bien que le système d'alarme existant continue d'être pris en charge, le système d'alerte offre des avantages significatifs et est plus facile à utiliser.

Étapes

1. Procédez comme suit pour obtenir une liste de toutes les alarmes déclenchées sur une période donnée.
   a. Sélectionnez **support** > **alarmes (hérité)** > **alarmes historiques**.
   b. Effectuez l'une des opérations suivantes :
      - Cliquez sur l'une des périodes.
      - Entrez une plage personnalisée, puis cliquez sur **requête personnalisée**.

2. Procédez comme suit pour découvrir la fréquence à laquelle les alarmes ont été déclenchées pour un attribut particulier.
   a. Sélectionnez **support** > **Outils** > **topologie de grille**.
   b. Sélectionnez ***grid node*** > ***service ou composant*** > **alarmes** > **Historique**.
   c. Sélectionnez l'attribut dans la liste.
   d. Effectuez l'une des opérations suivantes :
      - Cliquez sur l'une des périodes.
      - Entrez une plage personnalisée, puis cliquez sur **requête personnalisée**.

      Les alarmes sont répertoriées dans l'ordre chronologique inverse.
   e. Pour revenir au formulaire de demande d'historique des alarmes, cliquez sur **Historique**.

Informations associées

"Référence des alarmes (système hérité)"

Création d'alarmes personnalisées globales (système hérité)

Vous avez peut-être utilisé des alarmes personnalisées globales pour l'ancien système pour répondre à des exigences de surveillance spécifiques. Les alarmes personnalisées globales peuvent avoir des niveaux d'alarme qui remplacent les alarmes par défaut, ou elles peuvent surveiller des attributs qui n'ont pas d'alarme par défaut.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

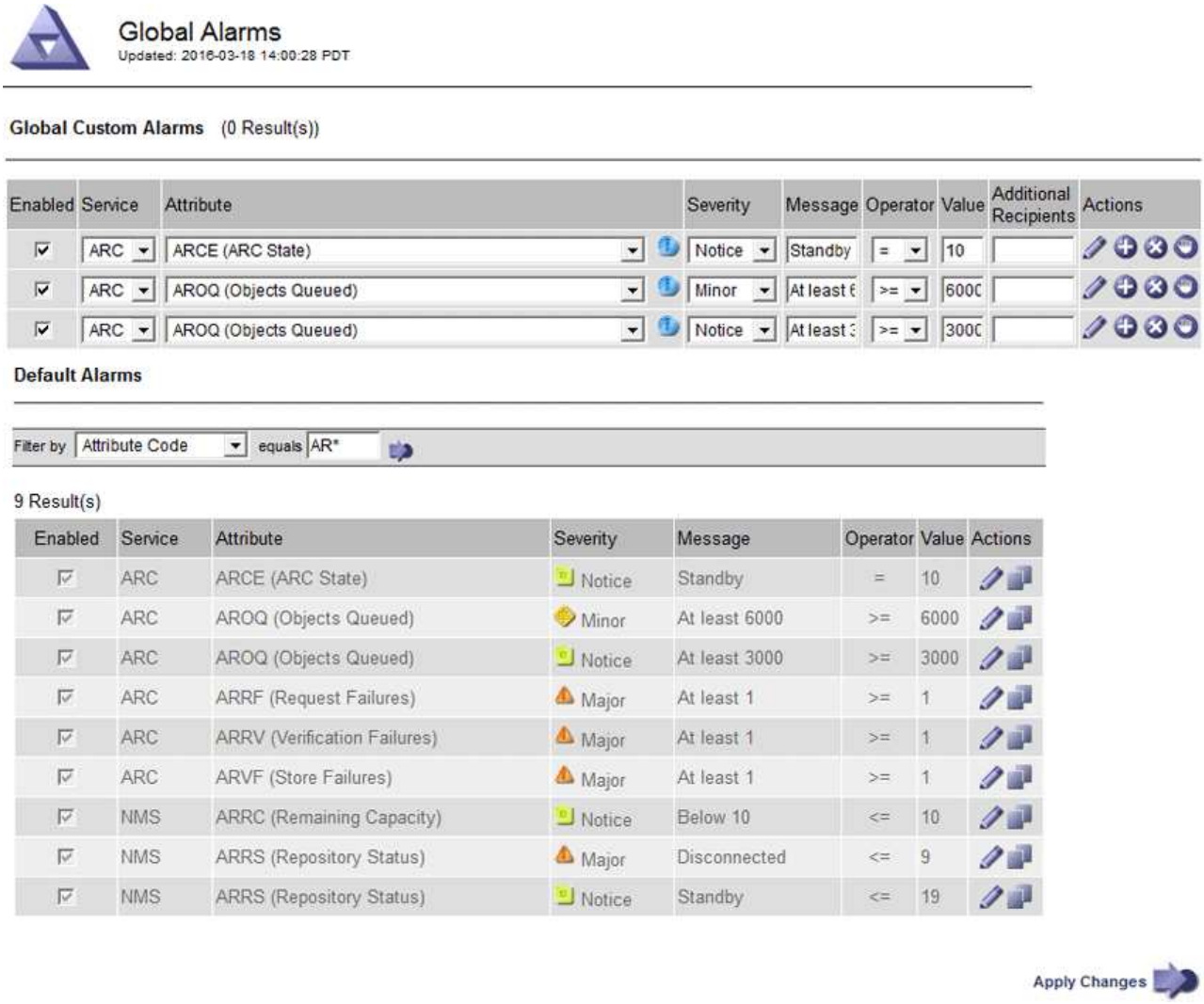
> Bien que le système d'alarme existant continue d'être pris en charge, le système d'alerte offre des avantages significatifs et est plus facile à utiliser.

Les alarmes personnalisées globales remplacent les alarmes par défaut. Vous ne devez pas modifier les valeurs d'alarme par défaut, sauf si cela est absolument nécessaire. En modifiant les alarmes par défaut, vous courez le risque de dissimulation de problèmes qui pourraient déclencher une alarme.

> Soyez très prudent si vous modifiez les paramètres d'alarme. Par exemple, si vous augmentez la valeur seuil d'une alarme, il se peut que vous ne déteciez pas un problème sous-jacent. Discutez de vos modifications proposées avec le support technique avant de modifier un réglage d'alarme.

Étapes

1. Sélectionnez **support** > **alarmes (hérité)** > **alarmes globales**.
2. Ajouter une nouvelle ligne au tableau des alarmes personnalisées globales :
   - Pour ajouter une nouvelle alarme, cliquez sur **Modifier** (S'il s'agit de la première entrée) ou **Insérer**.



- Pour modifier une alarme par défaut, recherchez l'alarme par défaut.
  i. Sous Filtrer par, sélectionnez **Code d'attribut** ou **Nom d'attribut**.
  ii. Saisissez une chaîne de recherche.

  Spécifiez quatre caractères ou utilisez des caractères génériques (Par exemple, Un ???? Ou AB*). Les astérisques (*) représentent plusieurs caractères et les points d'interrogation (?) représenter un seul caractère.

  iii. Cliquez sur la flèche , Ou appuyez sur **entrée**.
  iv. Dans la liste des résultats, cliquez sur **copie** en regard de l'alarme que vous souhaitez modifier.

  L'alarme par défaut est copiée dans le tableau des alarmes personnalisées globales.

3. Apportez toutes les modifications nécessaires aux paramètres d'alarmes personnalisées globales :

En-tête	Description
Activé	Cocher ou décocher la case pour activer ou désactiver l'alarme.

En-tête	Description
Attribut	Sélectionnez le nom et le code de l'attribut surveillé dans la liste de tous les attributs applicables au service ou au composant sélectionné. Pour afficher des informations sur l'attribut, cliquez sur **Info** à côté du nom de l'attribut.
Gravité	L'icône et le texte indiquant le niveau de l'alarme.
Messagerie	La raison de l'alarme (perte de connexion, espace de stockage inférieur à 10 %, etc.).
Opérateur	Opérateurs pour tester la valeur d'attribut actuelle par rapport au seuil de valeur : • = est égal à • > supérieur à • < moins de • >= supérieur ou égal à • <= inférieur ou égal à • ≠ non égal à
Valeur	Valeur de seuil de l'alarme utilisée pour tester la valeur réelle de l'attribut à l'aide de l'opérateur. L'entrée peut être un nombre unique, une plage de nombres spécifiée avec un signe deux-points (1:3) ou une liste de nombres et de plages délimitée par des virgules.
Destinataires supplémentaires	Une liste supplémentaire d'adresses e-mail à notifier lorsque l'alarme est déclenchée. Ceci s'ajoute à la liste de diffusion configurée sur la page **alarmes** > **Configuration de la messagerie**. Les listes sont délimitées par des virgules. **Remarque :** les listes de diffusion requièrent la configuration du serveur SMTP pour fonctionner. Avant d'ajouter des listes de diffusion, vérifiez que SMTP est configuré. Les notifications pour les alarmes personnalisées peuvent remplacer les notifications des alarmes Global Custom ou par défaut.
Actions	Boutons de commande pour : Modifier une ligne Insérer une ligne Supprimer une ligne Faites glisser une ligne vers le haut ou vers le bas Copier une ligne

4. Cliquez sur **appliquer les modifications**.

Informations associées

"Configuration des paramètres du serveur de messagerie pour les alarmes (système hérité)"

Désactivation des alarmes (système hérité)

Les alarmes du système d'alarme hérité sont activées par défaut, mais vous pouvez désactiver des alarmes qui ne sont pas nécessaires. Vous pouvez également désactiver les anciennes alarmes après avoir été complètement transférées vers le nouveau système d'alerte.

> Bien que le système d'alarme existant continue d'être pris en charge, le système d'alerte offre des avantages significatifs et est plus facile à utiliser.

Désactivation d'une alarme par défaut (système hérité)

Vous pouvez désactiver l'une des alarmes par défaut héritées pour l'ensemble du système.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

La désactivation d'une alarme pour un attribut qui a actuellement une alarme déclenchée n'efface pas l'alarme en cours. L'alarme sera désactivée lors du prochain dépassement du seuil d'alarme par l'attribut, ou vous pouvez effacer l'alarme déclenchée.

> Ne désactivez aucune des alarmes existantes tant que vous n'avez pas totalement migré vers le nouveau système d'alerte. Dans le cas contraire, vous risquez de ne pas détecter un problème sous-jacent avant d'empêcher la réalisation d'une opération critique.

Étapes

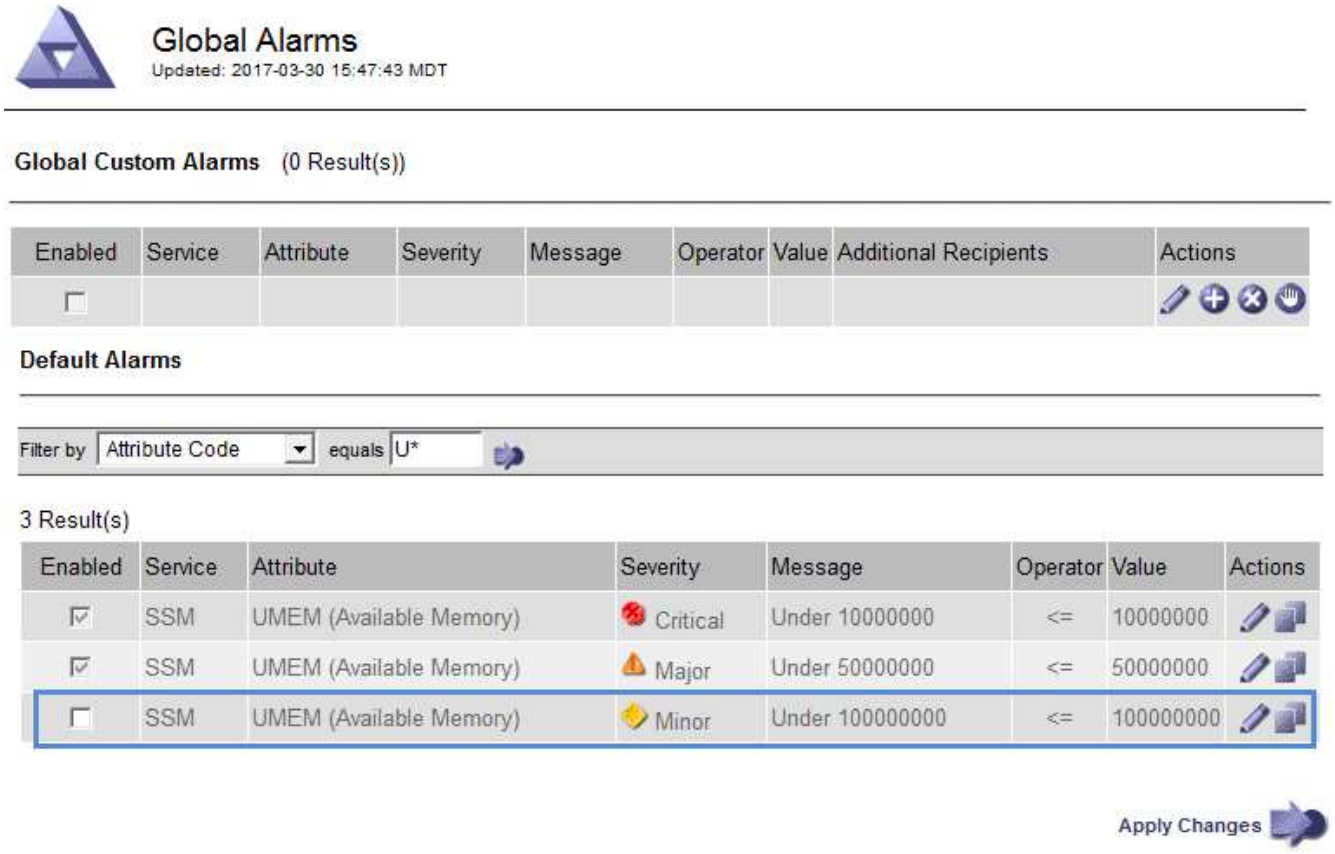
1. Sélectionnez **support** > **alarmes (hérité)** > **alarmes globales**.
2. Recherchez l'alarme par défaut à désactiver.
   a. Dans la section alarmes par défaut, sélectionnez **Filtrer par** > **Code d'attribut** ou **Nom d'attribut**.
   b. Saisissez une chaîne de recherche.

      Spécifiez quatre caractères ou utilisez des caractères génériques (Par exemple, Un ???? Ou AB*). Les astérisques (*) représentent plusieurs caractères et les points d'interrogation (?) représenter un seul caractère.

   c. Cliquez sur la flèche , Ou appuyez sur **entrée**.

      > La sélection de **Désactivé par défaut** affiche la liste de toutes les alarmes par défaut actuellement désactivées.

3. Dans le tableau des résultats de la recherche, cliquez sur l'icône Modifier pour l'alarme que vous souhaitez désactiver.



La case **Enabled** pour l'alarme sélectionnée devient active.

4. Décochez la case **Enabled**.
5. Cliquez sur **appliquer les modifications**.

   L'alarme par défaut est désactivée.

Désactivation des alarmes personnalisées globales (système hérité)

Vous pouvez désactiver une alarme personnalisée globale héritée pour l'ensemble du système.

Ce dont vous avez besoin

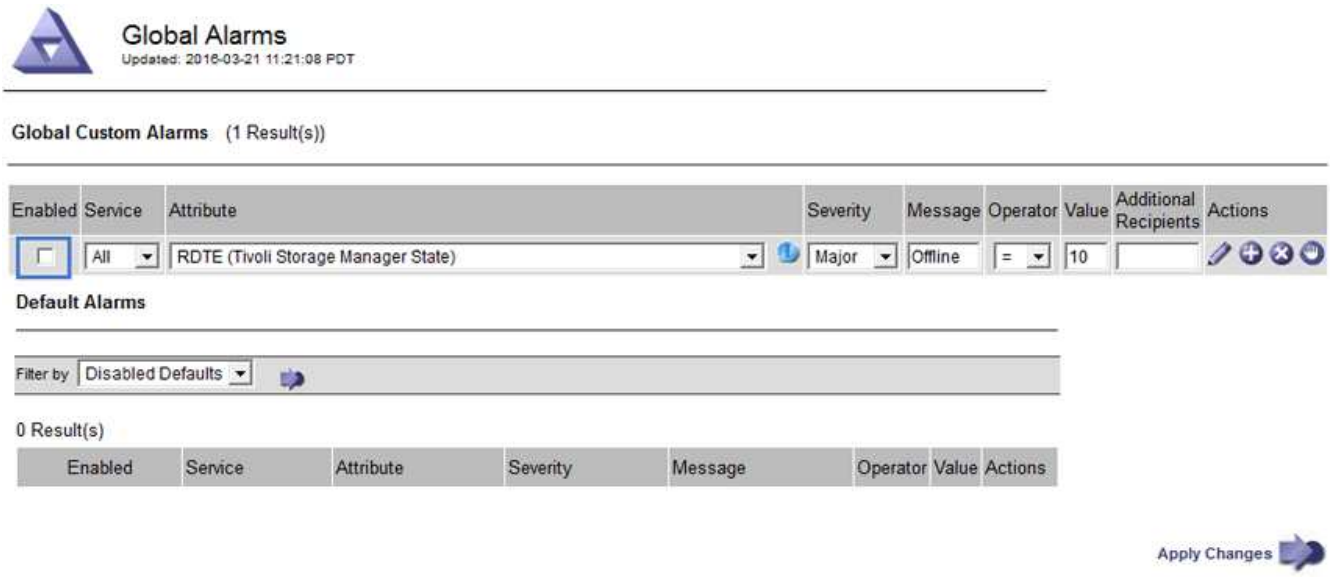
- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

La désactivation d'une alarme pour un attribut qui a actuellement une alarme déclenchée n'efface pas l'alarme en cours. L'alarme sera désactivée lors du prochain dépassement du seuil d'alarme par l'attribut, ou vous pouvez effacer l'alarme déclenchée.

Étapes

1. Sélectionnez **support** > **alarmes (hérité)** > **alarmes globales**.
2. Dans le tableau alarmes personnalisées globales, cliquez sur **Modifier** à côté de l'alarme que vous souhaitez désactiver.
3. Décochez la case **Enabled**.



4. Cliquez sur **appliquer les modifications**.

   L'alarme personnalisée globale est désactivée.

Suppression des alarmes déclenchées (système hérité)

Si une alarme héritée est déclenchée, vous pouvez l'effacer au lieu de la reconnaître.

Ce dont vous avez besoin

- Vous devez avoir le `Passwords.txt` fichier.

La désactivation d'une alarme pour un attribut qui a actuellement une alarme déclenchée contre elle n'efface pas l'alarme. L'alarme sera désactivée lors de la prochaine modification de l'attribut. Vous pouvez accuser réception de l'alarme ou, si vous voulez effacer immédiatement l'alarme plutôt que d'attendre que la valeur de l'attribut change (ce qui entraîne un changement de l'état d'alarme), vous pouvez effacer l'alarme déclenchée. Vous pouvez trouver ceci utile si vous voulez effacer une alarme immédiatement contre un attribut dont la valeur ne change pas souvent (par exemple, les attributs d'état).

1. Désactivez l'alarme.
2. Connectez-vous au nœud d'administration principal :
   a. Saisissez la commande suivante : *`ssh admin@primary_Admin_Node_IP`*
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

      Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.
3. Redémarrez le service NMS : `service nms restart`
4. Déconnectez-vous du nœud d'administration : `exit`

   L'alarme est effacée.

Informations associées

"Désactivation des alarmes (système hérité)"

Configuration des notifications pour les alarmes (système hérité)

Le système StorageGRID peut envoyer automatiquement des notifications par e-mail et SNMP lorsqu'une alarme est déclenchée ou qu'un état de service change.

Par défaut, les notifications par e-mail d'alarme ne sont pas envoyées. Pour les notifications par e-mail, vous devez configurer le serveur de messagerie et spécifier les destinataires. Pour les notifications SNMP, vous devez configurer l'agent SNMP.

Informations associées

"Utilisation de la surveillance SNMP"

Types de notifications d'alarme (système hérité)

Lorsqu'une alarme héritée est déclenchée, le système StorageGRID envoie deux types de notifications d'alarme : le niveau de gravité et l'état de service.

Notifications de niveau de gravité

Une notification par e-mail d'alarme est envoyée lorsqu'une alarme héritée est déclenchée à un niveau de gravité sélectionné :

- Avertissement
- Mineur
- Majeur
- Primordial

Une liste de diffusion reçoit toutes les notifications relatives à l'alarme pour la gravité sélectionnée. Une notification est également envoyée lorsque l'alarme quitte le niveau d'alarme — soit en étant résolue soit en entrant un niveau de gravité d'alarme différent.

Notifications d'état de service

Une notification d'état de service est envoyée lorsqu'un service (par exemple, le service LDR ou le service NMS) entre dans l'état de service sélectionné et lorsqu'il quitte l'état de service sélectionné. Des notifications d'état de service sont envoyées lorsqu'un service entre ou quitte l'un des États de service suivants :

- Inconnu
- Arrêt administratif

Une liste de diffusion reçoit toutes les notifications associées aux modifications de l'état sélectionné.

Informations associées

"Configuration des notifications par e-mail pour les alarmes (système hérité)"

Configuration des paramètres du serveur de messagerie pour les alarmes (système hérité)

Si vous souhaitez que StorageGRID envoie des notifications par e-mail lorsqu'une alarme héritée est déclenchée, vous devez spécifier les paramètres du serveur de messagerie SMTP. Le système StorageGRID

envoie uniquement des e-mails. Il ne peut pas recevoir d'e-mails.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

Utilisez ces paramètres pour définir le serveur SMTP utilisé pour les notifications par e-mail d'alarme et les e-mails AutoSupport hérités. Ces paramètres ne sont pas utilisés pour les notifications d'alerte.

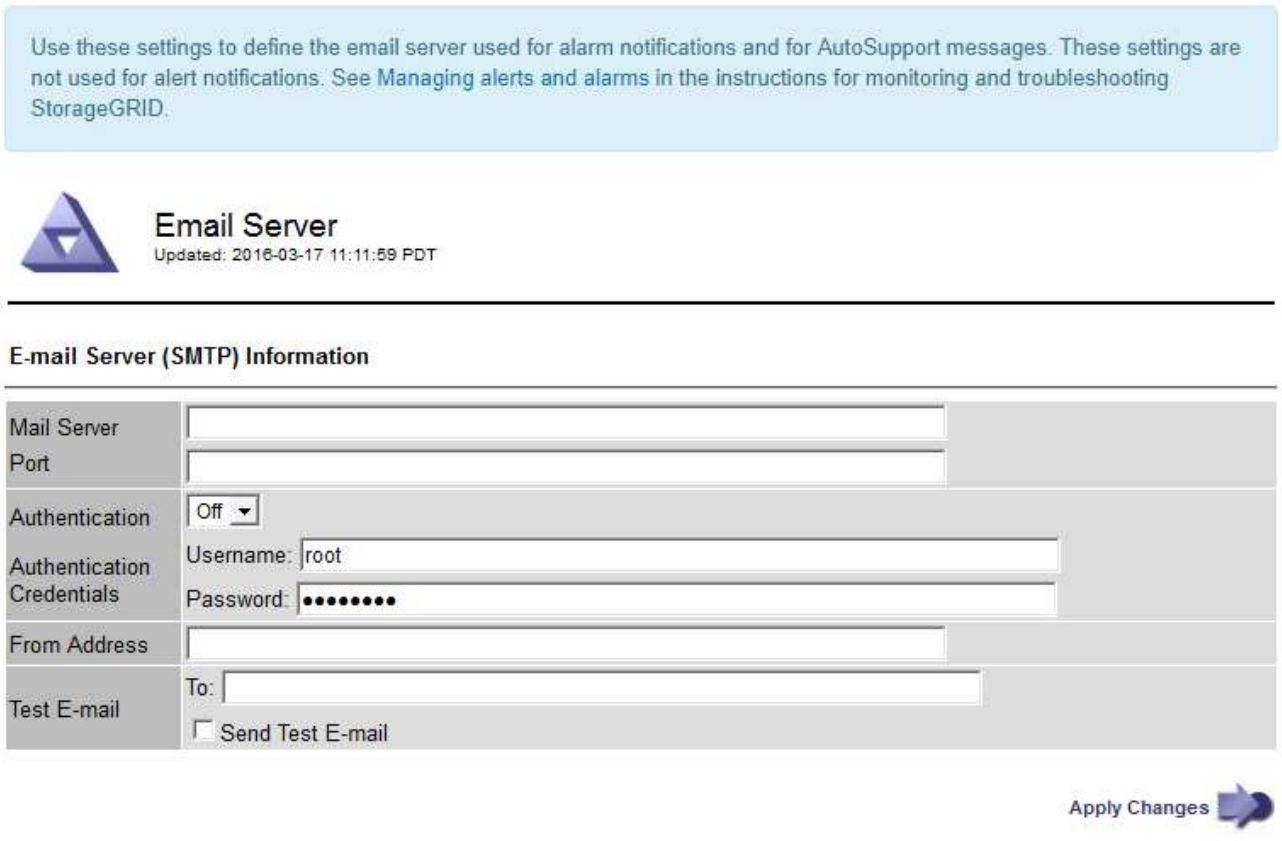
> Si vous utilisez SMTP comme protocole pour les messages AutoSupport, vous avez peut-être déjà configuré un serveur de messagerie SMTP. Le même serveur SMTP est utilisé pour les notifications par e-mail d'alarme. Vous pouvez donc ignorer cette procédure. Voir les instructions d'administration de StorageGRID.

SMTP est le seul protocole pris en charge pour l'envoi d'e-mails.

Étapes

1. Sélectionnez **support** > **alarmes (hérité)** > **Configuration des e-mails existants**.
2. Dans le menu E-mail, sélectionnez **serveur**.

   La page serveur de messagerie s'affiche. Cette page est également utilisée pour configurer le serveur de messagerie pour les messages AutoSupport.



3. Ajoutez les paramètres suivants du serveur de messagerie SMTP :

Élément	Description
Serveur de messagerie	Adresse IP du serveur de messagerie SMTP. Vous pouvez entrer un nom d'hôte plutôt qu'une adresse IP si vous avez déjà configuré les paramètres DNS sur le noeud d'administration.
Port	Numéro de port pour accéder au serveur de messagerie SMTP.
Authentification	Permet l'authentification du serveur de messagerie SMTP. Par défaut, l'authentification est désactivée.
Informations d'authentification	Nom d'utilisateur et mot de passe du serveur de messagerie SMTP. Si l'authentification est activée, un nom d'utilisateur et un mot de passe doivent être fournis pour accéder au serveur de messagerie SMTP.

4. Sous **de adresse**, entrez une adresse e-mail valide que le serveur SMTP reconnaîtra comme adresse e-mail d'envoi. Il s'agit de l'adresse électronique officielle à partir de laquelle l'e-mail est envoyé.
5. Vous pouvez également envoyer un e-mail de test pour confirmer que les paramètres de votre serveur de messagerie SMTP sont corrects.
   a. Dans la zone **Test E-mail** > **à**, ajoutez une ou plusieurs adresses auxquelles vous pouvez accéder.

      Vous pouvez entrer une seule adresse e-mail ou une liste d'adresses e-mail délimitée par des virgules. Comme le service NMS ne confirme pas le succès ou l'échec lors de l'envoi d'un e-mail de test, vous devez être en mesure de vérifier la boîte de réception du destinataire du test.

   b. Sélectionnez **Envoyer E-mail test**.
6. Cliquez sur **appliquer les modifications**.

   Les paramètres du serveur de messagerie SMTP sont enregistrés. Si vous avez saisi des informations pour un e-mail de test, cet e-mail est envoyé. Les e-mails de test sont immédiatement envoyés au serveur de messagerie et ne sont pas envoyés via la file d'attente de notifications. Dans un système avec plusieurs nœuds d'administration, chaque nœud d'administration envoie un e-mail. La réception de l'e-mail de test confirme que les paramètres de votre serveur de messagerie SMTP sont corrects et que le service NMS se connecte avec succès au serveur de messagerie. Un problème de connexion entre le service NMS et le serveur de messagerie déclenche l'alarme DES MINUTES héritées (état de notification NMS) au niveau de gravité mineure.

Informations associées

"Administrer StorageGRID"

Création de modèles d'e-mails d'alarme (système hérité)

Les modèles de courrier électronique vous permettent de personnaliser l'en-tête, le pied de page et l'objet d'une notification d'alarme existante. Vous pouvez utiliser des modèles d'e-mails pour envoyer des notifications uniques contenant le même corps de texte à différentes listes de diffusion.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

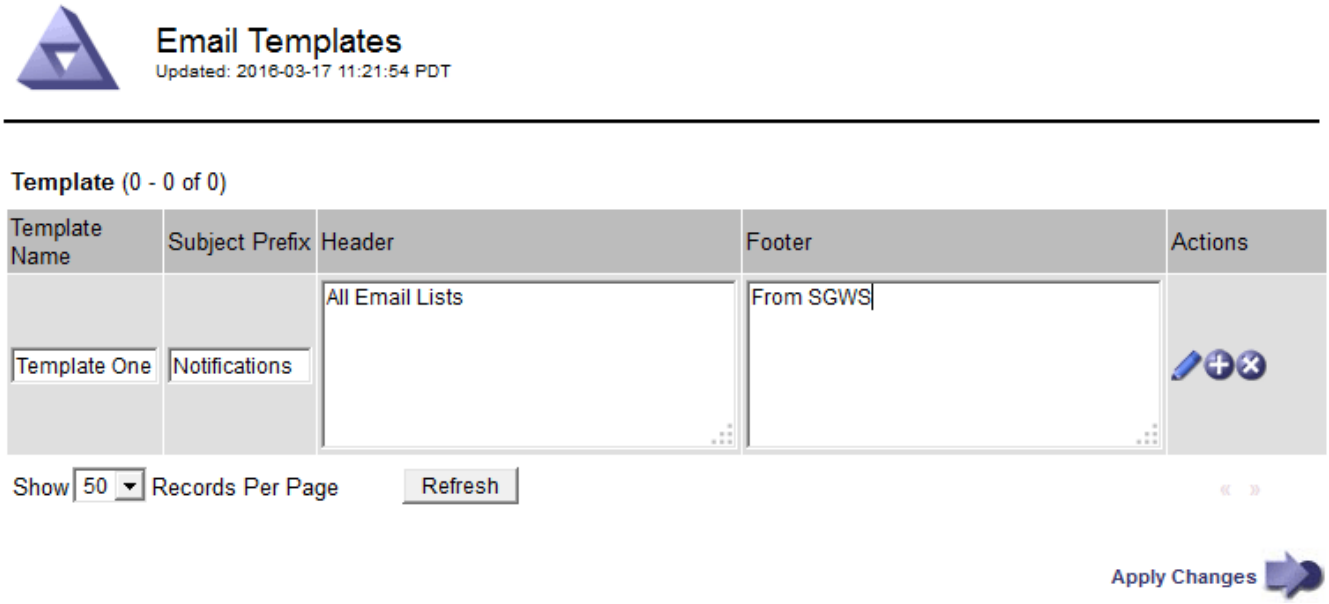
Description de la tâche

Utilisez ces paramètres pour définir les modèles d'e-mails utilisés pour les notifications d'alarme héritées. Ces paramètres ne sont pas utilisés pour les notifications d'alerte.

Différentes listes de diffusion peuvent nécessiter des informations de contact différentes. Les modèles n'incluent pas le corps du message électronique.

Étapes

1. Sélectionnez **support** > **alarmes (hérité)** > **Configuration des e-mails existants**.
2. Dans le menu E-mail, sélectionnez **modèles**.
3. Cliquez sur **Modifier*** **(Ou *Insérer** s'il ne s'agit pas du premier modèle).



4. Dans la nouvelle ligne, ajoutez ce qui suit :

Élément	Description
Nom du modèle	Nom unique utilisé pour identifier le modèle. Les noms de modèles ne peuvent pas être dupliqués.
Préfixe de l'objet	Facultatif. Préfixe qui apparaîtra au début de la ligne d'objet d'un e-mail. Les préfixes peuvent être utilisés pour configurer facilement les filtres d'e-mail et organiser les notifications.
En-tête	Facultatif. Texte d'en-tête qui apparaît au début du corps du message électronique. Le texte d'en-tête peut être utilisé pour prégérer le contenu de l'e-mail avec des informations telles que le nom et l'adresse de l'entreprise.

Élément	Description
Pied de page	Facultatif. Texte de pied de page qui apparaît à la fin du corps de l'e-mail. Le texte du pied de page peut être utilisé pour fermer l'e-mail avec des informations de rappel telles qu'un numéro de téléphone de contact ou un lien vers un site Web.

5. Cliquez sur **appliquer les modifications**.

   Un nouveau modèle pour les notifications est ajouté.

Création de listes de diffusion pour les notifications d'alarme (système hérité)

Les listes de diffusion vous permettent d'avertir les destinataires lorsqu'une alarme héritée est déclenchée ou lorsqu'un état de service change. Vous devez créer au moins une liste de diffusion pour pouvoir envoyer des notifications par e-mail d'alarme. Pour envoyer une notification à un seul destinataire, créez une liste de diffusion avec une adresse e-mail.

Ce dont vous avez besoin

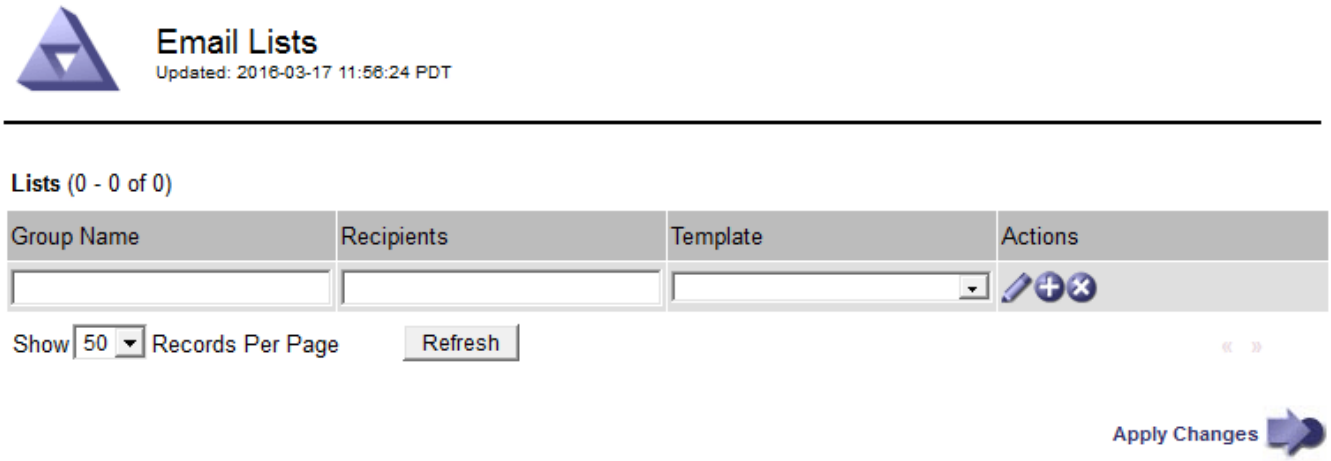
- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.
- Si vous souhaitez spécifier un modèle de courrier électronique pour la liste de diffusion (en-tête personnalisé, pied de page et ligne d'objet), vous devez avoir déjà créé le modèle.

Description de la tâche

Utilisez ces paramètres pour définir les listes de diffusion utilisées pour les notifications par e-mail d'alarme héritées. Ces paramètres ne sont pas utilisés pour les notifications d'alerte.

Étapes

1. Sélectionnez **support** > **alarmes (hérité)** > **Configuration des e-mails existants**.
2. Dans le menu E-mail, sélectionnez **listes**.
3. Cliquez sur **Modifier** (Ou **Insérer** s'il ne s'agit pas de la première liste de diffusion).



4. Dans la nouvelle ligne, ajoutez les éléments suivants :

Élément	Description
Nom du groupe	Nom unique utilisé pour identifier la liste de diffusion. Les noms de listes de diffusion ne peuvent pas être dupliqués. **Remarque :** si vous modifiez le nom d'une liste de diffusion, le changement n'est pas propagé aux autres emplacements qui utilisent le nom de la liste de diffusion. Vous devez mettre à jour manuellement toutes les notifications configurées pour utiliser le nouveau nom de liste de diffusion.
Destinataires	Une seule adresse e-mail, une liste de diffusion précédemment configurée ou une liste délimitée par des virgules d'adresses e-mail et de listes de diffusion auxquelles les notifications seront envoyées. **Remarque :** si une adresse e-mail appartient à plusieurs listes de diffusion, une seule notification par e-mail est envoyée lorsqu'un événement de déclenchement de notification se produit.
Modèle	Vous pouvez également sélectionner un modèle de courrier électronique pour ajouter un en-tête, un pied de page et une ligne d'objet uniques aux notifications envoyées à tous les destinataires de cette liste de diffusion.

5. Cliquez sur **appliquer les modifications**.

   Une nouvelle liste de diffusion est créée.

Informations associées

"Création de modèles d'e-mails d'alarme (système hérité)"

Configuration des notifications par e-mail pour les alarmes (système hérité)

Pour recevoir des notifications par e-mail pour le système d'alarme existant, les destinataires doivent être membres d'une liste de diffusion et cette liste doit être ajoutée à la page Notifications. Les notifications sont configurées pour envoyer des e-mails aux destinataires uniquement lorsqu'une alarme avec un niveau de gravité spécifié est déclenchée ou lorsqu'un état de service change. Ainsi, les destinataires ne reçoivent que les notifications dont ils ont besoin.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.
- Vous devez avoir configuré une liste d'e-mails.

Description de la tâche

Utilisez ces paramètres pour configurer les notifications pour les alarmes héritées. Ces paramètres ne sont pas utilisés pour les notifications d'alerte.

Si une adresse e-mail (ou une liste) appartient à plusieurs listes de diffusion, une seule notification par e-mail est envoyée lorsqu'un événement de déclenchement de notification se produit. Par exemple, un groupe d'administrateurs au sein de votre organisation peut être configuré pour recevoir des notifications pour toutes les alarmes, quelle que soit leur gravité. Un autre groupe peut uniquement exiger des notifications pour les alarmes dont la gravité est critique. Vous pouvez appartenir aux deux listes. Si une alarme critique est déclenchée, vous ne recevez qu'une seule notification.

Étapes

1. Sélectionnez **support** > **alarmes (hérité)** > **Configuration des e-mails existants**.
2. Dans le menu E-mail, sélectionnez **Notifications**.
3. Cliquez sur **Modifier** (Ou **Insérer** s'il ne s'agit pas de la première notification).
4. Sous liste de courrier électronique, sélectionnez la liste de diffusion.
5. Sélectionnez un ou plusieurs niveaux de gravité d'alarme et États de service.
6. Cliquez sur **appliquer les modifications**.

   Des notifications sont envoyées à la liste de diffusion lorsque des alarmes avec le niveau de gravité d'alarme ou l'état de service sélectionné sont déclenchées ou modifiées.

Informations associées

"Création de listes de diffusion pour les notifications d'alarme (système hérité)"

"Types de notifications d'alarme (système hérité)"

Suppression des notifications d'alarme pour une liste de diffusion (système existant)

Vous pouvez supprimer les notifications d'alarme pour une liste de diffusion lorsque vous ne souhaitez plus que la liste de diffusion reçoive des notifications relatives aux alarmes. Par exemple, vous pouvez supprimer les notifications relatives aux alarmes existantes après avoir été passé à l'aide des notifications par e-mail d'alerte.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

Utilisez ces paramètres pour supprimer les notifications par e-mail pour l'ancien système d'alarme. Ces paramètres ne s'appliquent pas aux notifications par e-mail d'alerte.

> Bien que le système d'alarme existant continue d'être pris en charge, le système d'alerte offre des avantages significatifs et est plus facile à utiliser.

Étapes

1. Sélectionnez **support** > **alarmes (hérité)** > **Configuration des e-mails existants**.
2. Dans le menu E-mail, sélectionnez **Notifications**.
3. Cliquez sur **Modifier** en regard de la liste de diffusion pour laquelle vous souhaitez supprimer les notifications.
4. Sous Supprimer, cochez la case en regard de la liste de diffusion que vous souhaitez supprimer ou

sélectionnez **Supprimer** en haut de la colonne pour supprimer toutes les listes de diffusion.

5. Cliquez sur **appliquer les modifications**.

   Les notifications d'alarme héritées sont supprimées pour les listes d'envoi sélectionnées.

Suppression des notifications par e-mail à l'échelle du système

Vous pouvez bloquer la capacité du système StorageGRID à envoyer des notifications par e-mail pour les alarmes héritées et les messages AutoSupport déclenchés par des événements.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

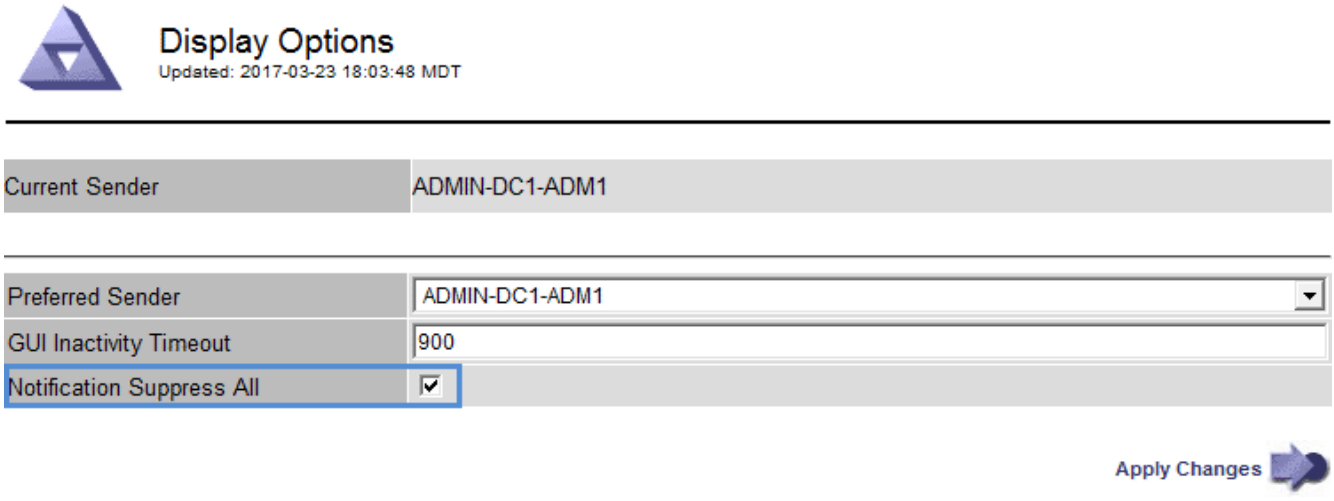
Description de la tâche

Utilisez cette option pour supprimer les notifications par e-mail pour les alarmes héritées et les messages AutoSupport déclenchés par des événements.

> Cette option ne supprime pas les notifications par e-mail d'alerte. Elle ne supprime pas non plus les messages AutoSupport hebdomadaires ou déclenchés par l'utilisateur.

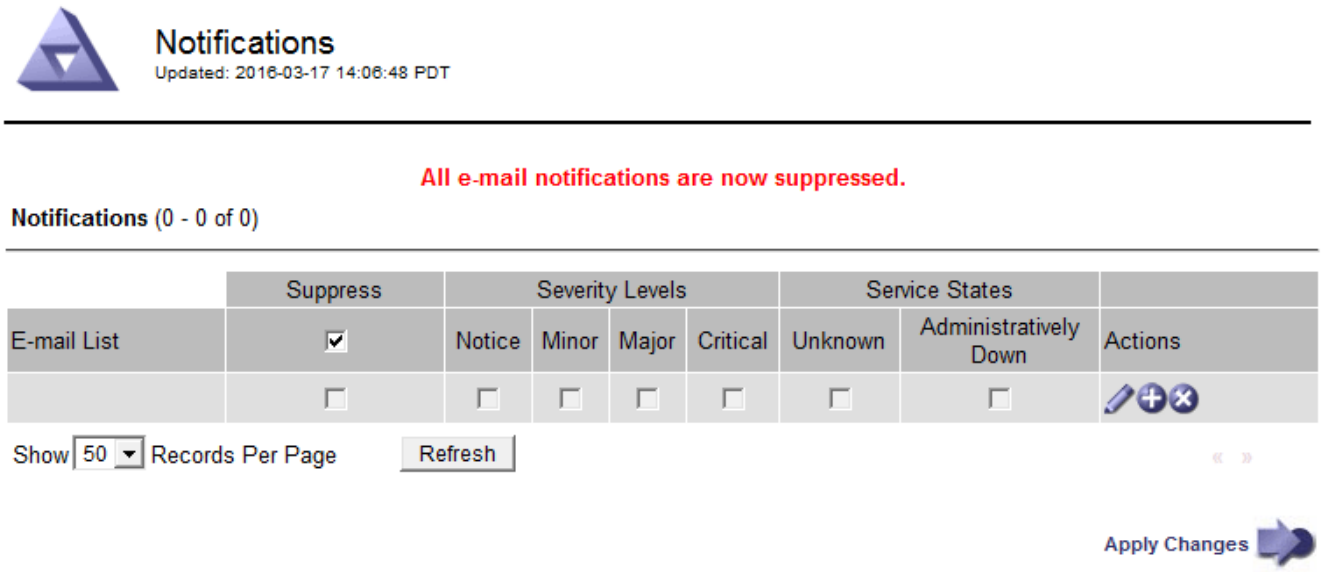
Étapes

1. Sélectionnez **Configuration** > **Paramètres système** > **Options d'affichage**.
2. Dans le menu Options d'affichage, sélectionnez **Options**.
3. Sélectionnez **Supprimer toutes les notifications**.



4. Cliquez sur **appliquer les modifications**.

   La page Notifications (**Configuration** > **Notifications**) affiche le message suivant :



Informations associées

"Administrer StorageGRID"

Utilisation de 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.

- "Configuration de l'agent SNMP"
- "Mise à jour de l'agent SNMP"

Capacités

Chaque nœud StorageGRID exécute un agent SNMP, ou un démon, qui fournit une base d'informations de gestion (MIB). La MIB StorageGRID contient des définitions de tableau et de notification pour les alertes et les alarmes. La base MIB contient également des informations de description du système, telles que la plateforme et le numéro de modèle pour chaque nœud. Chaque nœud StorageGRID supporte également un sous-ensemble d'objets MIB-II.

Au départ, le protocole SNMP est désactivé sur tous les nœuds. Lorsque vous configurez l'agent SNMP, tous les nœuds StorageGRID reçoivent la même configuration.

L'agent SNMP StorageGRID prend en charge les trois versions du protocole SNMP. Il fournit un accès MIB en lecture seule pour les requêtes et il peut envoyer deux types de notifications événementielle à un système de gestion :

- **Les traps** sont des notifications envoyées par l'agent SNMP qui ne nécessitent pas d'accusé de réception par le système de gestion. Les interruptions servent à signaler au système de gestion qu'une alerte s'est produite au sein de StorageGRID, par exemple.

  Les traps sont pris en charge dans les trois versions de SNMP.

- **Inform** sont similaires aux pièges, mais ils exigent une reconnaissance du système de gestion. Si l'agent SNMP ne reçoit pas d'accusé de réception dans un certain temps, il renvoie l'information jusqu'à ce qu'un accusé de réception soit reçu ou que la valeur de nouvelle tentative maximale ait été atteinte.

Les informations sont prises en charge dans SNMPv2c et SNMPv3.

Les notifications d'interruption et d'information sont envoyées dans les cas suivants :

- Une alerte par défaut ou personnalisée est déclenchée à tout niveau de gravité. Pour supprimer les notifications SNMP pour une alerte, vous devez configurer un silence pour l'alerte. Les notifications d'alerte sont envoyées par n'importe quel nœud d'administration configuré pour être l'expéditeur préféré.
- Certaines alarmes (système hérité) sont déclenchées à des niveaux de gravité spécifiés ou plus.

> Les notifications SNMP ne sont pas envoyées pour chaque alarme ou chaque gravité d'alarme.

Prise en charge de la version SNMP

Le tableau fournit un résumé détaillé des éléments pris en charge pour chaque version de SNMP.

	SNMPv1	SNMPv2c	SNMPv3
Requêtes	Requêtes MIB en lecture seule	Requêtes MIB en lecture seule	Requêtes MIB en lecture seule
Authentification par requête	Chaîne de communauté	Chaîne de communauté	Utilisateur USM (User Security Model)
Notifications	Traps uniquement	Pièges et information	Pièges et information
Authentification des notifications	Communauté d'interruptions par défaut ou chaîne de communauté personnalisée pour chaque destination d'interruption	Communauté d'interruptions par défaut ou chaîne de communauté personnalisée pour chaque destination d'interruption	Utilisateur USM pour chaque destination d'interruption

Limites

- StorageGRID supporte l'accès MIB en lecture seule. L'accès en lecture/écriture n'est pas pris en charge.
- Tous les nœuds de la grille reçoivent la même configuration.
- SNMPv3 : StorageGRID ne prend pas en charge le mode support transport (TSM).
- SNMPv3 : le seul protocole d'authentification pris en charge est SHA (HMAC-SHA-96).
- SNMPv3 : le seul protocole de confidentialité pris en charge est AES.

Accès à la MIB

Vous pouvez accéder au fichier de définition MIB à l'emplacement suivant sur n'importe quel nœud StorageGRID :

/Usr/share/snmp/mibs/NETAPP-STORAGEGRID-MIB.txt

Informations associées

"Référence des alertes"

"Référence des alarmes (système hérité)"

"Alarmes générant des notifications SNMP (système hérité)"

"Neutralisation des notifications d'alerte"

Configuration de l'agent SNMP

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

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer de l'autorisation accès racine.

Description de la tâche

L'agent SNMP StorageGRID prend en charge les trois versions du protocole SNMP. Vous pouvez configurer l'agent pour une ou plusieurs versions.

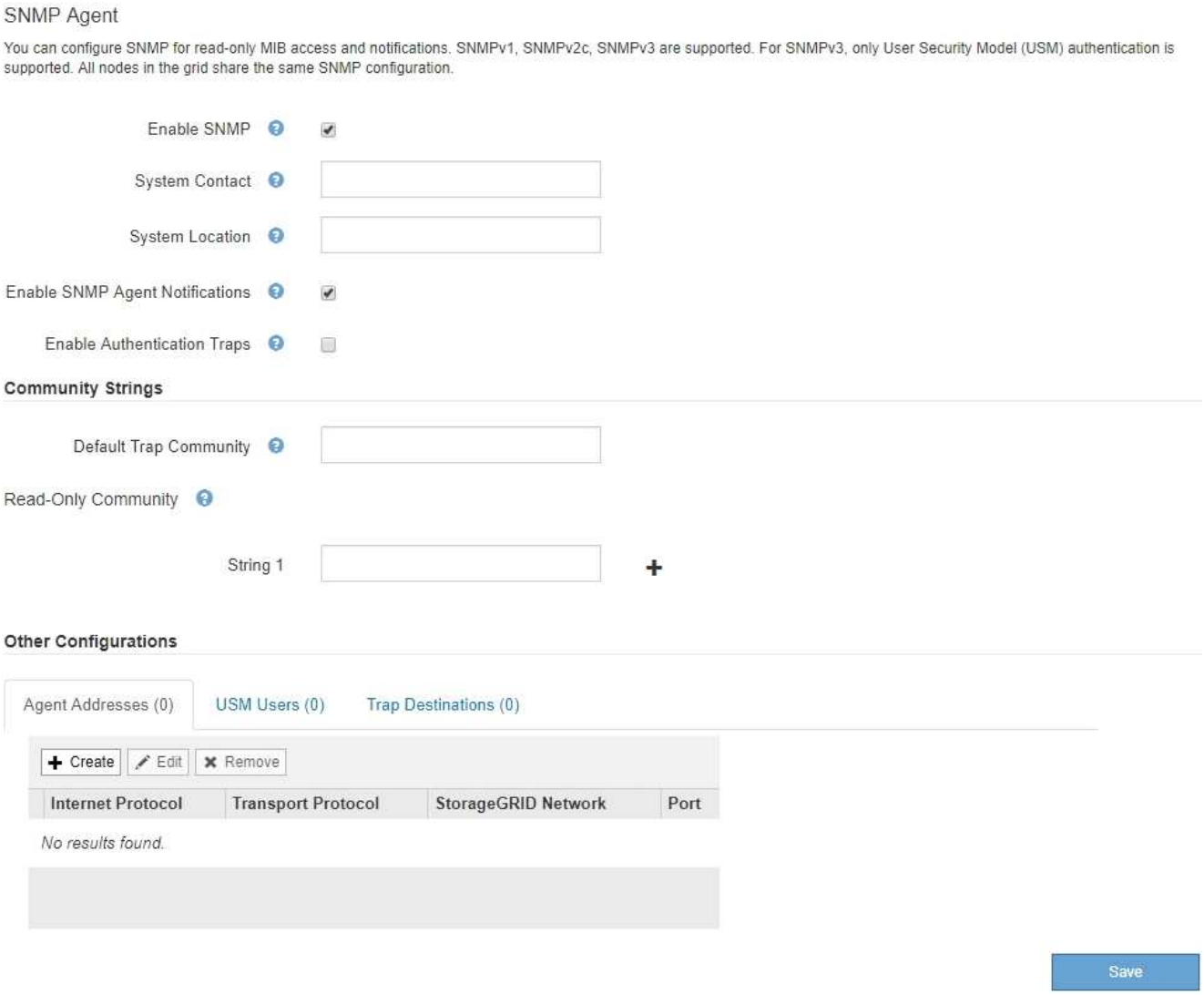
Étapes

1. Sélectionnez **Configuration** > **surveillance** > **agent SNMP**.

   La page agent SNMP s'affiche.

2. Pour activer l'agent SNMP sur tous les nœuds de la grille, cochez la case **Activer SNMP**.

   Les champs de configuration d'un agent SNMP s'affichent.



3. Dans le champ **Contact système**, entrez la valeur que vous souhaitez que StorageGRID vous apporte dans les messages SNMP pour sysContact.

   Le contact système est généralement une adresse e-mail. La valeur indiquée s'applique à tous les nœuds du système StorageGRID. **Contact système** peut comporter un maximum de 255 caractères.

4. Dans le champ **emplacement du système**, entrez la valeur que vous souhaitez que StorageGRID vous apporte dans les messages SNMP pour sysLocation.

   L'emplacement du système peut être toute information utile pour identifier l'emplacement de votre système StorageGRID. Par exemple, vous pouvez utiliser l'adresse d'un établissement. La valeur indiquée s'applique à tous les nœuds du système StorageGRID. **Emplacement du système** peut comporter un maximum de 255 caractères.

5. Cochez la case **Activer les notifications d'agent SNMP** si vous souhaitez que l'agent SNMP StorageGRID envoie des notifications d'interruption et informe les notifications.

   Si cette case n'est pas cochée, l'agent SNMP prend en charge l'accès MIB en lecture seule, mais il n'envoie pas de notifications SNMP.

6. Cochez la case **Activer les interruptions d'authentification** si vous souhaitez que l'agent SNMP StorageGRID envoie une interruption d'authentification s'il reçoit un message de protocole mal authentifié.

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

   Les champs de cette section sont utilisés pour l'authentification communautaire dans SNMPv1 ou SNMPv2c. Ces champs ne s'appliquent pas au protocole SNMPv3.

   a. Dans le champ **Default Trap Community**, vous pouvez également saisir la chaîne de communauté par défaut que vous souhaitez utiliser pour les destinations de déroutement.

      Selon les besoins, vous pouvez fournir une autre chaîne de communauté (« personnalisée ») lorsque vous définir une destination de recouvrement spécifique.

      Valeur par défaut Trap Community peut comporter un maximum de 32 caractères et ne peut pas contenir d'espaces.

   b. Pour **Read-Only Community**, entrez une ou plusieurs chaînes de communauté pour autoriser l'accès MIB en lecture seule sur les adresses d'agent IPv4 et IPv6. Cliquez sur le signe plus ➕ pour ajouter plusieurs chaînes.

      Lorsque le système de gestion interroge la MIB StorageGRID, il envoie une chaîne de communauté. Si la chaîne de communauté correspond à l'une des valeurs spécifiées ici, l'agent SNMP envoie une réponse au système de gestion.

      Chaque chaîne de communauté peut comporter un maximum de 32 caractères et ne peut pas contenir d'espaces. Jusqu'à cinq chaînes sont autorisées.

      ⓘ Pour assurer la sécurité de votre système StorageGRID, n'utilisez pas « public » comme fil de communauté. Si vous n'entrez pas de chaîne de communauté, l'agent SNMP utilise l'ID de grille de votre système StorageGRID comme chaîne de communauté.

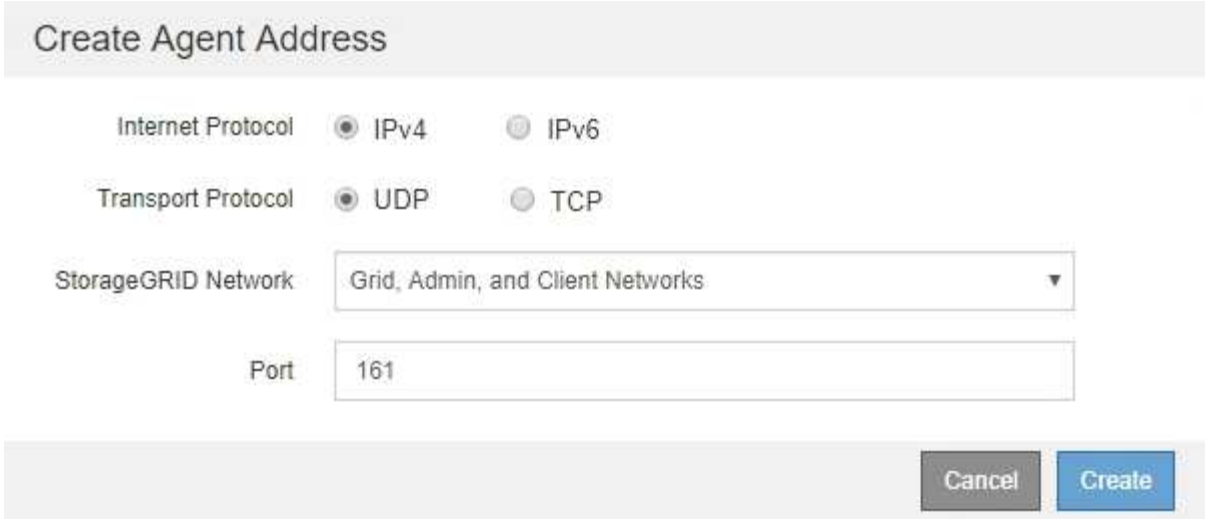
8. Vous pouvez également sélectionner l'onglet adresses d'agent dans la section autres configurations.

   Utilisez cet onglet pour spécifier une ou plusieurs « adresses d'écoute ». Ce sont les adresses StorageGRID sur lesquelles l'agent SNMP peut recevoir des requêtes. Chaque adresse de l'agent inclut un protocole Internet, un protocole de transport, un réseau StorageGRID et éventuellement un port.

   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.

   a. Cliquez sur **Créer**.

      La boîte de dialogue Créer une adresse d'agent s'affiche.



b. Pour **Internet Protocol**, indiquez si cette adresse doit utiliser IPv4 ou IPv6.

   Par défaut, SNMP utilise IPv4.

c. Pour **transport Protocol**, sélectionnez si cette adresse utilisera UDP ou TCP.

   Par défaut, SNMP utilise UDP.

d. Dans le champ **réseau StorageGRID**, sélectionnez le réseau StorageGRID sur lequel la requête sera reçue.

   - Réseau Grid, Admin et client : StorageGRID doit écouter les requêtes SNMP sur les trois réseaux.
   - Réseau Grid
   - Réseau d'administration
   - Réseau client

   > Pour vous assurer que les communications client avec StorageGRID restent sécurisées, vous ne devez pas créer d'adresse d'agent pour le réseau client.

e. Dans le champ **Port**, saisissez éventuellement le numéro de port que l'agent SNMP doit écouter.

   Le port UDP par défaut d'un agent SNMP est 161, mais vous pouvez entrer n'importe quel numéro de port inutilisé.

   > 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.

f. Cliquez sur **Créer**.

   L'adresse de l'agent est créée et ajoutée à la table.

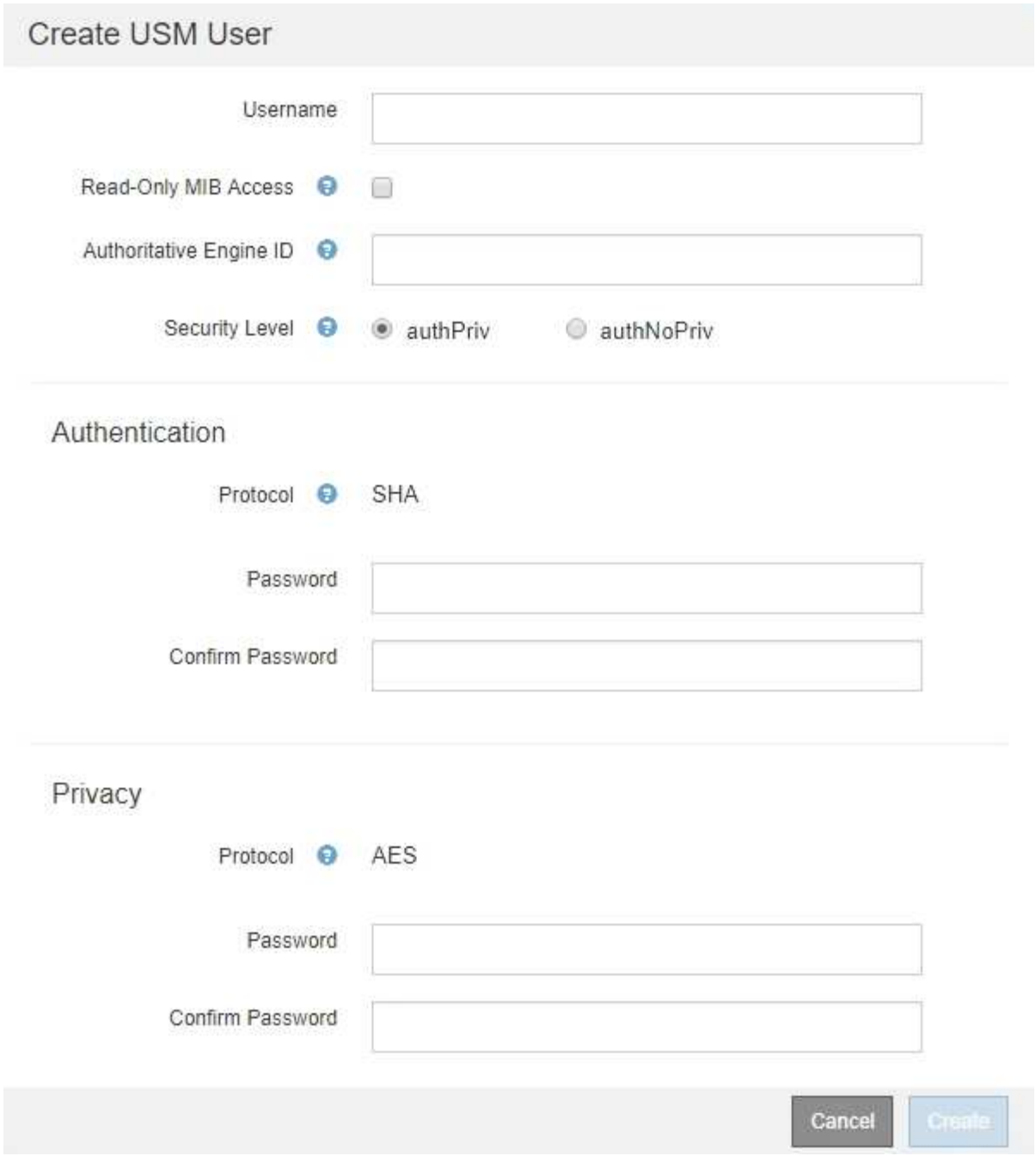
9. Si vous utilisez SNMPv3, sélectionnez l'onglet utilisateurs USM dans la section autres configurations.

   Utilisez cet onglet pour définir les utilisateurs USM autorisés à interroger la MIB ou à recevoir des interruptions et des informations.

   Cette étape ne s'applique pas si vous utilisez uniquement SNMPv1 ou SNMPv2c.

   a. Cliquez sur **Créer**.

      La boîte de dialogue Créer un utilisateur USM s'affiche.



b. Saisissez un **Nom d'utilisateur** unique pour cet utilisateur USM.

   Les noms d'utilisateur ont un maximum de 32 caractères et ne peuvent pas contenir d'espaces. Le nom d'utilisateur ne peut pas être modifié après la création de l'utilisateur.

c. Cochez la case **accès MIB en lecture seule** si cet utilisateur doit avoir un accès en lecture seule à la base de données MIB.

   Si vous sélectionnez **accès MIB en lecture seule**, le champ **ID moteur autorisée** est désactivé.

   > Les utilisateurs d'USM disposant d'un accès MIB en lecture seule ne peuvent pas avoir d'ID de moteur.

d. Si cet utilisateur sera utilisé dans une destination INFORM, saisissez l'ID de moteur * faisant autorité

pour cet utilisateur.

> Les destinations SNMPv3 INFORM doivent avoir des utilisateurs avec des ID de moteur. La destination du trap SNMPv3 ne peut pas avoir d'utilisateurs avec des ID de moteur.

L'ID de moteur faisant autorité peut être de 5 à 32 octets en hexadécimal.

e. Sélectionnez un niveau de sécurité pour l'utilisateur USM.
   - **AuthPriv** : cet utilisateur communique avec l'authentification et la confidentialité (cryptage). Vous devez spécifier un protocole d'authentification et un mot de passe ainsi qu'un protocole de confidentialité et un mot de passe.
   - **AuthNoPriv**: Cet utilisateur communique avec l'authentification et sans confidentialité (pas de cryptage). Vous devez spécifier un protocole d'authentification et un mot de passe.

f. Entrez et confirmez le mot de passe que cet utilisateur utilisera pour l'authentification.

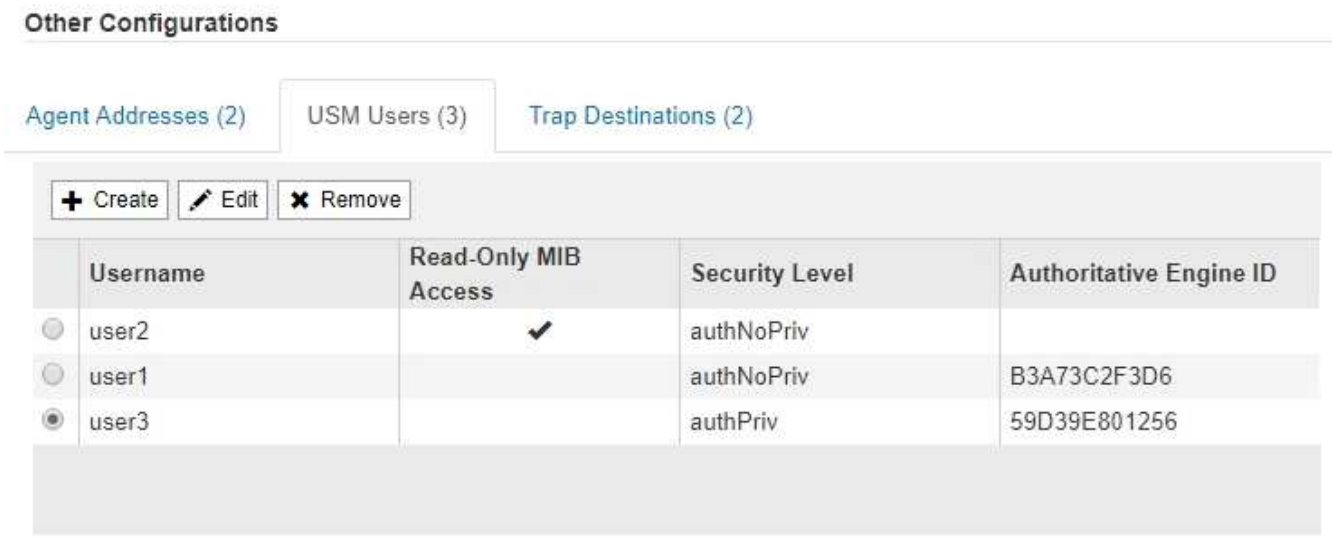
> Le seul protocole d'authentification pris en charge est SHA (HMAC-SHA-96).

g. Si vous avez sélectionné **authPriv**, entrez et confirmez le mot de passe que cet utilisateur utilisera pour la confidentialité.

> Le seul protocole de confidentialité pris en charge est AES.

h. Cliquez sur **Créer**.

L'utilisateur USM est créé et ajouté à la table.

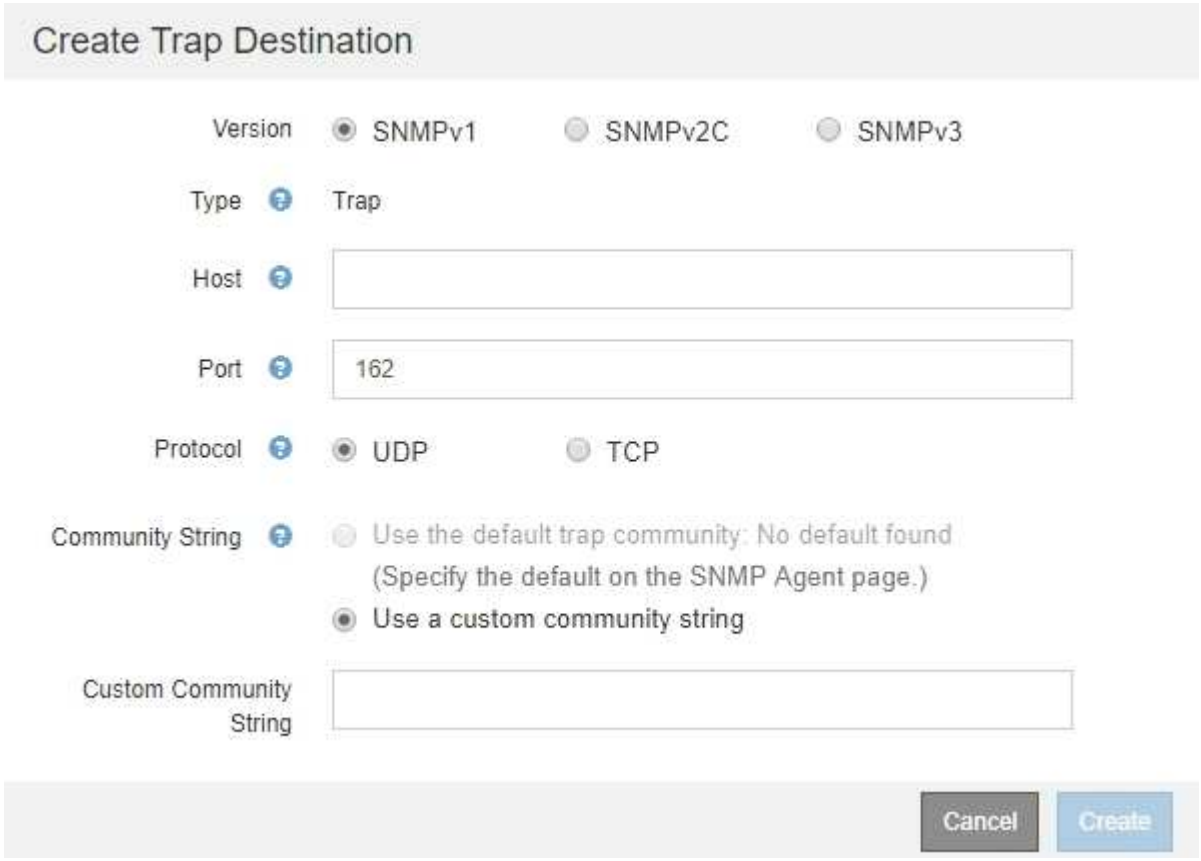


10. dans la section autres configurations, sélectionnez l'onglet destinations de recouvrement.

L'onglet destinations de recouvrement permet de définir une ou plusieurs destinations pour les notifications d'interruption StorageGRID ou d'information. Lorsque vous activez l'agent SNMP et cliquez sur **Enregistrer**, StorageGRID commence à envoyer des notifications à chaque destination définie. Des notifications sont envoyées lorsque des alertes et des alarmes sont déclenchées. Les notifications standard sont également envoyées pour les entités MIB-II prises en charge (par exemple, ifdown et coldStart).

a. Cliquez sur **Créer**.

La boîte de dialogue Créer une destination de recouvrement s'affiche.



b. Dans le champ **version**, sélectionnez la version SNMP à utiliser pour cette notification.

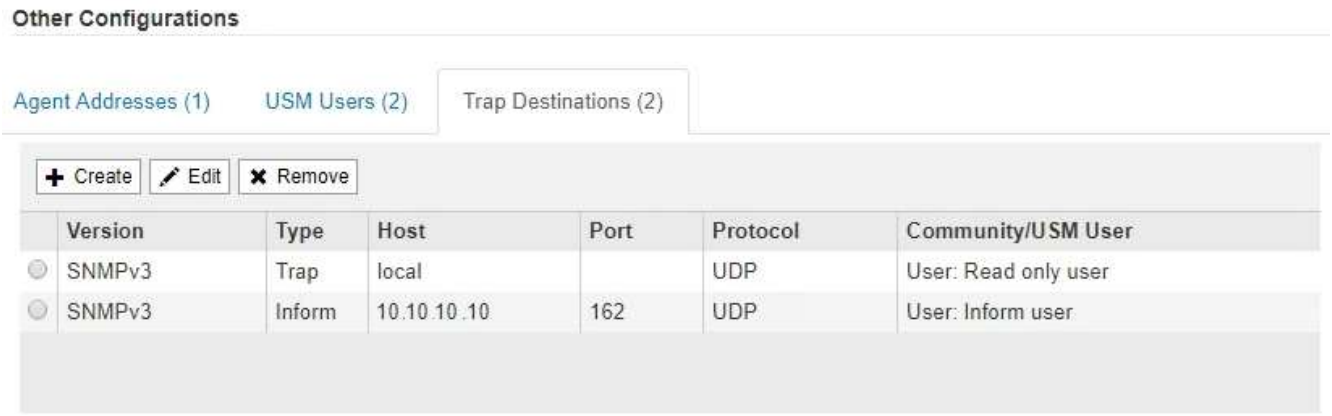
c. Remplissez le formulaire en fonction de la version que vous avez sélectionnée

Version	Spécifiez ces informations
SNMPv1	**Remarque :** pour SNMPv1, l'agent SNMP ne peut envoyer que des interruptions. Les informations ne sont pas prises en charge. i. Dans le champ **Host**, entrez une adresse IPv4 ou IPv6 (ou FQDN) pour recevoir l'interruption. ii. Pour **Port**, utilisez la valeur par défaut (162), sauf si vous devez utiliser une autre valeur. (162 est le port standard des traps SNMP.) iii. Pour **Protocol**, utilisez la valeur par défaut (UDP). TCP est également pris en charge. (UDP est le protocole standard d'interruption SNMP.) iv. Utilisez la communauté d'interruptions par défaut, si l'une d'entre elles a été spécifiée sur la page agent SNMP, ou entrez une chaîne de communauté personnalisée pour cette destination d'interruption. La chaîne de communauté personnalisée peut comporter un maximum de 32 caractères et ne peut pas contenir d'espaces.
SNMPv2c	i. Indiquez si la destination sera utilisée pour les interruptions ou pour les informations. ii. Dans le champ **Host**, entrez une adresse IPv4 ou IPv6 (ou FQDN) pour recevoir l'interruption. iii. Pour **Port**, utilisez la valeur par défaut (162), sauf si vous devez utiliser une autre valeur. (162 est le port standard des traps SNMP.) iv. Pour **Protocol**, utilisez la valeur par défaut (UDP). TCP est également pris en charge. (UDP est le protocole standard d'interruption SNMP.) v. Utilisez la communauté d'interruptions par défaut, si l'une d'entre elles a été spécifiée sur la page agent SNMP, ou entrez une chaîne de communauté personnalisée pour cette destination d'interruption. La chaîne de communauté personnalisée peut comporter un maximum de 32 caractères et ne peut pas contenir d'espaces.

Version	Spécifiez ces informations
SNMPv3	i. Indiquez si la destination sera utilisée pour les interruptions ou pour les informations. ii. Dans le champ **Host**, entrez une adresse IPv4 ou IPv6 (ou FQDN) pour recevoir l'interruption. iii. Pour **Port**, utilisez la valeur par défaut (162), sauf si vous devez utiliser une autre valeur. (162 est le port standard des traps SNMP.) iv. Pour **Protocol**, utilisez la valeur par défaut (UDP). TCP est également pris en charge. (UDP est le protocole standard d'interruption SNMP.) v. Sélectionnez l'utilisateur USM qui sera utilisé pour l'authentification. ◦ Si vous avez sélectionné **Trap**, seuls les utilisateurs d'USM sans ID de moteur faisant autorité sont affichés. ◦ Si vous avez sélectionné **INFORM**, seuls les utilisateurs d'USM avec des ID de moteur faisant autorité sont affichés.

d. Cliquez sur **Créer**.

La destination de la trappe est créée et ajoutée à la table.



11. Une fois la configuration de l'agent SNMP terminée, cliquez sur **Enregistrer**

La nouvelle configuration de l'agent SNMP devient active.

Informations associées

"Neutralisation des notifications d'alerte"

Mise à jour de 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.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer de l'autorisation accès racine.

Description de la tâche

Chaque fois que vous mettez à jour la configuration de l'agent SNMP, sachez que vous devez cliquer sur **Enregistrer** en bas de la page agent SNMP pour valider les modifications que vous avez effectuées sur chaque onglet.

Étapes

1. Sélectionnez **Configuration** > **surveillance** > **agent SNMP**.

   La page agent SNMP s'affiche.

2. Pour désactiver l'agent SNMP sur tous les nœuds de la grille, décochez la case **Activer SNMP** et cliquez sur **Enregistrer**.

   L'agent SNMP est désactivé pour tous les nœuds de la grille. Si vous réactivez ultérieurement l'agent, tous les paramètres de configuration SNMP précédents sont conservés.

3. Vous pouvez également mettre à jour les valeurs saisies pour **Contact système** et **emplacement système**.
4. Si vous ne souhaitez plus que l'agent SNMP StorageGRID envoie des interruptions et informe les notifications, désélectionnez la case à cocher **Activer les notifications d'agent SNMP**.

   Lorsque cette case à cocher n'est pas sélectionnée, l'agent SNMP prend en charge l'accès MIB en lecture seule, mais n'envoie aucune notification SNMP.

5. Si vous ne souhaitez plus que l'agent SNMP StorageGRID envoie un trap d'authentification lorsqu'il reçoit un message de protocole mal authentifié, désélectionnez la case à cocher **Activer les traps** d'authentification.
6. Si vous utilisez SNMPv1 ou SNMPv2c, vous pouvez mettre à jour la section chaînes de communauté.

   Les champs de cette section sont utilisés pour l'authentification communautaire dans SNMPv1 ou SNMPv2c. Ces champs ne s'appliquent pas au protocole SNMPv3.

   > Si vous souhaitez supprimer la chaîne de communauté par défaut, vous devez d'abord vous assurer que toutes les destinations de déroutement utilisent une chaîne de communauté personnalisée.

7. 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 ». Ce sont les adresses StorageGRID sur lesquelles l'agent SNMP peut recevoir des requêtes. Chaque adresse de l'agent inclut un protocole Internet, un protocole de transport, un réseau StorageGRID et un port.

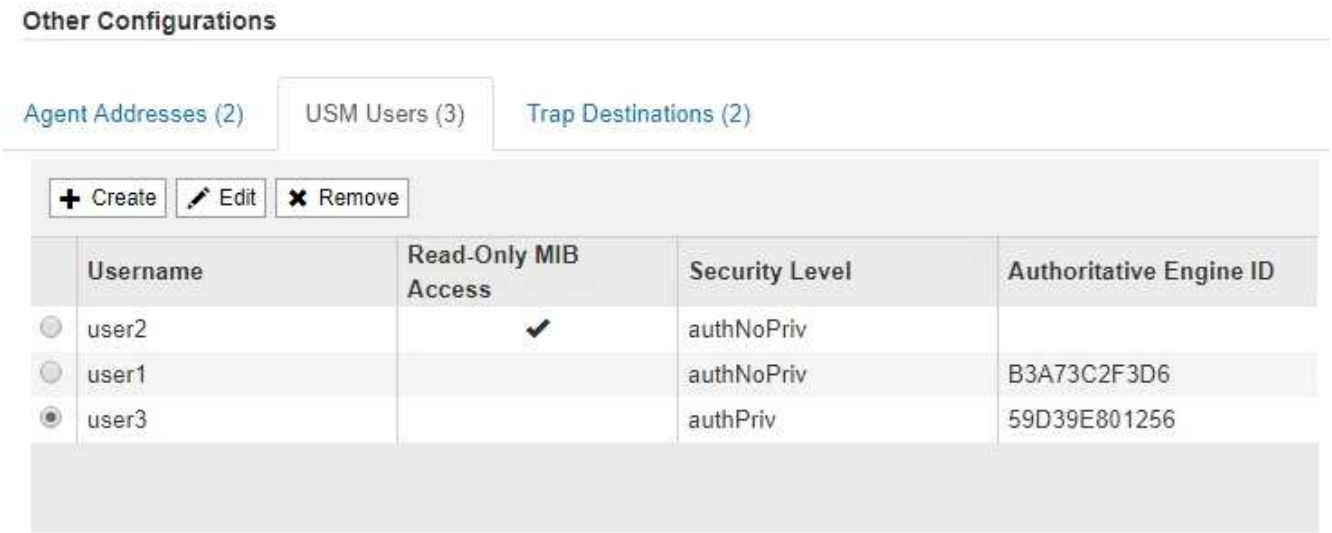
a. Pour ajouter une adresse d'agent, cliquez sur **Créer**. Ensuite, reportez-vous à l'étape pour connaître les adresses des agents dans les instructions de configuration de l'agent SNMP.

b. Pour modifier une adresse d'agent, sélectionnez le bouton radio correspondant à l'adresse, puis cliquez sur **Modifier**. Ensuite, reportez-vous à l'étape pour connaître les adresses des agents dans les instructions de configuration de l'agent SNMP.

c. Pour supprimer une adresse d'agent, sélectionnez le bouton radio correspondant à l'adresse et cliquez sur **Supprimer**. Cliquez ensuite sur **OK** pour confirmer que vous souhaitez supprimer cette adresse.

d. Pour valider vos modifications, cliquez sur **Enregistrer** en bas de la page Agent SNMP.

8. Pour mettre à jour les utilisateurs USM, sélectionnez l'onglet utilisateurs USM dans la section autres configurations.



Utilisez cet onglet pour définir les utilisateurs USM autorisés à interroger la MIB ou à recevoir des interruptions et des informations.

a. Pour ajouter un utilisateur USM, cliquez sur **Créer**. Reportez-vous ensuite à l'étape pour les utilisateurs d'USM dans les instructions de configuration de l'agent SNMP.

b. Pour modifier un utilisateur USM, sélectionnez le bouton radio de l'utilisateur, puis cliquez sur **Modifier**.

Reportez-vous ensuite à l'étape pour les utilisateurs d'USM dans les instructions de configuration de l'agent SNMP.

Le nom d'utilisateur d'un utilisateur USM existant ne peut pas être modifié. Si vous devez modifier un nom d'utilisateur, vous devez le supprimer et en créer un nouveau.

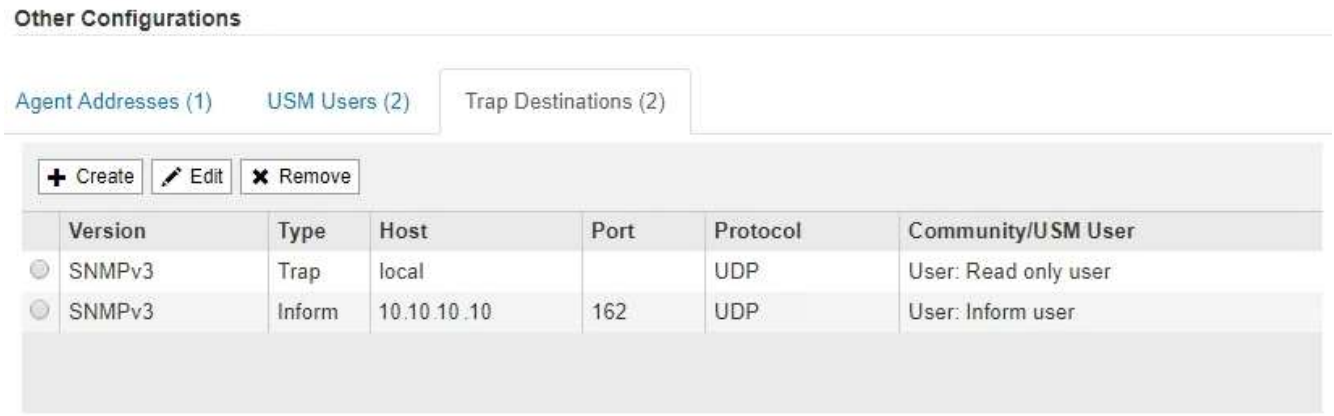
> Si vous ajoutez ou supprimez l'ID moteur faisant autorité d'un utilisateur et que cet utilisateur est actuellement sélectionné pour une destination, vous devez modifier ou supprimer la destination, comme indiqué à l'étape Destination du trap SNMP. Sinon, une erreur de validation se produit lorsque vous enregistrez la configuration de l'agent SNMP.

c. Pour supprimer un utilisateur USM, sélectionnez le bouton radio de l'utilisateur et cliquez sur **Supprimer**. Cliquez ensuite sur **OK** pour confirmer que vous souhaitez supprimer cet utilisateur.

> Si l'utilisateur que vous avez supprimé est actuellement sélectionné pour une destination de recouvrement, vous devez modifier ou supprimer la destination, comme indiqué à l'étape Destination du trap SNMP. Sinon, une erreur de validation se produit lorsque vous enregistrez la configuration de l'agent SNMP.

a. Pour valider vos modifications, cliquez sur **Enregistrer** en bas de la page Agent SNMP.

1. Pour mettre à jour les destinations de recouvrement, sélectionnez l'onglet destinations de recouvrement dans la section autres configurations.



L'onglet destinations de recouvrement permet de définir une ou plusieurs destinations pour les notifications d'interruption StorageGRID ou d'information. Lorsque vous activez l'agent SNMP et cliquez sur **Enregistrer**, StorageGRID commence à envoyer des notifications à chaque destination définie. Des

notifications sont envoyées lorsque des alertes et des alarmes sont déclenchées. Les notifications standard sont également envoyées pour les entités MIB-II prises en charge (par exemple, ifdown et coldStart).

   a. Pour ajouter une destination d'interruption, cliquez sur **Créer**. Reportez-vous ensuite à l'étape pour connaître les destinations de déroutement dans les instructions de configuration de l'agent SNMP.
   b. Pour modifier une destination de recouvrement, sélectionnez le bouton radio de l'utilisateur et cliquez sur **Modifier**. Reportez-vous ensuite à l'étape pour connaître les destinations de déroutement dans les instructions de configuration de l'agent SNMP.
   c. Pour supprimer une destination d'interruption, sélectionnez le bouton radio de la destination, puis cliquez sur **Supprimer**. Cliquez ensuite sur **OK** pour confirmer que vous souhaitez supprimer cette destination.
   d. Pour valider vos modifications, cliquez sur **Enregistrer** en bas de la page Agent SNMP.

2. Lorsque vous avez mis à jour la configuration de l'agent SNMP, cliquez sur **Enregistrer**.

Informations associées

"Configuration de l'agent SNMP"

Collecte de données StorageGRID supplémentaires

De nombreuses autres méthodes permettent de collecter et d'analyser des données utiles lors de l'analyse de l'état de votre système StorageGRID ou lors de la collaboration avec le support technique pour résoudre un problème.

- "Utilisation de graphiques et de rapports"
- "Surveillance et PERFORMANCES ACCRUES"
- "Surveillance des opérations de vérification d'objets"
- "Contrôle des événements"
- "Vérification des messages d'audit"
- "Collecte des fichiers journaux et des données système"
- "Déclenchement manuel de l'un des messages AutoSupport"
- "Affichage de l'arborescence de la grille topologique"
- "L'examen des metrics de support"
- "Exécution des diagnostics"
- "Création d'applications de surveillance personnalisées"

Utilisation de graphiques et de rapports

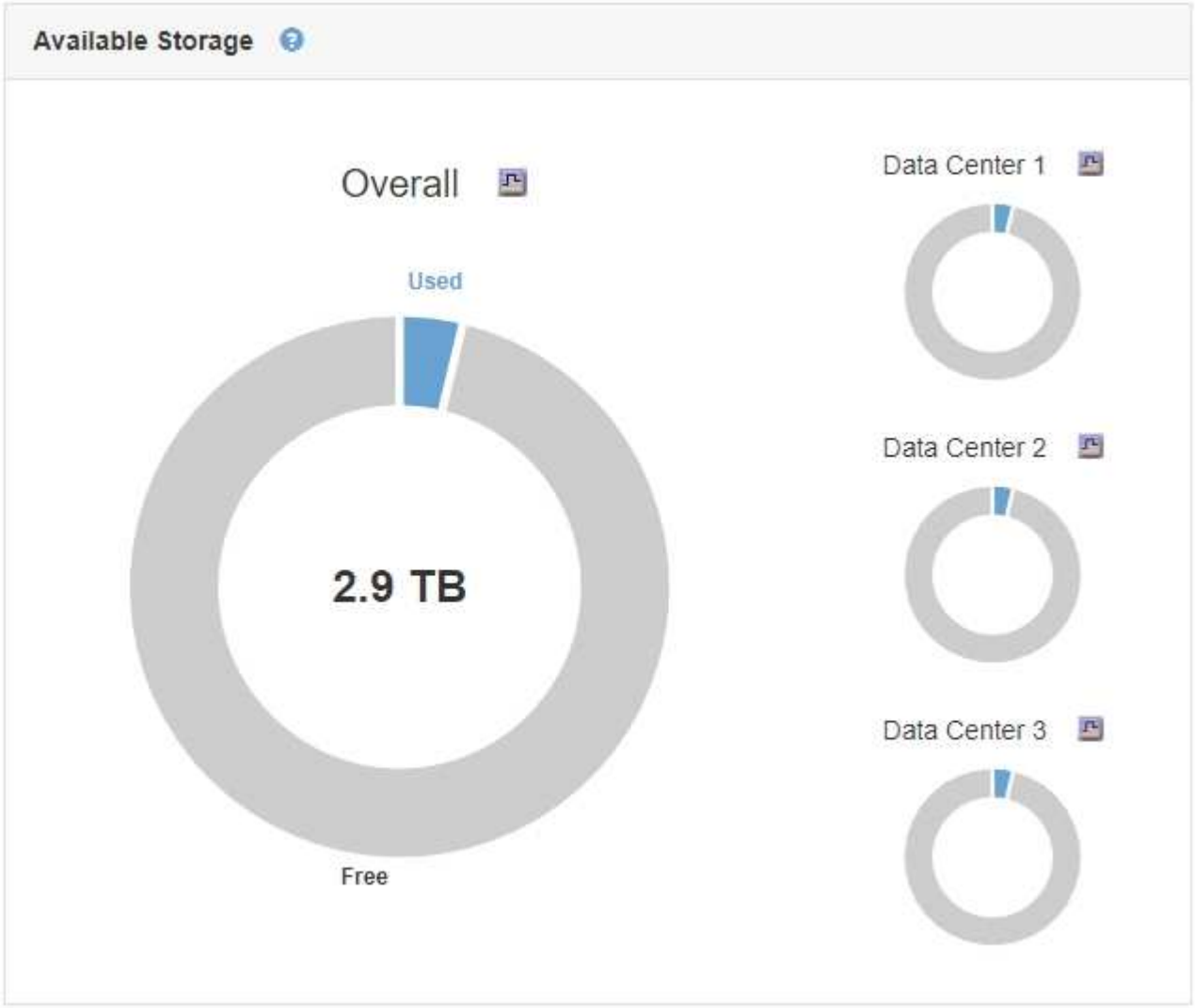
Vous pouvez utiliser des graphiques et des rapports pour surveiller l'état du système StorageGRID et résoudre les problèmes. Les types de graphiques et de rapports disponibles dans Grid Manager incluent des graphiques circulaires (sur le tableau de bord uniquement), des graphiques et des rapports texte.

Types de graphiques et de graphiques

Les graphiques et les graphiques résument les valeurs des mesures et des attributs

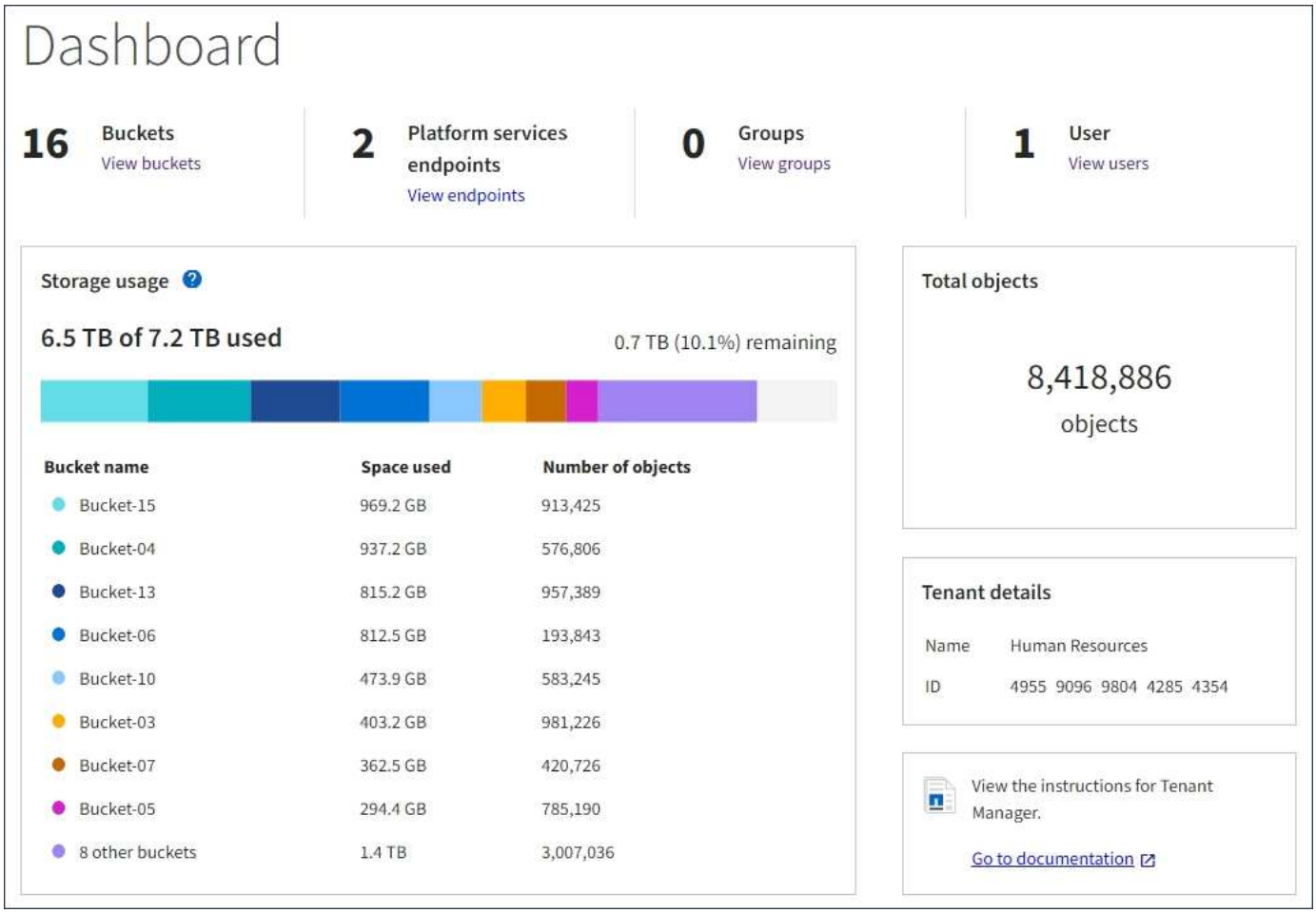
StorageGRID spécifiques.

Le tableau de bord de Grid Manager inclut des graphiques circulaires (donut) pour résumer le stockage disponible pour la grille et chaque site.



Le panneau Storage usage du tableau de bord de tenant Manager affiche les éléments suivants :

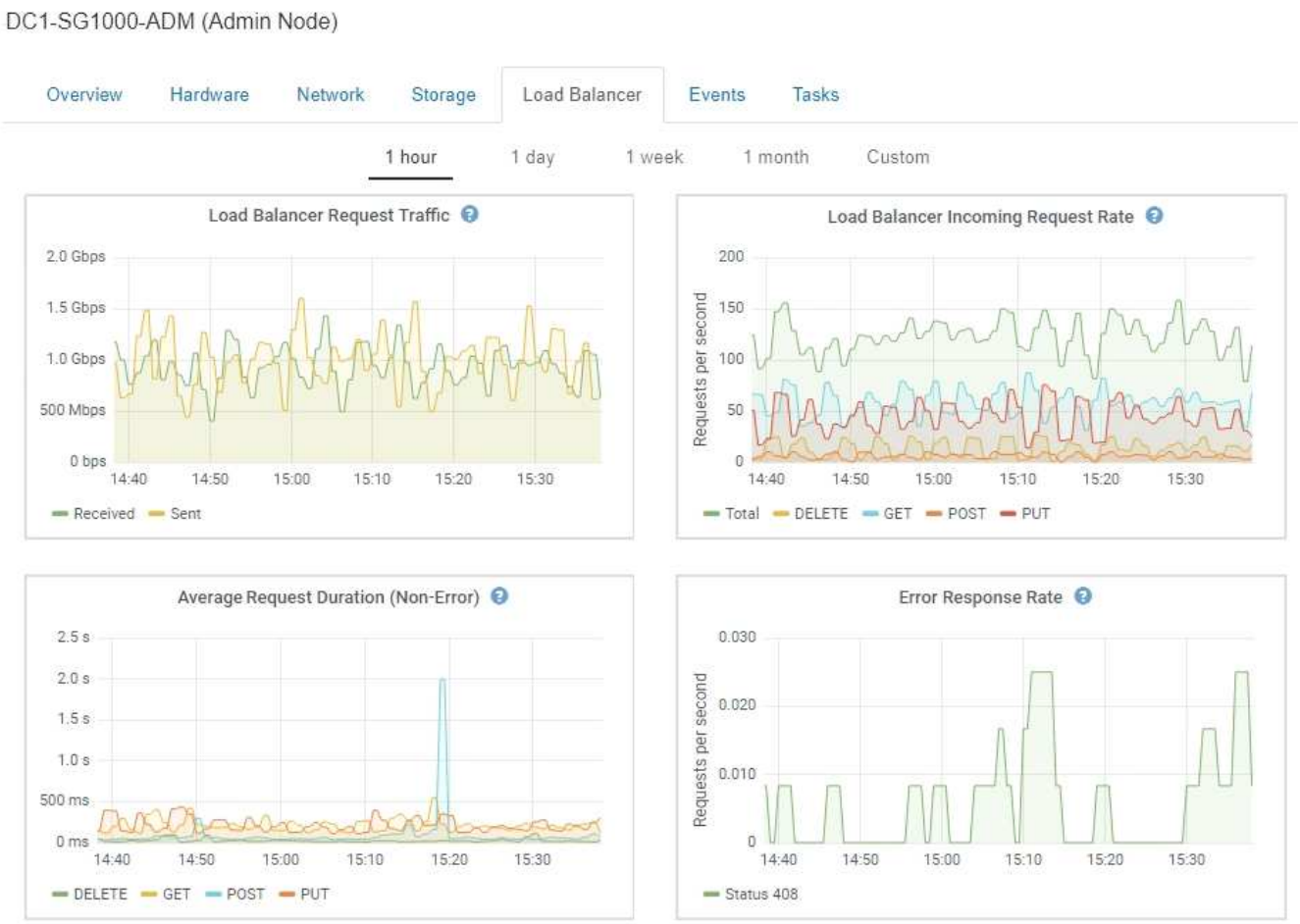
- Liste des compartiments les plus grands (S3) ou des conteneurs (Swift) du locataire
- Un graphique à barres qui représente les tailles relatives des grands godets ou conteneurs
- La quantité totale d’espace utilisé et, si un quota est défini, la quantité et le pourcentage d’espace restant



De plus, les graphiques qui montrent comment les métriques et les attributs StorageGRID changent au fil du temps sont disponibles à partir de la page noeuds et de la page **support** > **Outils** > **topologie de grille**.

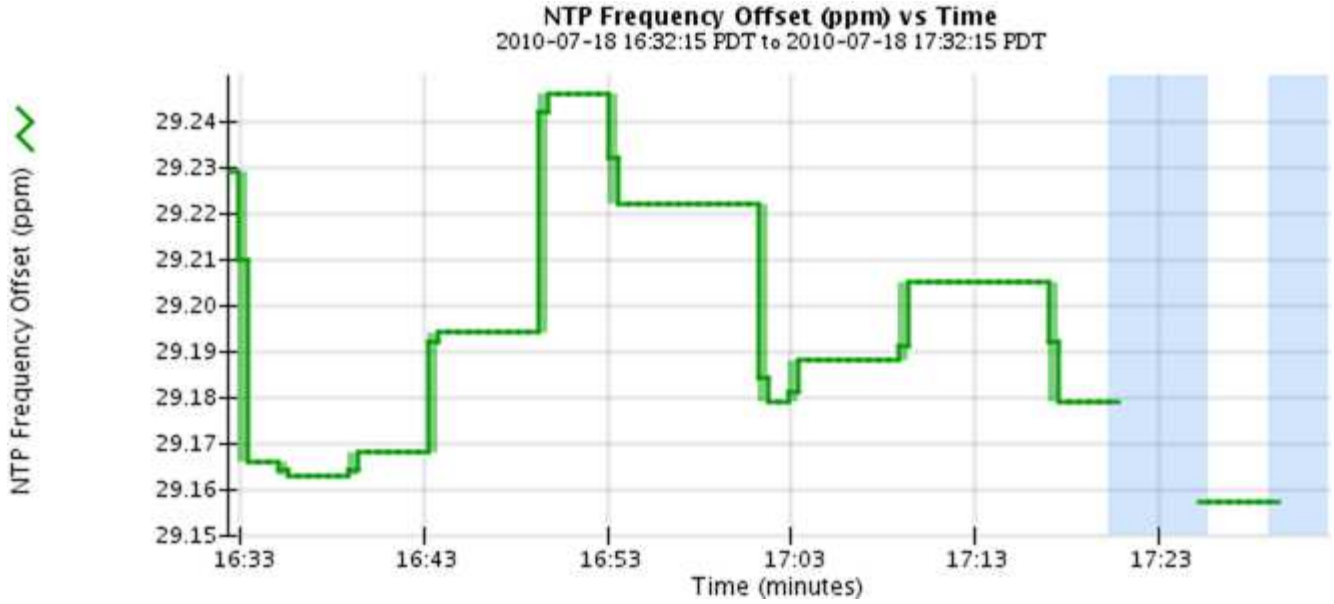
Il existe quatre types de graphiques :

- **Graphiques Grafana** : affichés sur la page nœuds, les graphiques Grafana sont utilisés pour tracer les valeurs des metrics Prometheus dans le temps. Par exemple, l'onglet **Nodes** > **Load Balancer** d'un noeud d'administration comprend quatre graphiques Grafana.

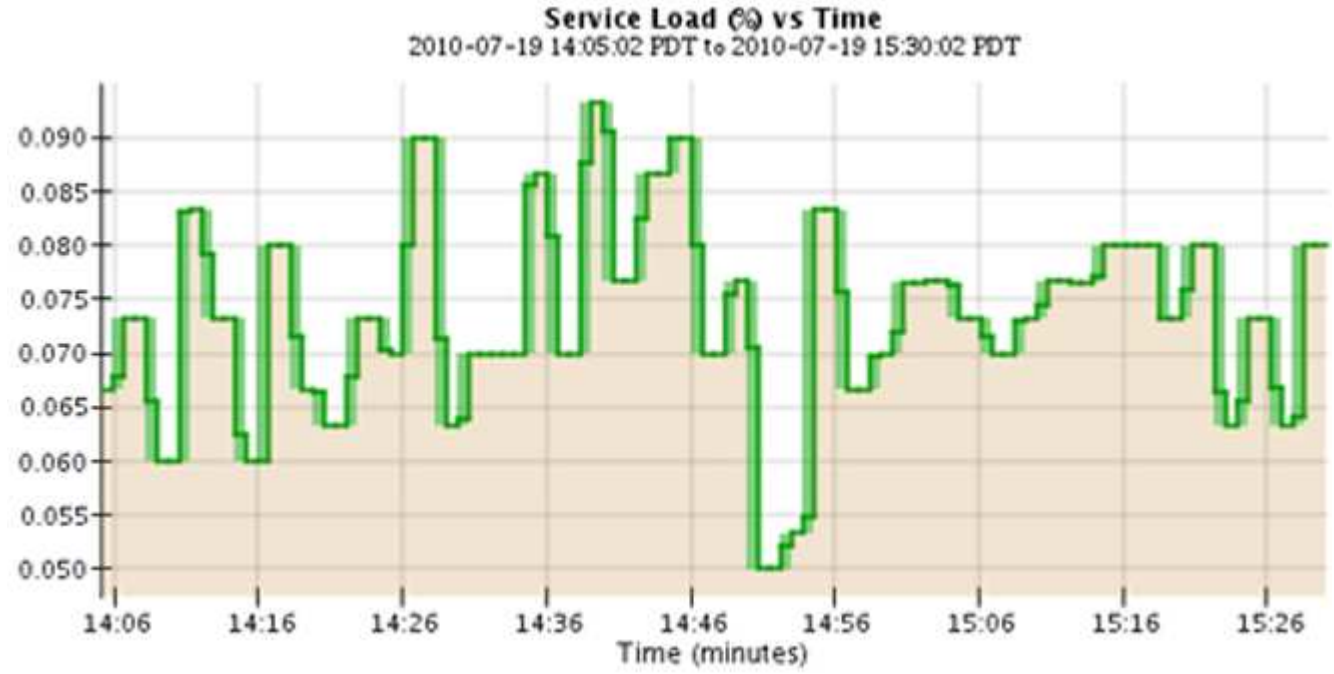


Les graphiques Grafana sont également inclus dans les tableaux de bord pré-construits disponibles à partir de la page **support** > **Outils** > **métriques**.

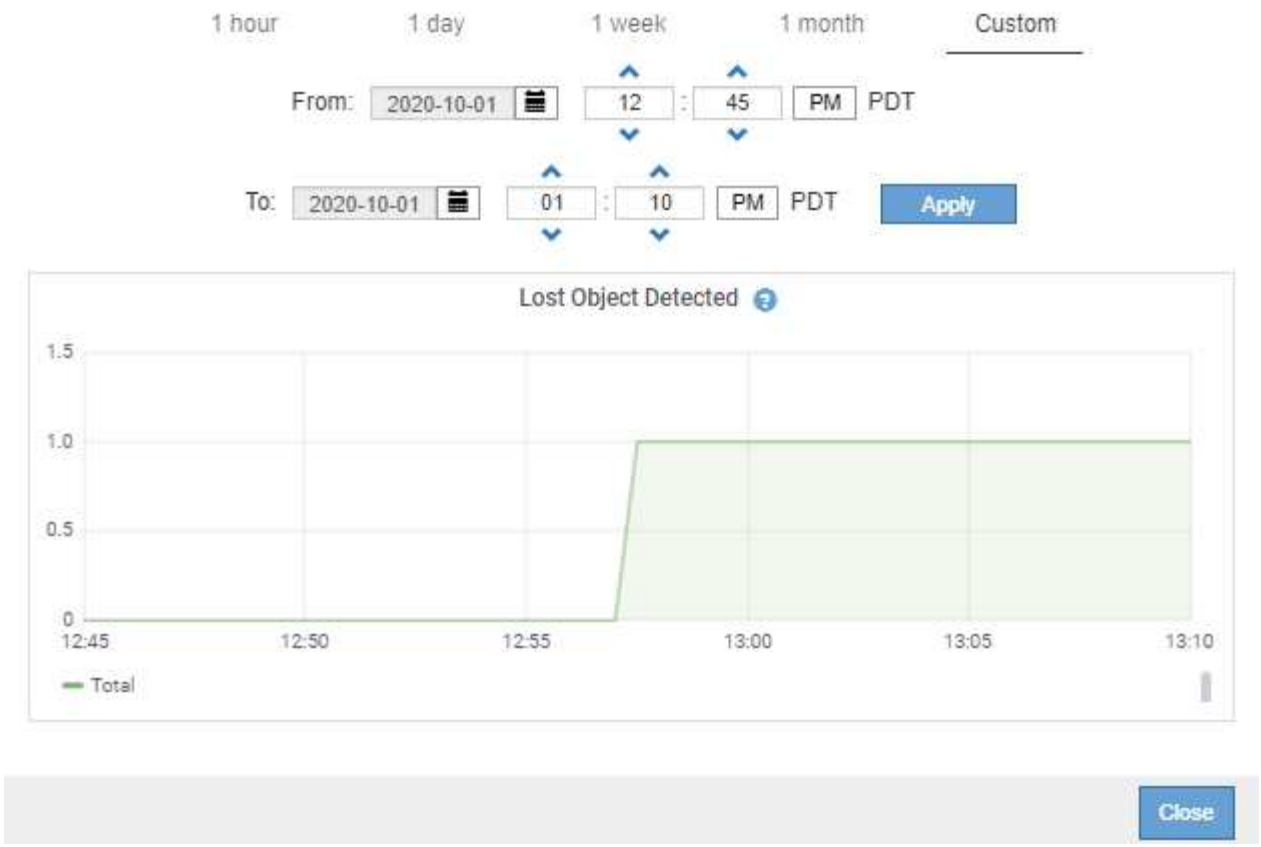
- **Graphes linéaires** : disponible à partir de la page noeuds et à partir de la page **support** > **Outils** > **topologie de grille** (cliquez sur l'icône du graphique) Après une valeur de données), des graphes linéaires sont utilisés pour tracer les valeurs des attributs StorageGRID qui ont une valeur unitaire (tels que le décalage de fréquence NTP, en ppm). Les modifications de la valeur sont tracées dans des intervalles de données réguliers (bacs) au fil du temps.



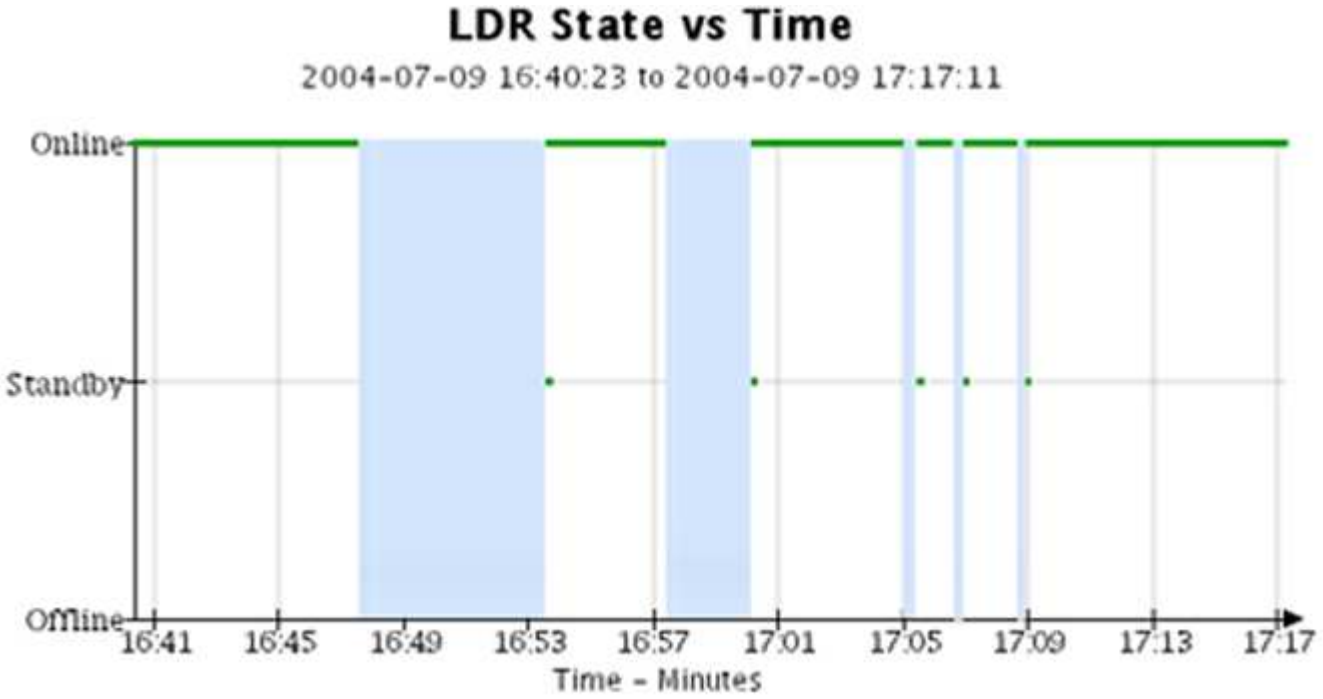
- **Graphes de zone** : disponible à partir de la page noeuds et à partir de la page **support** > **Outils** > **topologie de grille** (cliquez sur l'icône du graphique) après une valeur de données), les graphes de zone sont utilisés pour tracer les quantités d'attributs volumétriques, telles que les nombres d'objets ou les valeurs de charge de service. Les graphiques de zone sont similaires aux graphiques de ligne, mais incluent un ombrage marron clair en dessous de la ligne. Les modifications de la valeur sont tracées dans des intervalles de données réguliers (bacs) au fil du temps.



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



- **Graphique d'état** : disponible à partir de la page **support** > **Outils** > **topologie de grille** (cliquez sur l'icône du graphique) après une valeur de données), les graphiques d'état sont utilisés pour tracer les valeurs d'attribut représentant des états distincts tels qu'un état de service qui peut être en ligne, en attente ou hors ligne. Les graphiques d'état sont similaires aux graphiques linéaires, mais la transition est discontinue. En d'autres termes, la valeur passe d'une valeur d'état à une autre.



Informations associées

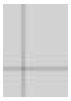
"Affichage de la page nœuds"

"Affichage de l'arborescence de la grille topologique"

"L'examen des metrics de support"

Légende du graphique

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

Échantillon	Signification
	Les valeurs des attributs signalés sont tracées à l'aide de lignes vert foncé.
	Un ombrage vert clair autour des lignes vert foncé indique que les valeurs réelles de cette plage de temps varient et ont été « binning » pour un tracé plus rapide. La ligne foncée représente la moyenne pondérée. La plage en vert clair indique les valeurs maximum et minimum dans le bac. L'ombrage marron clair est utilisé pour les graphiques de zone pour indiquer les données volumétriques.
	Les zones vierges (aucune donnée tracée) indiquent que les valeurs d'attribut ne sont pas disponibles. L'arrière-plan peut être bleu, gris ou un mélange de gris et de bleu, selon l'état du service signalant l'attribut.
	L'ombrage bleu clair indique que certaines ou toutes les valeurs d'attribut à ce moment étaient indéterminées ; l'attribut n'a pas signalé de valeurs parce que le service était dans un état inconnu.
	L'ombrage gris indique que certaines ou toutes les valeurs d'attribut à ce moment n'étaient pas connues car le service signalant les attributs était administrativement en panne.
	Un mélange d'ombrage gris et bleu indique que certaines des valeurs d'attribut au moment étaient indéterminées (parce que le service était dans un état inconnu), tandis que d'autres n'étaient pas connus car le service signalant les attributs était administrativement en panne.

Affichage des graphiques et des graphiques

La page nœuds contient les graphiques et les graphiques auxquels vous devez accéder

régulièrement pour surveiller les attributs tels que la capacité de stockage et le débit. Dans certains cas, en particulier lorsque vous travaillez avec le support technique, vous pouvez utiliser la page **support** > **Outils** > **topologie de grille** pour accéder à des graphiques supplémentaires.

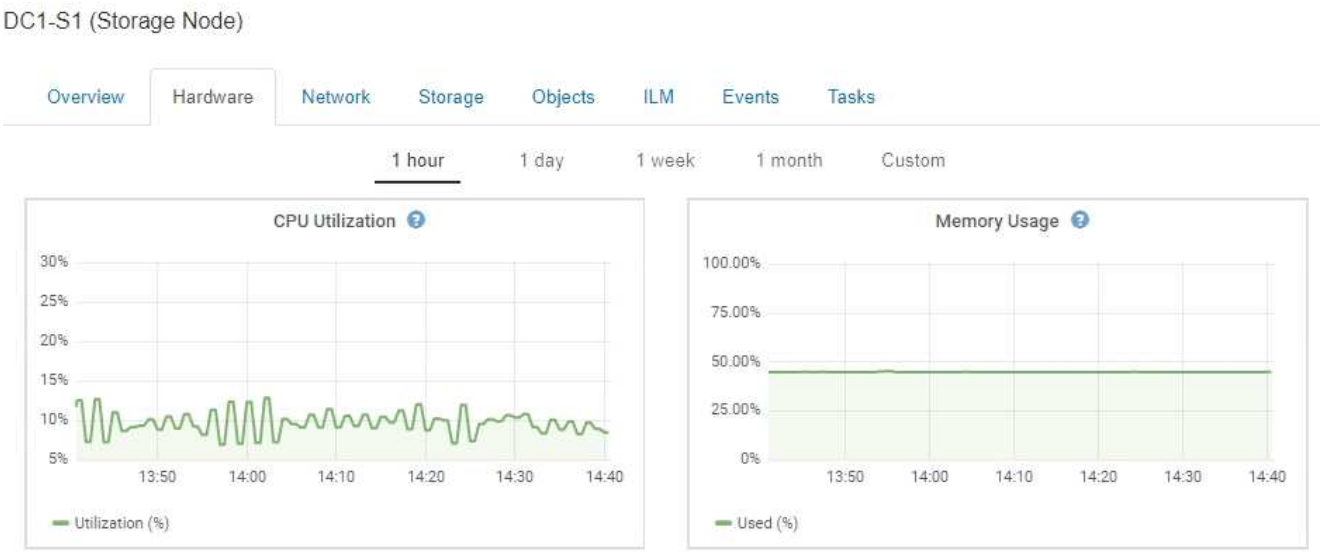
Ce dont vous avez besoin

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

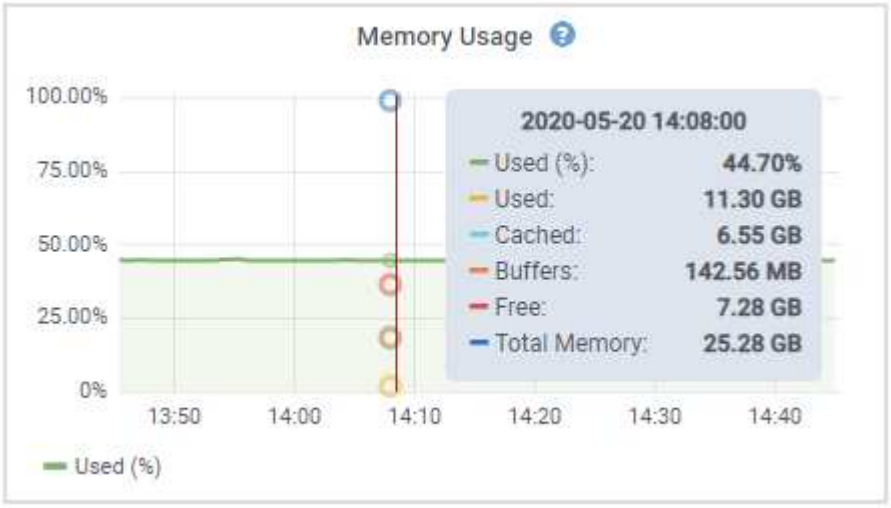
Étapes

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

   Certains onglets comprennent un ou plusieurs graphiques Grafana, qui sont utilisés pour tracer les valeurs des metrics Prometheus dans le temps. Par exemple, l'onglet **Nodes** > **Hardware** d'un nœud inclut deux diagrammes Grafana.



3. Vous pouvez également passer le curseur sur la carte pour afficher des valeurs plus détaillées pour un point donné dans le temps.

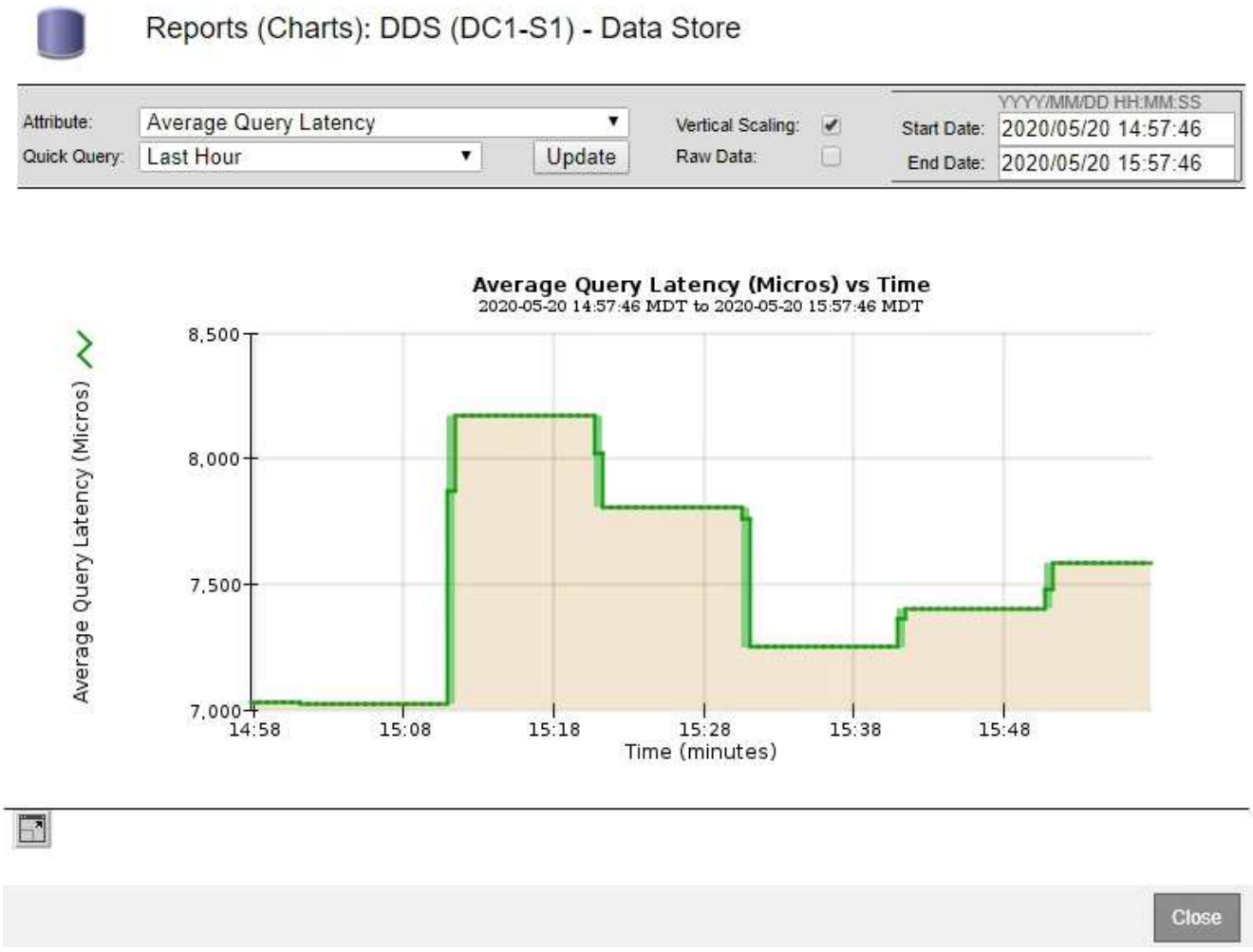


4. Si nécessaire, vous pouvez souvent afficher un graphique pour un attribut ou une mesure spécifique. Dans

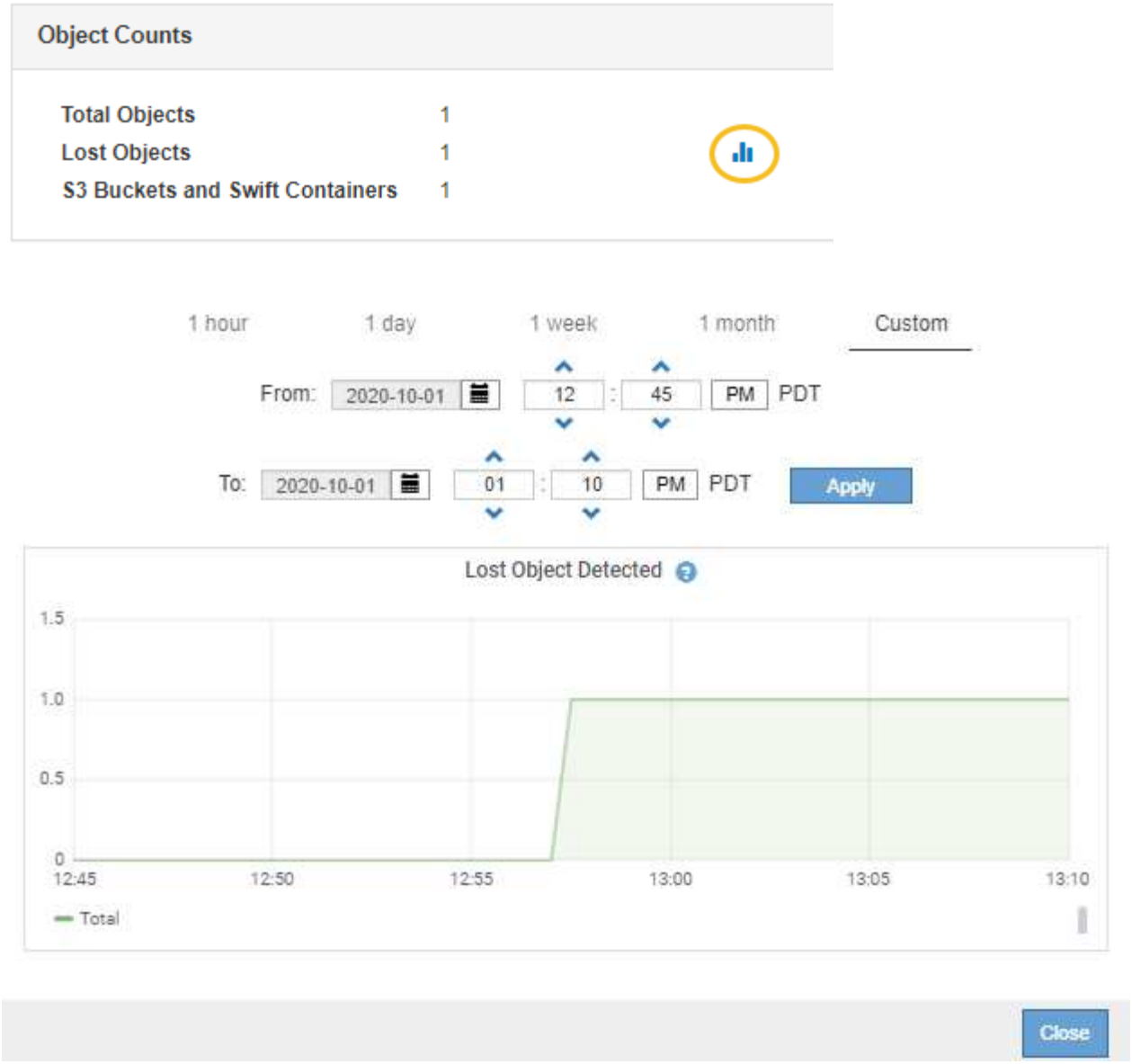
le tableau de la page nœuds, cliquez sur l'icône du graphique ou à droite du nom de l'attribut.

Les graphiques ne sont pas disponibles pour tous les indicateurs et attributs.

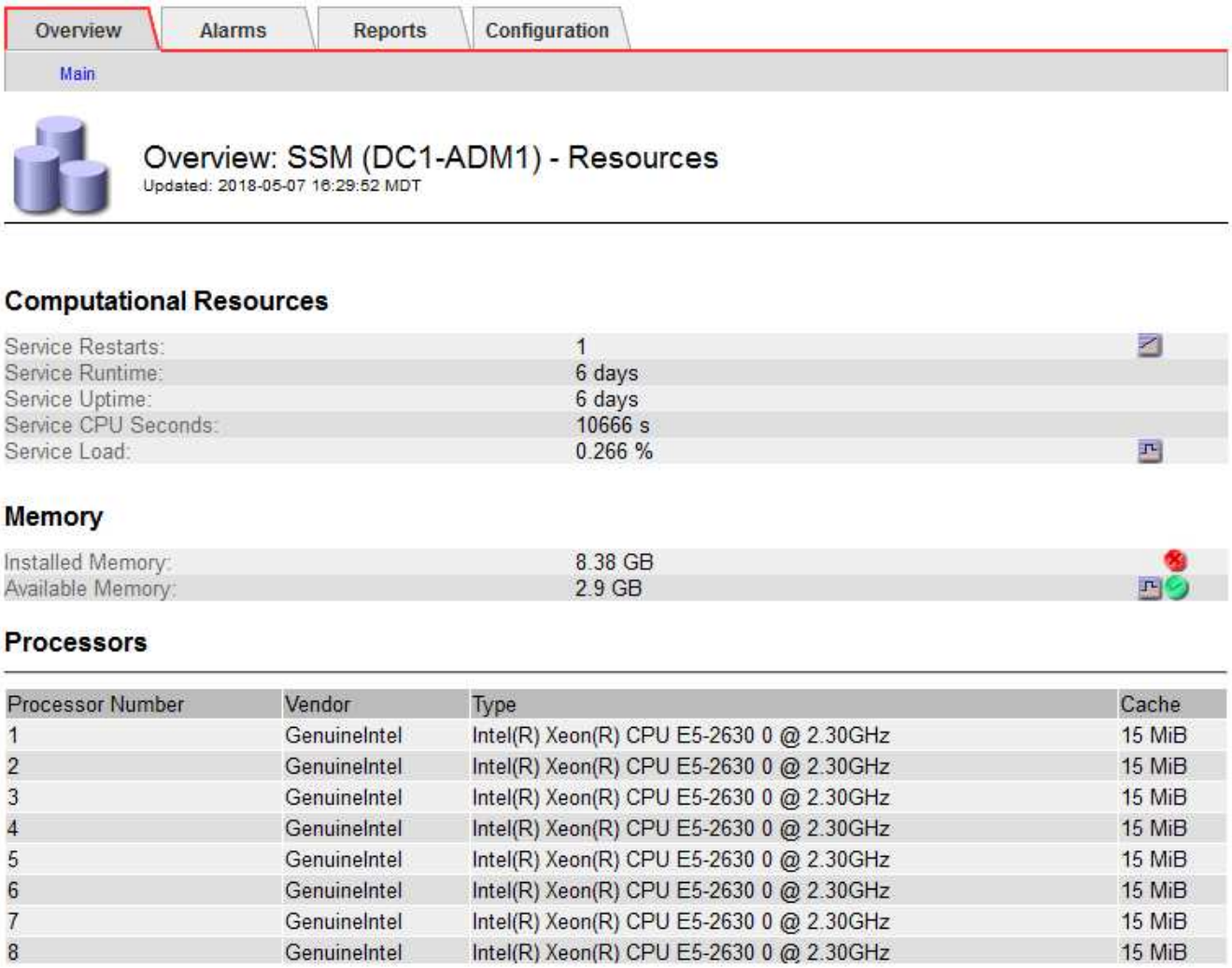
Exemple 1 : dans l'onglet objets d'un noeud de stockage, vous pouvez cliquer sur l'icône du graphique pour afficher la latence moyenne d'une requête de métadonnées au fil du temps.



Exemple 2 : dans l'onglet objets d'un noeud de stockage, vous pouvez cliquer sur l'icône du graphique Pour afficher 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 noeud, sélectionnez **support** > **Outils** > **topologie de grille**.
6. Sélectionnez ***grid node*** > ***component ou service*** > **Présentation** > **main**.



7. Cliquez sur 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 du dernier jour.

Génération de graphiques

Les graphiques affichent une représentation graphique des valeurs de données d'attribut. Vous pouvez générer des rapports sur un site de data Center, un nœud grid, un composant ou un service.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

Étapes

1. Sélectionnez **support** > **Outils** > **topologie de grille**.
2. Sélectionnez ***grid node*** > ***component ou service*** > **Rapports** > **diagrammes**.
3. Sélectionnez l'attribut à rapporter dans la liste déroulante **attribut**.
4. Pour forcer l'axe y à commencer à zéro, décochez la case **mise à l'échelle verticale**.

5. Pour afficher les valeurs avec précision totale, cochez la case **données brutes** ou arrondissez les valeurs à un maximum de trois décimales (par exemple, pour les attributs signalés sous forme de pourcentages), décochez la case **données brutes**.
6. Sélectionnez la période à laquelle effectuer le rapport dans la liste déroulante **requête rapide**.

   Sélectionnez l'option requête personnalisée pour sélectionner une plage de temps spécifique.

   Le graphique apparaît après quelques instants. Prévoir plusieurs minutes pour la totalisation de longues plages de temps.

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

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

8. Cliquez sur **mettre à jour**.

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

9. Si vous souhaitez imprimer le graphique, cliquez avec le bouton droit de la souris et sélectionnez **Imprimer**, puis modifiez les paramètres de l'imprimante requis et cliquez sur **Imprimer**.

Types de rapports texte

Les rapports texte affichent une représentation textuelle des valeurs de données d'attribut traitées par le service NMS. Il existe deux types de rapports générés selon la période de temps sur laquelle vous vous signalez : des rapports de texte brut pour des périodes inférieures à une semaine et des rapports de texte agrégés pour des périodes supérieures à une semaine.

Rapports de texte brut

Un rapport en texte brut affiche des détails sur l'attribut sélectionné :

- Heure de réception : date et heure locales auxquelles une valeur d'échantillon des données d'un attribut a été traitée par le service NMS.
- Heure de l'échantillon : date et heure locales auxquelles une valeur d'attribut a été échantillonnée ou modifiée à la source.
- Valeur : valeur d'attribut au moment de l'échantillon.

Text Results for Services: Load - System Logging

2010-07-18 15:58:39 PDT To 2010-07-19 15:58:39 PDT

Time Received	Sample Time	Value
2010-07-19 15:58:09	2010-07-19 15:58:09	0.016 %
2010-07-19 15:56:06	2010-07-19 15:56:06	0.024 %
2010-07-19 15:54:02	2010-07-19 15:54:02	0.033 %
2010-07-19 15:52:00	2010-07-19 15:52:00	0.016 %
2010-07-19 15:49:57	2010-07-19 15:49:57	0.008 %
2010-07-19 15:47:54	2010-07-19 15:47:54	0.024 %
2010-07-19 15:45:50	2010-07-19 15:45:50	0.016 %
2010-07-19 15:43:47	2010-07-19 15:43:47	0.024 %
2010-07-19 15:41:43	2010-07-19 15:41:43	0.032 %
2010-07-19 15:39:40	2010-07-19 15:39:40	0.024 %
2010-07-19 15:37:37	2010-07-19 15:37:37	0.008 %
2010-07-19 15:35:34	2010-07-19 15:35:34	0.016 %
2010-07-19 15:33:31	2010-07-19 15:33:31	0.024 %
2010-07-19 15:31:27	2010-07-19 15:31:27	0.032 %
2010-07-19 15:29:24	2010-07-19 15:29:24	0.032 %
2010-07-19 15:27:21	2010-07-19 15:27:21	0.049 %
2010-07-19 15:25:18	2010-07-19 15:25:18	0.024 %
2010-07-19 15:21:12	2010-07-19 15:21:12	0.016 %
2010-07-19 15:19:09	2010-07-19 15:19:09	0.008 %
2010-07-19 15:17:07	2010-07-19 15:17:07	0.016 %

Agréger les rapports de texte

Un rapport texte agrégé affiche des données sur une période plus longue (généralement une semaine) qu'un rapport texte brut. Chaque entrée est le résultat d'un résumé de plusieurs valeurs d'attribut (un ensemble de valeurs d'attribut) par le service NMS dans le temps en une seule entrée avec des valeurs moyennes, maximales et minimales dérivées de l'agrégation.

Chaque entrée affiche les informations suivantes :

- Heure d'agrégation : dernière date et heure locales que le service NMS a agrégées (recueillies) un ensemble de valeurs d'attribut modifiées.
- Valeur moyenne : moyenne de la valeur de l'attribut sur la période de temps agrégée.
- Valeur minimale : valeur minimale sur la période de temps agrégée.
- Valeur maximale : valeur maximale sur la période de temps agrégée.

Text Results for Attribute Send to Relay Rate

2010-07-11 16:02:46 PDT To 2010-07-19 16:02:46 PDT

Aggregate Time	Average Value	Minimum Value	Maximum Value
2010-07-19 15:59:52	0.271072196 Messages/s	0.266649743 Messages/s	0.274983464 Messages/s
2010-07-19 15:53:52	0.275585378 Messages/s	0.266562352 Messages/s	0.283302736 Messages/s
2010-07-19 15:49:52	0.279315709 Messages/s	0.233318712 Messages/s	0.333313579 Messages/s
2010-07-19 15:43:52	0.28181323 Messages/s	0.241651024 Messages/s	0.374976601 Messages/s
2010-07-19 15:39:52	0.284233141 Messages/s	0.249982001 Messages/s	0.324971987 Messages/s
2010-07-19 15:33:52	0.325752083 Messages/s	0.266641993 Messages/s	0.358306197 Messages/s
2010-07-19 15:29:52	0.278531507 Messages/s	0.274984766 Messages/s	0.283320999 Messages/s
2010-07-19 15:23:52	0.281437642 Messages/s	0.274981961 Messages/s	0.291577735 Messages/s
2010-07-19 15:17:52	0.261563307 Messages/s	0.258318006 Messages/s	0.266655787 Messages/s
2010-07-19 15:13:52	0.265159147 Messages/s	0.258318557 Messages/s	0.26663986 Messages/s

Génération de rapports texte

Les rapports texte affichent une représentation textuelle des valeurs de données d'attribut traitées par le service NMS. Vous pouvez générer des rapports sur un site de data Center, un nœud grid, un composant ou un service.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

Pour les données d'attribut qui devraient changer en permanence, ces données d'attribut sont échantillonnées par le service NMS (à la source) à intervalles réguliers. Pour les données d'attribut qui changent rarement (par exemple, les données en fonction d'événements tels que les changements d'état ou d'état), une valeur d'attribut est envoyée au service NMS lorsque la valeur change.

Le type de rapport affiché dépend de la période configurée. Par défaut, les rapports de texte agrégés sont générés pour les périodes de plus d'une semaine.

Le texte gris indique que le service a été désactivé administrativement au cours de l'échantillonnage. Le texte bleu indique que le service était dans un état inconnu.

Étapes

1. Sélectionnez **support** > **Outils** > **topologie de grille**.
2. Sélectionnez ***grid node*** > ***component ou service*** > **Reports** > **Text**.
3. Sélectionnez l'attribut à rapporter dans la liste déroulante **attribut**.
4. Sélectionnez le nombre de résultats par page dans la liste déroulante **Résultats par page**.
5. Pour arrondir les valeurs à un maximum de trois décimales (par exemple, pour les attributs signalés sous forme de pourcentages), décochez la case **données brutes**.
6. Sélectionnez la période à laquelle effectuer le rapport dans la liste déroulante **requête rapide**.

   Sélectionnez l'option requête personnalisée pour sélectionner une plage de temps spécifique.

Le rapport apparaît après quelques instants. Prévoir plusieurs minutes pour la totalisation de longues plages de temps.

7. Si vous avez sélectionné requête personnalisée, vous devez personnaliser la période de rapport en entrant **Date de début** et **Date de fin**.

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

8. Cliquez sur **mettre à jour**.

   Un rapport texte est généré au bout de quelques instants. Prévoir plusieurs minutes pour la totalisation de longues plages de temps. En fonction de la durée définie pour la requête, un rapport texte brut ou texte agrégé s'affiche.

9. Si vous souhaitez imprimer le rapport, cliquez avec le bouton droit de la souris et sélectionnez **Imprimer**, puis modifiez les paramètres de l'imprimante requis et cliquez sur **Imprimer**.

Exportation de rapports texte

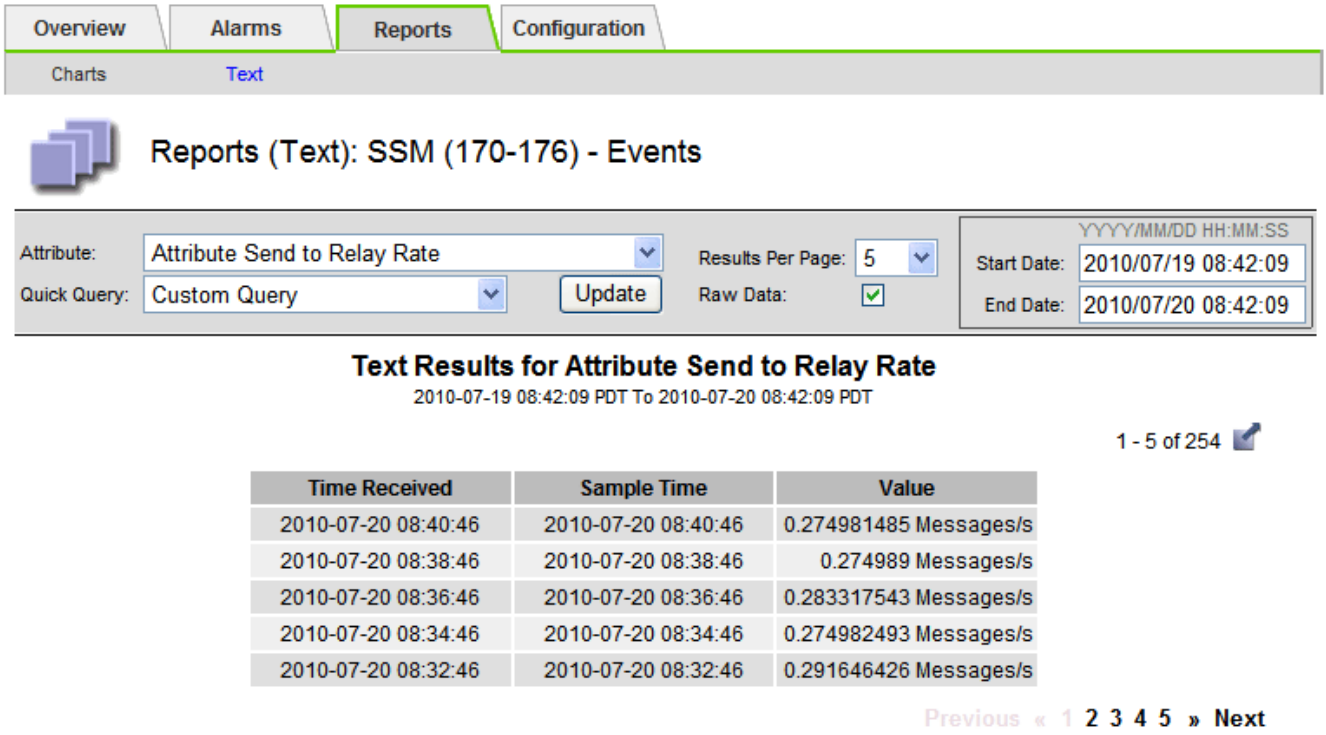
Les rapports texte exportés ouvrent un nouvel onglet de navigateur, qui vous permet de sélectionner et de copier les données.

Description de la tâche

Les données copiées peuvent ensuite être enregistrées dans un nouveau document (par exemple, une feuille de calcul) et utilisées pour analyser les performances du système StorageGRID.

Étapes

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



La fenêtre Exporter un rapport texte s'ouvre et affiche le rapport.

```
Grid ID: 000 000
OID: 2.16.124.113590.2.1.400019.1.1.1.1.16996732.200
Node Path: Site/170-176/SSM/Events
Attribute: Attribute Send to Relay Rate (ABSR)
Query Start Date: 2010-07-19 08:42:09 PDT
Query End Date: 2010-07-20 08:42:09 PDT
Time Received,Time Received (Epoch),Sample Time,Sample Time (Epoch),Value,Type
2010-07-20 08:40:46,1279640446559000,2010-07-20 08:40:46,1279640446537209,0.274981485 Messages/s,U
2010-07-20 08:38:46,1279640326561000,2010-07-20 08:38:46,1279640326529124,0.274989 Messages/s,U
2010-07-20 08:36:46,1279640206556000,2010-07-20 08:36:46,1279640206524330,0.283317543 Messages/s,U
2010-07-20 08:34:46,1279640086540000,2010-07-20 08:34:46,1279640086517645,0.274982493 Messages/s,U
2010-07-20 08:32:46,1279639966543000,2010-07-20 08:32:46,1279639966510022,0.291646426 Messages/s,U
2010-07-20 08:30:46,1279639846561000,2010-07-20 08:30:46,1279639846501672,0.308315369 Messages/s,U
2010-07-20 08:28:46,1279639726527000,2010-07-20 08:28:46,1279639726494673,0.291657509 Messages/s,U
2010-07-20 08:26:46,1279639606526000,2010-07-20 08:26:46,1279639606490890,0.266627739 Messages/s,U
2010-07-20 08:24:46,1279639486495000,2010-07-20 08:24:46,1279639486473368,0.258318523 Messages/s,U
2010-07-20 08:22:46,1279639366480000,2010-07-20 08:22:46,1279639366466497,0.274985902 Messages/s,U
2010-07-20 08:20:46,1279639246469000,2010-07-20 08:20:46,1279639246460346,0.283253871 Messages/s,U
2010-07-20 08:18:46,1279639126469000,2010-07-20 08:18:46,1279639126426669,0.274982804 Messages/s,U
2010-07-20 08:16:46,1279639006437000,2010-07-20 08:16:46,1279639006419168,0.283315503 Messages/s,U
```

4. Sélectionnez et copiez le contenu de la fenêtre Exporter un rapport texte.

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

Surveillance et PERFORMANCES ACCRUES

Vous pouvez surveiller les performances de certaines opérations, telles que le stockage et la récupération d'objets, afin de faciliter l'identification des modifications qui pourraient

nécessiter une investigation plus poussée.

Description de la tâche

Pour contrôler LES PUT et GET, vous pouvez exécuter les commandes S3 et Swift directement depuis un poste de travail ou à l'aide de l'application open source S3tester. Ces méthodes vous permettent d'évaluer la performance indépendamment des facteurs externes à StorageGRID, tels que les problèmes liés à une application client ou à un réseau externe.

Lorsque vous effectuez des tests de MISE EN PLACE et D'OBTENTION d'opérations, suivez les instructions suivantes :

- Utilisez des tailles d'objet comparables aux objets que vous ingérer dans votre grid.
- Exécutez vos opérations sur des sites locaux et distants.

Les messages du journal d'audit indiquent le temps total nécessaire à l'exécution de certaines opérations. Par exemple, pour déterminer le temps de traitement total d'une demande GET S3, vous pouvez vérifier la valeur de l'attribut TIME dans le message d'audit SGET. Vous pouvez également trouver l'attribut HEURE dans les messages d'audit pour les opérations suivantes :

- **S3**: SUPPRIMER, OBTENIR, TÊTE, métadonnées mises à jour, POST, EN
- **SWIFT**: SUPPRIMER, OBTENIR, TÊTE, METTRE

Lors de l'analyse des résultats, examinez le temps moyen requis pour répondre à une demande, ainsi que le débit global que vous pouvez atteindre. Répétez les mêmes tests régulièrement et notez les résultats afin de pouvoir identifier les tendances qui peuvent nécessiter une enquête.

- Vous pouvez télécharger S3tester à partir de github:https://github.com/s3tester

Informations associées

"Examiner les journaux d'audit"

Surveillance des opérations de vérification d'objets

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

Ce dont vous avez besoin

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

Description de la tâche

Deux processus de vérification fonctionnent ensemble pour assurer l'intégrité des données :

- **Vérification de l'arrière-plan** s'exécute automatiquement, en vérifiant continuellement l'exactitude des données de l'objet.

  La vérification en arrière-plan vérifie automatiquement et en continu tous les nœuds de stockage pour déterminer s'il existe des copies corrompues des données d'objet répliquées et codées par effacement. Si un problème est détecté, le système StorageGRID tente automatiquement de remplacer les données d'objet corrompues à partir des copies stockées ailleurs dans le système. La vérification en arrière-plan ne s'exécute pas sur les nœuds d'archivage ou 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 premier plan** peut être déclenchée par un utilisateur pour vérifier plus rapidement l'existence (mais pas l'exactitude) des données d'objet.

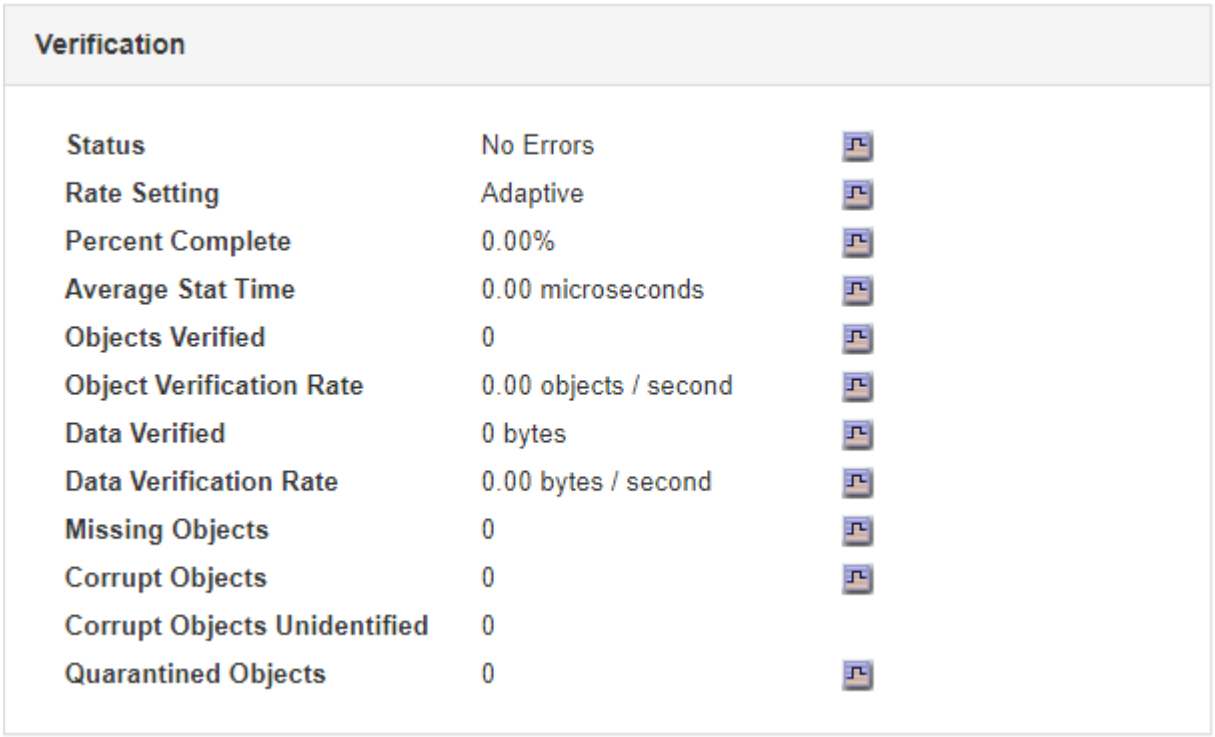
  La vérification à l'avant-plan vous permet de vérifier l'existence de données d'objet répliquées et codées par effacement sur un nœud de stockage spécifique, en vérifiant que chaque objet devrait être présent. Vous pouvez exécuter une vérification en premier plan sur tout ou partie des magasins d'objets d'un nœud de stockage afin de déterminer s'il y a des problèmes d'intégrité avec un périphérique de stockage. Un grand nombre d'objets manquants peut indiquer un problème de stockage.

Pour consulter les résultats des vérifications d'arrière-plan et de premier plan, telles que des objets corrompus ou manquants, consultez la page nœuds d'un nœud de stockage. Vous devez rechercher immédiatement toute instance de données d'objet corrompues ou manquantes afin de déterminer la cause première.

Étapes

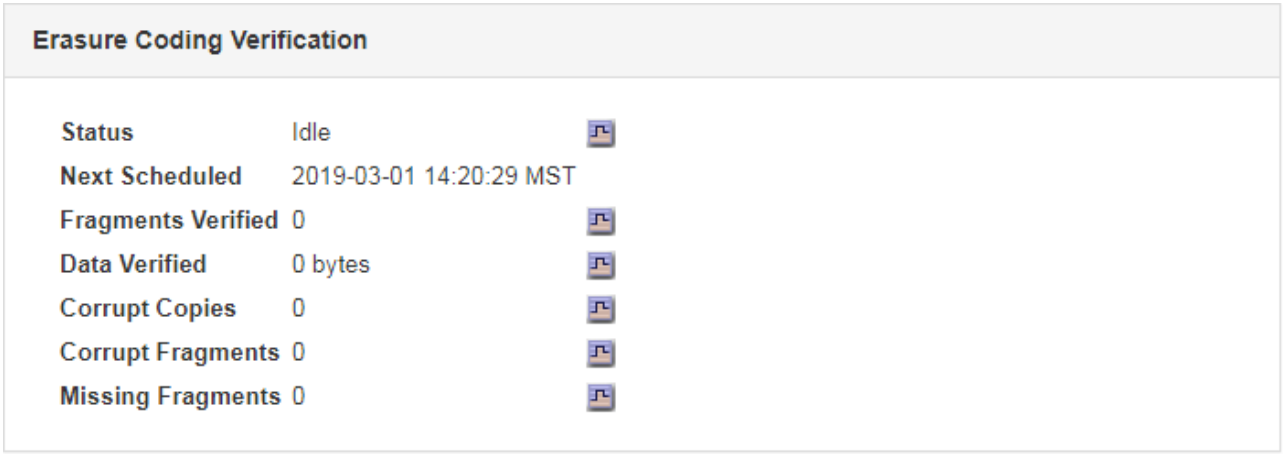
1. Sélectionnez **noeuds**.
2. Sélectionnez ***Storage Node*** > **objets**.
3. Pour vérifier les résultats de vérification :

   - Pour vérifier la vérification des données d'objet répliqué, consultez les attributs de la section Vérification.



Cliquez sur le nom d'un attribut dans le tableau pour afficher le texte d'aide.

   - Pour vérifier la vérification des fragments avec code d'effacement, sélectionnez ***Storage Node*** > **ILM** et examinez les attributs dans la table Vérification du code d'effacement.



Cliquez sur le nom d'un attribut dans le tableau pour afficher le texte d'aide.

Informations associées

"Vérification de l'intégrité des objets"

Contrôle des événements

Vous pouvez surveiller les événements détectés par un nœud de grille, y compris les événements personnalisés que vous avez créés pour suivre les événements qui sont consignés sur le serveur syslog. Le message dernier événement affiché dans Grid Manager fournit plus d'informations sur l'événement le plus récent.

Les messages d'événement sont également répertoriés dans le `/var/local/log/bycast-err.log` fichier journal.

L'alarme SMTT (Total Events) peut être déclenchée à plusieurs reprises par des problèmes tels que des problèmes de réseau, des pannes de courant ou des mises à niveau. Cette section contient des informations sur l'analyse des événements afin de mieux comprendre pourquoi ces alarmes se sont produites. Si un événement s'est produit à cause d'un problème connu, il est possible de réinitialiser les compteurs d'événements.

Vérification des événements à partir de la page nœuds

La page nœuds répertorie les événements système pour chaque nœud de grid.

1. Sélectionnez **noeuds**.
2. Sélectionnez ***grid node*** > **Events**.
3. En haut de la page, déterminez si un événement est affiché pour **dernier événement**, qui décrit le dernier événement détecté par le nœud de la grille.

   L'événement est retransmis en compte à partir du nœud de la grille et inclut tous les messages du journal avec un niveau de gravité D'ERREUR ou CRITIQUE.

4. Consultez le tableau pour voir si le nombre d'événements ou d'erreurs n'est pas nul.
5. Après avoir résolu les problèmes, cliquez sur **Réinitialiser les nombres d'événements** pour remettre les nombres à zéro.

Vérification des événements à partir de la page topologie de la grille

La page topologie de la grille répertorie également les événements système pour chaque nœud de la grille.

1. Sélectionnez **support** > **Outils** > **topologie de grille**.
2. Sélectionnez ***site*** > ***grid node*** > **SSM** > **Events** > **Overview** > **main**.

Informations associées

"Réinitialisation du nombre d'événements"

"Référence des fichiers journaux"

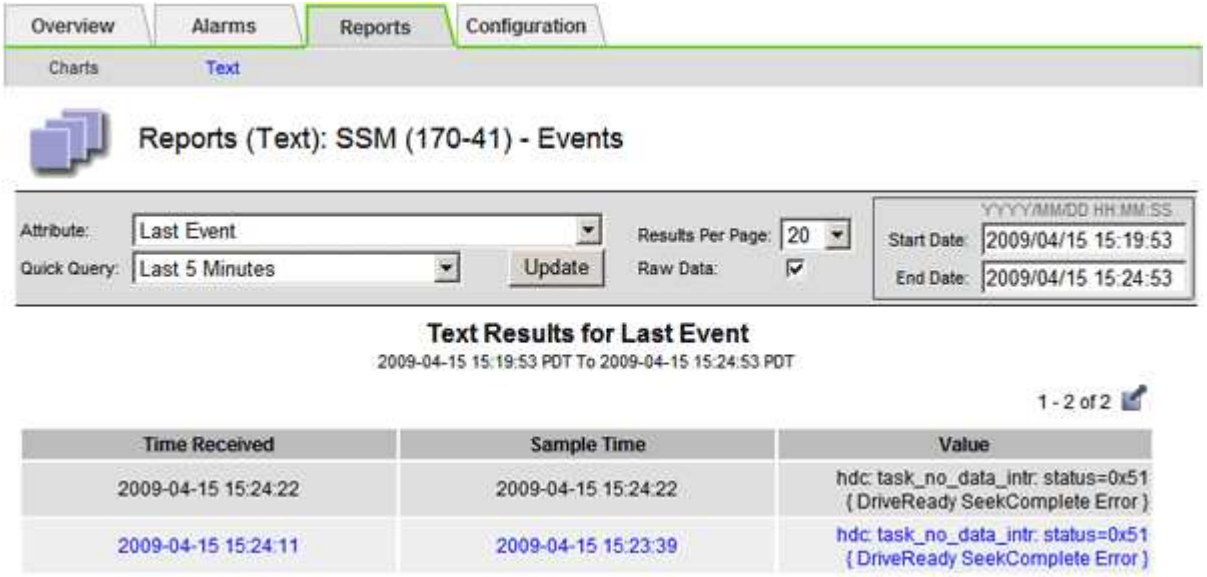
Vérification des événements précédents

Vous pouvez générer une liste de messages d'événement précédents pour vous aider à isoler les problèmes qui se sont produits auparavant.

1. Sélectionnez **support** > **Outils** > **topologie de grille**.
2. Sélectionnez ***site*** > ***grid node*** > **SSM** > **Events** > **Reports**.
3. Sélectionnez **texte**.

   L'attribut **dernier événement** n'apparaît pas dans la vue graphiques.

4. Remplacez **attribut** par **dernier événement**.
5. Vous pouvez également sélectionner une période pour **requête rapide**.
6. Cliquez sur **mettre à jour**.



Informations associées

"Utilisation de graphiques et de rapports"

Réinitialisation du nombre d'événements

Une fois les événements système résolus, vous pouvez réinitialiser le nombre d'événements à zéro.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer de l'autorisation Configuration de la page de topologie de la grille.

Étapes

1. Sélectionnez **Nodes** > ***Grid Node*** > **Events**.
2. Assurez-vous que tout événement avec un compte supérieur à 0 a été résolu.
3. Cliquez sur **Réinitialiser le nombre d'événements**.

Events

Last Event No Events

Description	Count
Abnormal Software Events	0
Account Service Events	0
Cassandra Heap Out Of Memory Errors	0
Cassandra unhandled exceptions	0
Chunk Service Events	0
Custom Events	0
Data-Mover Service Events	0
File System Errors	0
Forced Termination Events	0
Hotfix Installation Failure Events	0
I/O Errors	0
IDE Errors	0
Identity Service Events	0
Kernel Errors	0
Kernel Memory Allocation Failure	0
Keystone Service Events	0
Network Receive Errors	0
Network Transmit Errors	0
Node Errors	0
Out Of Memory Errors	0
Replicated State Machine Service Events	0
SCSI Errors	0
Stat Service Events	0
Storage Hardware Events	0
System Time Events	0

Reset event counts

Les événements personnalisés vous permettent de suivre tous les événements utilisateur du noyau, du démon, de l'erreur et du niveau critique consignés sur le serveur syslog. Un événement personnalisé peut être utile pour surveiller l'occurrence des messages du journal système (et donc les événements de sécurité réseau et les défaillances matérielles).

Description de la tâche

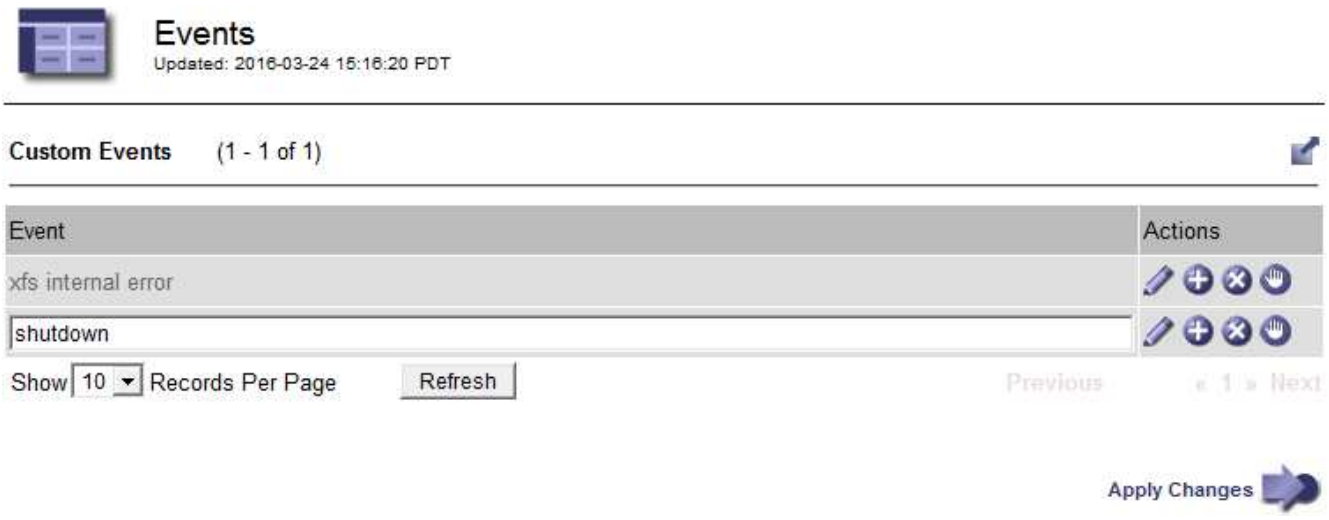
Pensez à créer des événements personnalisés pour surveiller les problèmes récurrents. Les considérations suivantes s'appliquent aux événements personnalisés.

- Après la création d'un événement personnalisé, chaque occurrence de celui-ci est surveillée. Vous pouvez afficher une valeur de nombre cumulé pour tous les événements personnalisés sur la page **Nodes** > ***grid node*** > **Events**.
- Pour créer un événement personnalisé basé sur des mots-clés dans `/var/log/messages` ou `/var/log/syslog` les fichiers journaux de 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/log/messages` ou `/var/log/syslog` les fichiers seront mis en correspondance à moins qu'ils ne satisfassent aux exigences indiquées ci-dessus.

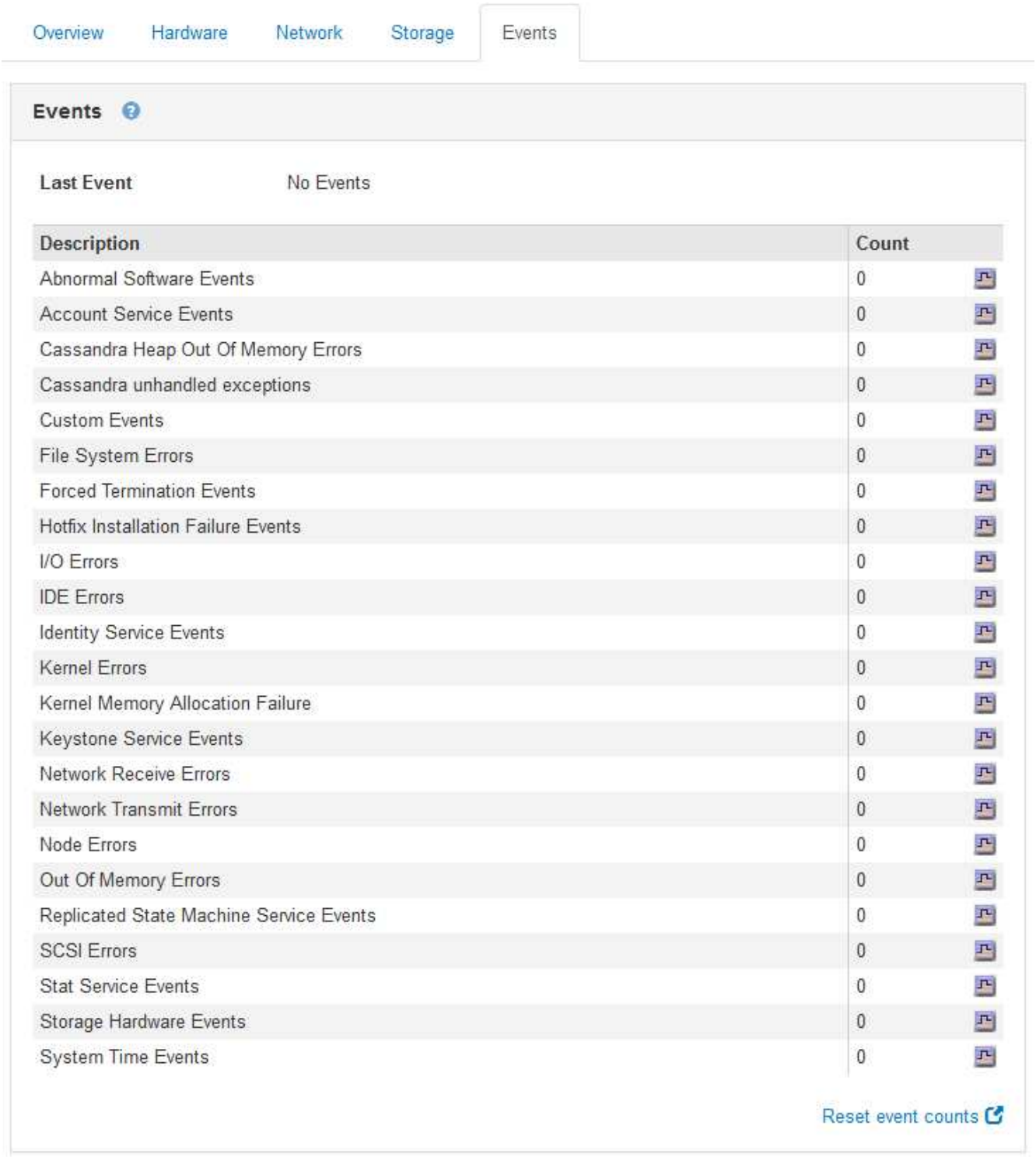
Étapes

1. Sélectionnez **Configuration** > **surveillance** > **événements**.
2. Cliquez sur **Modifier** (Ou **Insérer** si ce n'est pas le premier événement).
3. Entrez une chaîne d'événement personnalisée, par exemple, l'arrêt



4. Cliquez sur **appliquer les modifications**.
5. Sélectionnez **noeuds**. Sélectionnez ensuite ***grid node*** > **Events**.
6. Localisez l'entrée événements personnalisés dans le tableau Evénements et surveillez la valeur de **Count**.

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



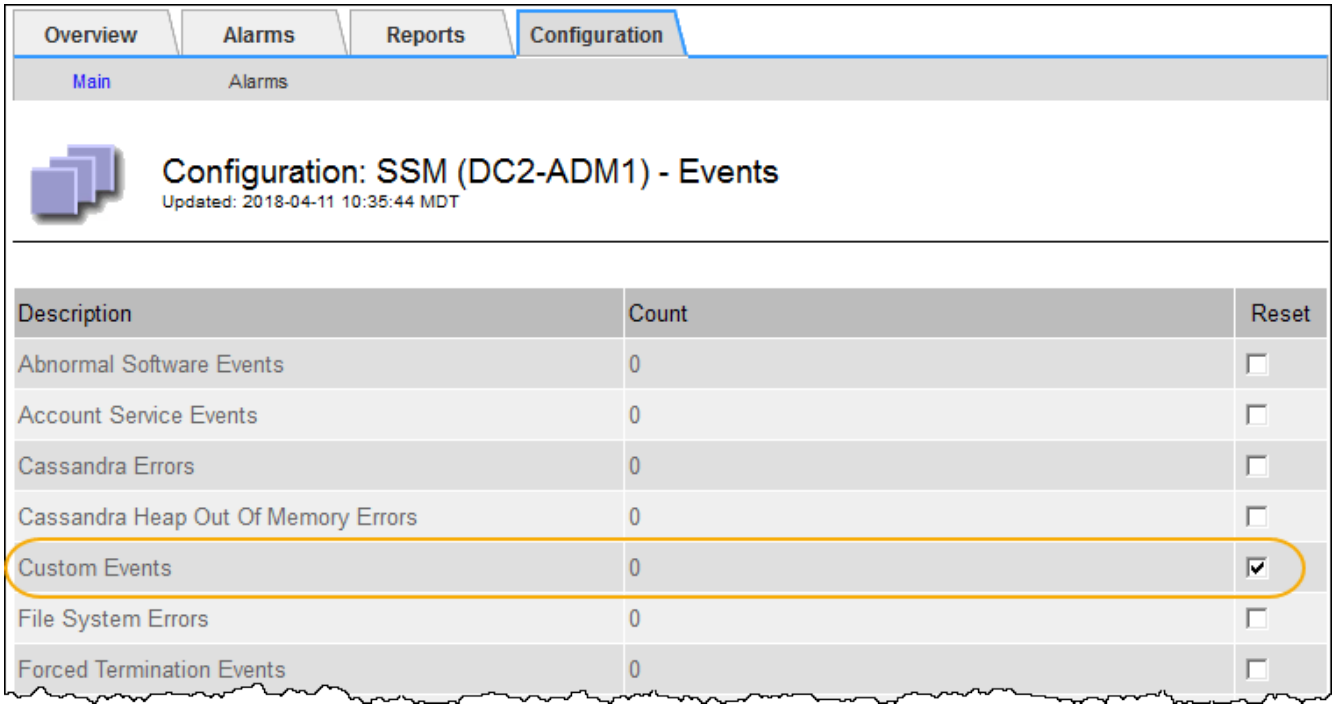
Réinitialisation du nombre d'événements personnalisés à zéro

Si vous souhaitez réinitialiser le compteur uniquement pour les événements personnalisés, vous devez utiliser la page topologie de la grille dans le menu support.

Description de la tâche

La réinitialisation d'un compteur entraîne le déclenchement de l'alarme par l'événement suivant. En revanche, lorsque vous reconnaissez une alarme, celle-ci n'est déclenchée que si le niveau de seuil suivant est atteint.

1. Sélectionnez **support** > **Outils** > **topologie de grille**.
2. Sélectionnez ***GRID node*** > **SSM** > **Events** > **Configuration** > **main**.
3. Cochez la case **Réinitialiser** pour les événements personnalisés.



4. Cliquez sur **appliquer les modifications**.

Vérification des messages d'audit

Les messages d'audit vous permettent de mieux comprendre le fonctionnement détaillé de votre système StorageGRID. Vous pouvez utiliser les journaux d'audit pour résoudre les problèmes et évaluer les performances.

Pendant le fonctionnement normal du système, tous les services StorageGRID génèrent des messages d'audit comme suit :

- Les messages d'audit système sont liés au système d'audit lui-même, à l'état du nœud de la grille, à l'activité des tâches à l'échelle du système et aux opérations de sauvegarde du service.
- Les messages d'audit du stockage objet sont liés au stockage et à la gestion des objets dans StorageGRID, notamment le stockage objet et les récupérations, les transferts entre nœuds de grille et nœuds de grille, et les vérifications.
- Les messages d'audit de lecture et d'écriture du client sont consignés lorsqu'une application client S3 ou Swift demande de créer, de modifier ou de récupérer un objet.
- Les messages d'audit de gestion consigne les demandes des utilisateurs vers l'API de gestion.

Chaque nœud d'administration stocke les messages d'audit dans des fichiers texte. Le partage d'audit contient le fichier actif (audit.log) ainsi que les journaux d'audit compressés des jours précédents.

Pour faciliter l'accès aux journaux d'audit, vous pouvez configurer l'accès des clients au partage d'audit pour NFS et CIFS (obsolète). Vous pouvez également accéder aux fichiers journaux d'audit directement à partir de la ligne de commande du nœud d'administration.

Pour plus de détails sur le fichier journal d'audit, le format des messages d'audit, les types de messages d'audit et les outils disponibles pour analyser les messages d'audit, reportez-vous aux instructions pour les messages d'audit. Pour savoir comment configurer l'accès client d'audit, reportez-vous aux instructions d'administration de StorageGRID.

Informations associées

"Examiner les journaux d'audit"

"Administrer StorageGRID"

Collecte des fichiers journaux et des données système

Vous pouvez utiliser le Gestionnaire de grille pour récupérer les fichiers journaux et les données système (y compris les données de configuration) de votre système StorageGRID.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.
- Vous devez disposer de la phrase secrète pour le provisionnement.

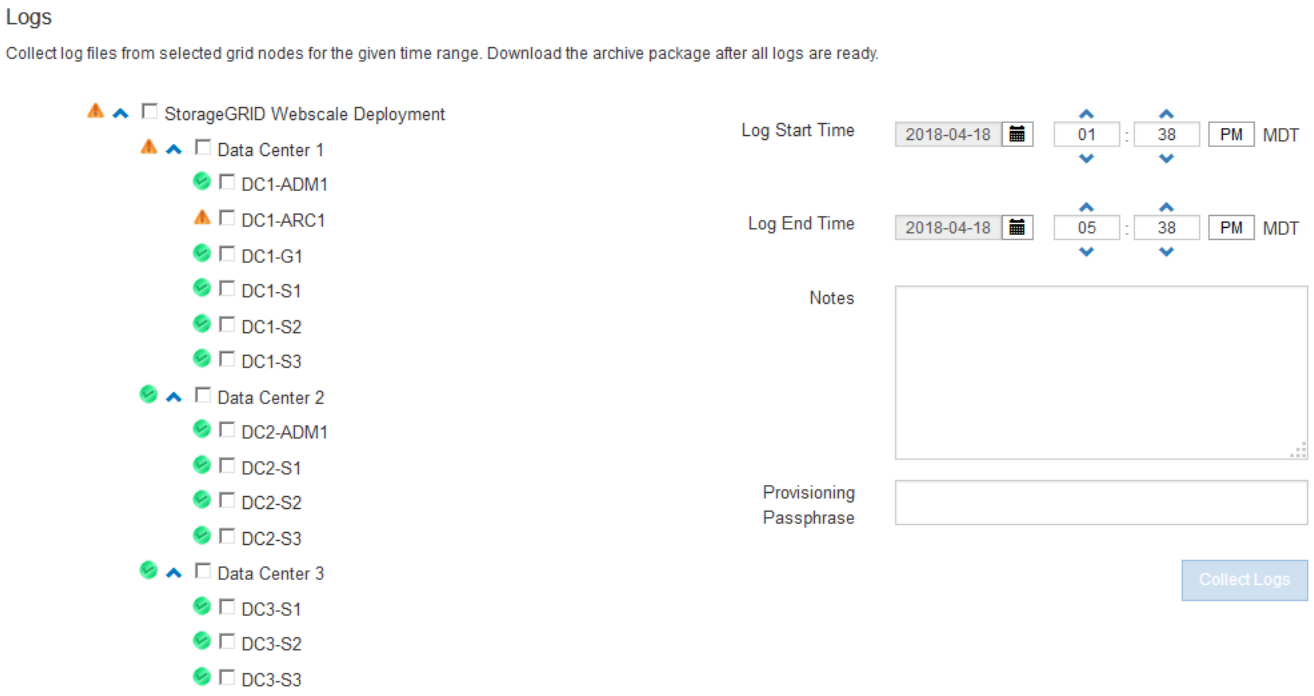
À propos de ce taak

Vous pouvez utiliser Grid Manager pour recueillir des fichiers journaux, des données système et des données de configuration à partir de n'importe quel nœud de la grille pour la période sélectionnée. Les données sont collectées et archivées dans un fichier .tar.gz que vous pouvez ensuite télécharger sur votre ordinateur local.

Étant donné que les fichiers journaux d'application peuvent être très volumineux, le répertoire de destination où vous téléchargez les fichiers journaux archivés doit disposer d'au moins 1 Go d'espace libre.

Étapes

1. Sélectionnez **support** > **Outils** > **journaux**.



2. Sélectionnez les nœuds de grille pour lesquels vous souhaitez collecter les fichiers journaux.

   Si nécessaire, vous pouvez collecter des fichiers journaux pour l'intégralité de la grille ou un site de data Center.

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

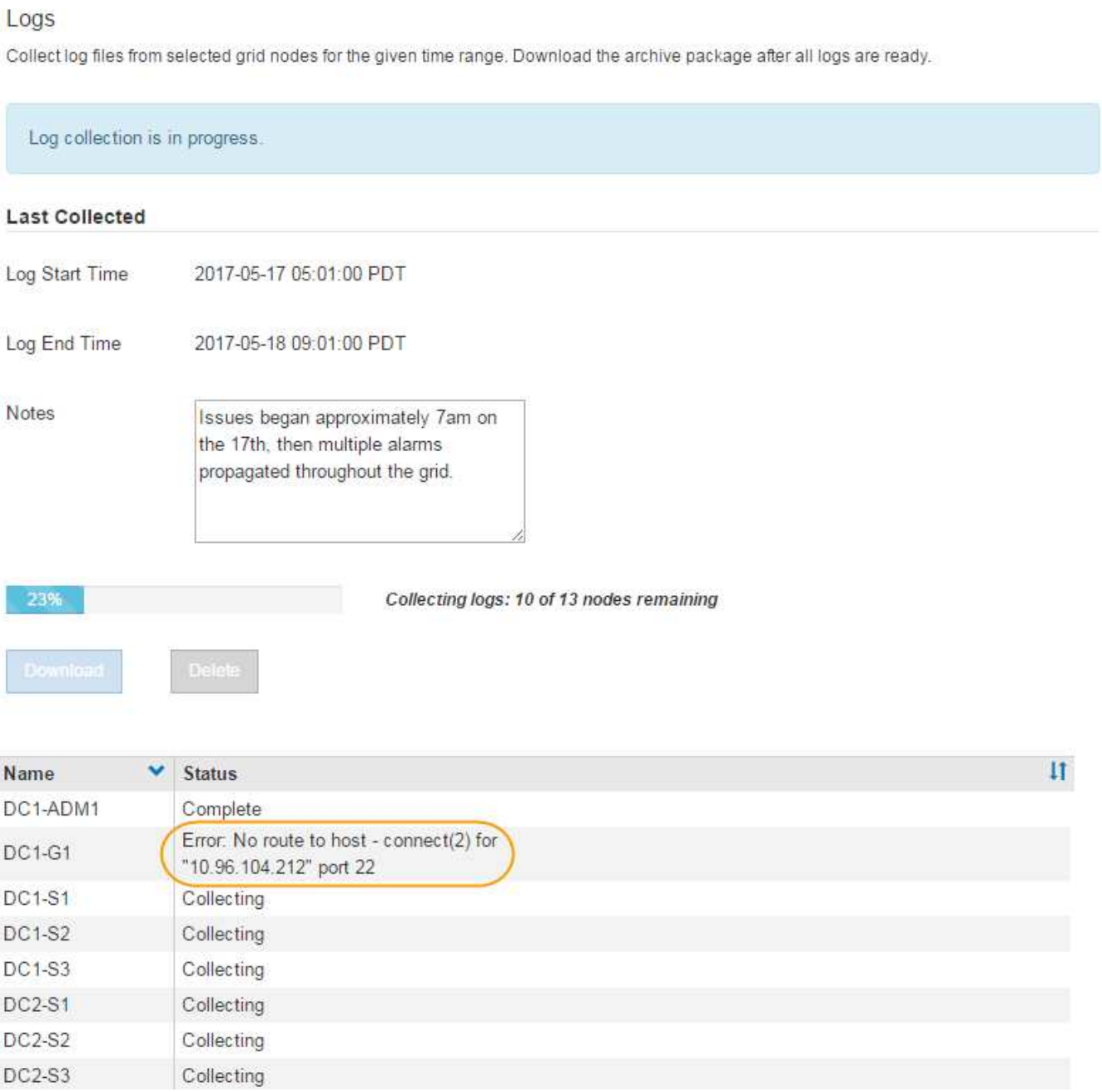
   Si vous sélectionnez une période très longue ou que vous collectez des journaux de tous les nœuds d'un grand grid, l'archivage des journaux risque de devenir trop volumineux pour être stocké sur un nœud, ou trop volumineux pour être collecté sur le nœud d'administration principal pour le téléchargement. Dans ce cas, vous devez redémarrer la collecte de journaux avec un jeu de données plus petit.

4. Vous pouvez également saisir des notes sur les fichiers journaux que vous recueillez dans la zone de texte **Notes**.

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

5. Saisissez le mot de passe de provisionnement de votre système StorageGRID dans la zone de texte **phrase de passe de provisionnement**.
6. Cliquez sur **collecter les journaux**.

   Lorsque vous soumettez une nouvelle demande, la collection précédente de fichiers journaux est supprimée.



Vous pouvez utiliser la page journaux pour surveiller la progression de la collecte des fichiers journaux pour chaque nœud de la grille.

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

7. Cliquez sur **Télécharger** lorsque la collecte des fichiers journaux est terminée.

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

Une fois que vous avez terminé

Vous pouvez télécharger à nouveau le package d'archivage des fichiers journaux ultérieurement si nécessaire.

Vous pouvez également cliquer sur **Supprimer** pour supprimer le paquet d'archives de fichiers journaux et libérer de l'espace disque. Le progiciel d'archivage du fichier journal actuel est automatiquement supprimé lors de la prochaine collecte de fichiers journaux.

Informations associées

"Référence des fichiers journaux"

Déclenchement manuel de l'un des messages AutoSupport

Pour aider le support technique à résoudre les problèmes liés à votre système StorageGRID, vous pouvez déclencher manuellement un message AutoSupport à envoyer.

Ce dont vous avez besoin

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

Étapes

1. Sélectionnez **support** > **Outils** > **AutoSupport**.

   La page AutoSupport s'affiche avec l'onglet **Paramètres** sélectionné.

2. Sélectionnez **Envoyer AutoSupport déclenchée par l'utilisateur**.

   StorageGRID tente d'envoyer un message AutoSupport au support technique. Si la tentative réussit, les valeurs **résultat le plus récent** et **dernier temps** réussi dans l'onglet **Résultats** sont mises à jour. En cas de problème, la valeur **résultat** la plus récente est mise à jour sur "échec" et StorageGRID n'essaie pas d'envoyer à nouveau le message AutoSupport.

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

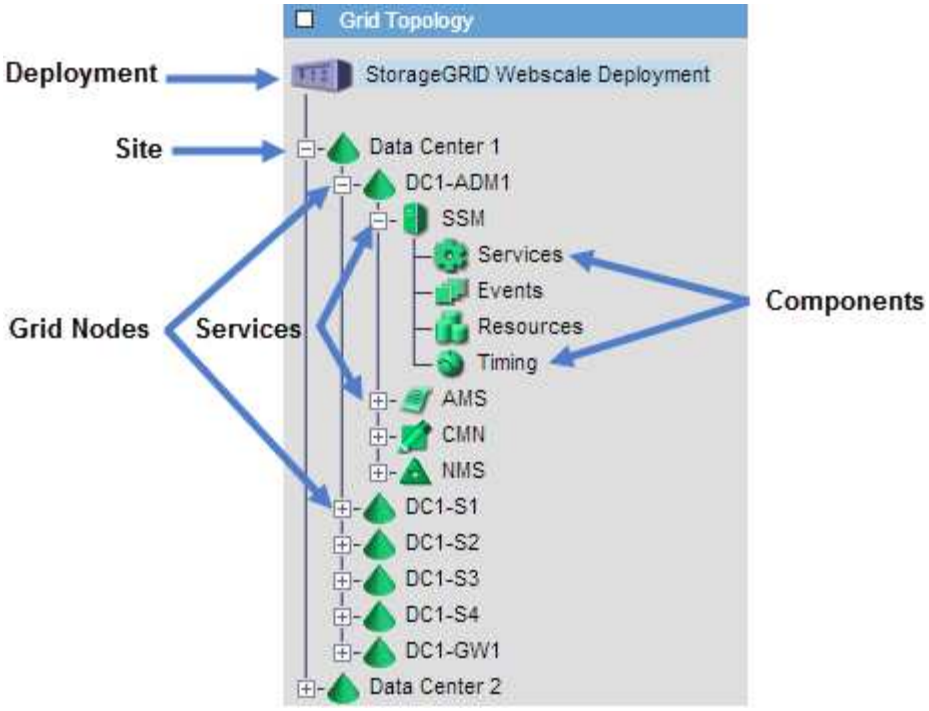
Informations associées

"Configuration des paramètres du serveur de messagerie pour les alarmes (système hérité)"

Affichage de l'arborescence de la grille topologique

L'arborescence de la grille topologie permet d'accéder à des informations détaillées sur les éléments du système StorageGRID, notamment les sites, les nœuds de la grille, les services et les composants. Dans la plupart des cas, il vous suffit d'accéder à l'arborescence de la grille topologique lorsque vous y êtes invité ou lorsque vous collaborez avec le support technique.

Pour accéder à l'arborescence de la topologie de grille, sélectionnez **support** > **Outils** > **topologie de grille**.



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

L'examen des metrics de support

Lorsque vous dépannez un problème, vous pouvez consulter les graphiques et les metrics détaillés de votre système StorageGRID en collaboration avec le support technique.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

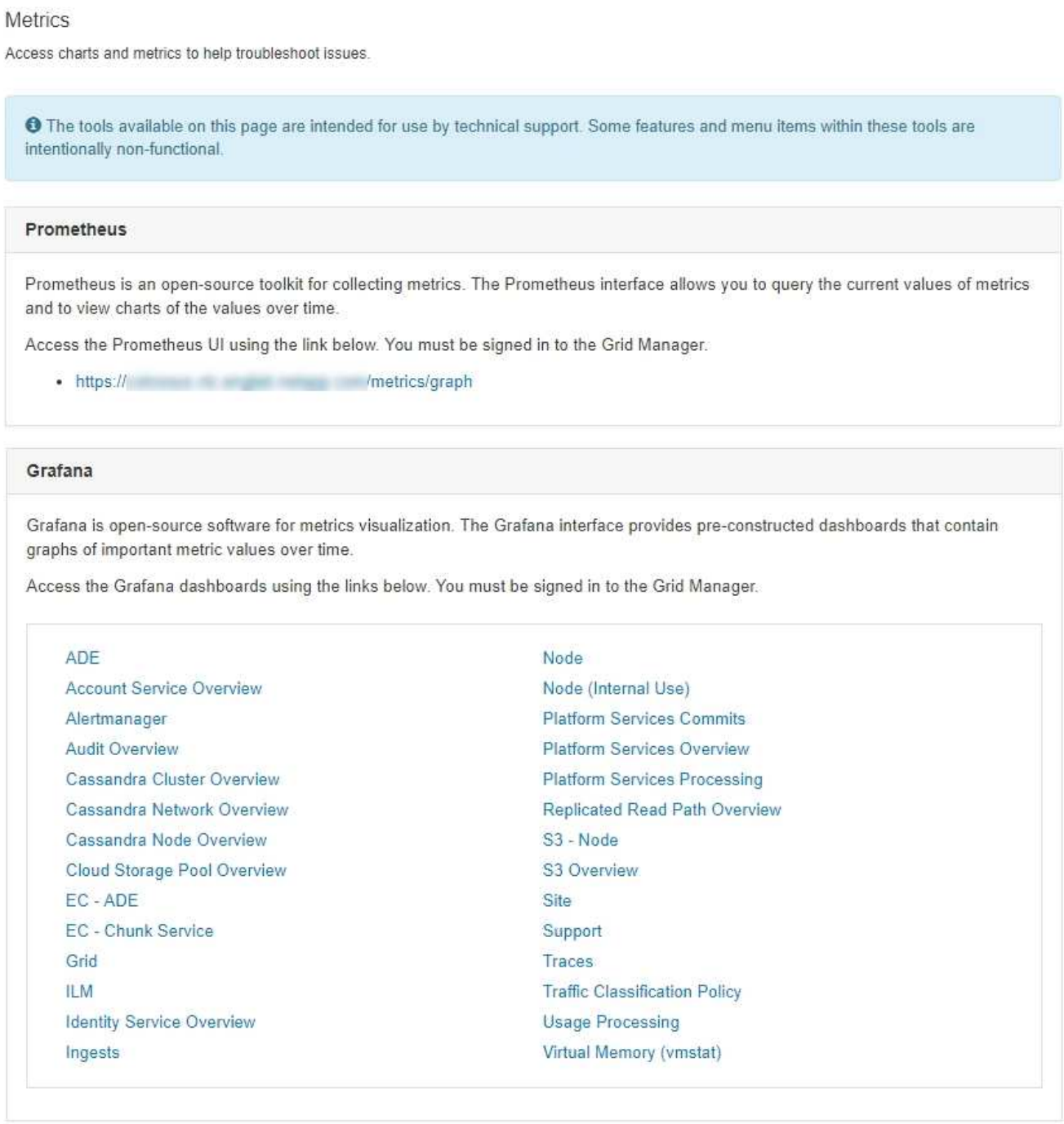
La page Metrics vous permet d'accéder aux interfaces utilisateur de Prometheus et Grafana. Prometheus est un logiciel open source qui permet de collecter des metrics. Grafana est un logiciel open source permettant de visualiser les metrics.

> ⓘ Les outils disponibles sur la page métriques sont destinés au support technique. Certaines fonctions et options de menu de ces outils sont intentionnellement non fonctionnelles et peuvent faire l'objet de modifications.

Étapes

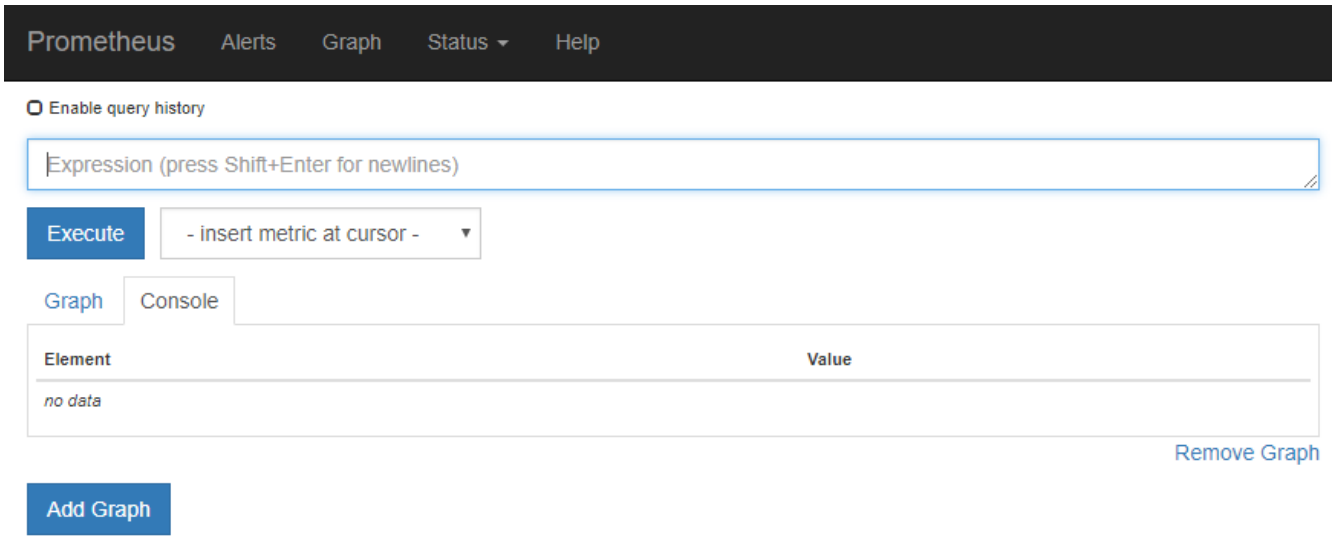
1. Comme indiqué par le support technique, sélectionnez **support** > **Outils** > **métriques**.

   La page métriques s'affiche.



2. Pour interroger les valeurs actuelles des metrics StorageGRID et afficher les graphiques des valeurs dans le temps, cliquez sur le lien de la section Prometheus.

   L'interface Prometheus s'affiche. Vous pouvez utiliser cette interface pour exécuter des requêtes sur les mesures StorageGRID disponibles et pour générer des graphiques sur les mesures StorageGRID au fil du temps.



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

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

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

Informations associées

"Metrics Prometheus couramment utilisés"

Exécution des diagnostics

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

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

La page Diagnostics effectue un ensemble de contrôles de diagnostic sur l'état actuel de la grille. Chaque vérification de diagnostic peut avoir l'un des trois États suivants :

- **Normal** : toutes les valeurs sont comprises dans la plage normale.

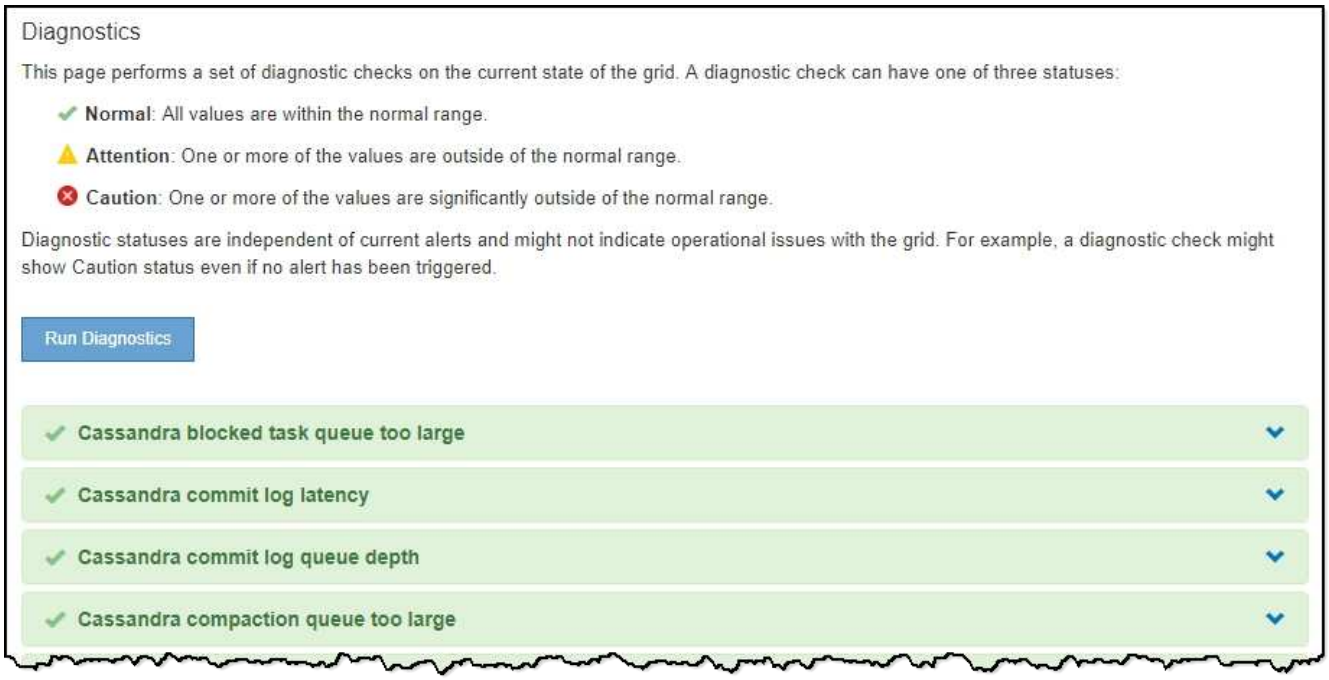
- ⚠ **Attention** : une ou plusieurs valeurs sont hors de la plage normale.
- ⊗ **Attention** : une ou plusieurs valeurs sont significativement en dehors de la plage normale.

Les États de diagnostic sont indépendants des alertes en cours et peuvent ne pas indiquer de problèmes opérationnels dans la grille. Par exemple, une vérification de diagnostic peut afficher l'état de mise en garde même si aucune alerte n'a été déclenchée.

Étapes

1. Sélectionnez **support** > **Outils** > **Diagnostics**.

   La page Diagnostics s'affiche et répertorie les résultats de chaque vérification de diagnostic. Dans l'exemple, tous les diagnostics ont un état Normal.



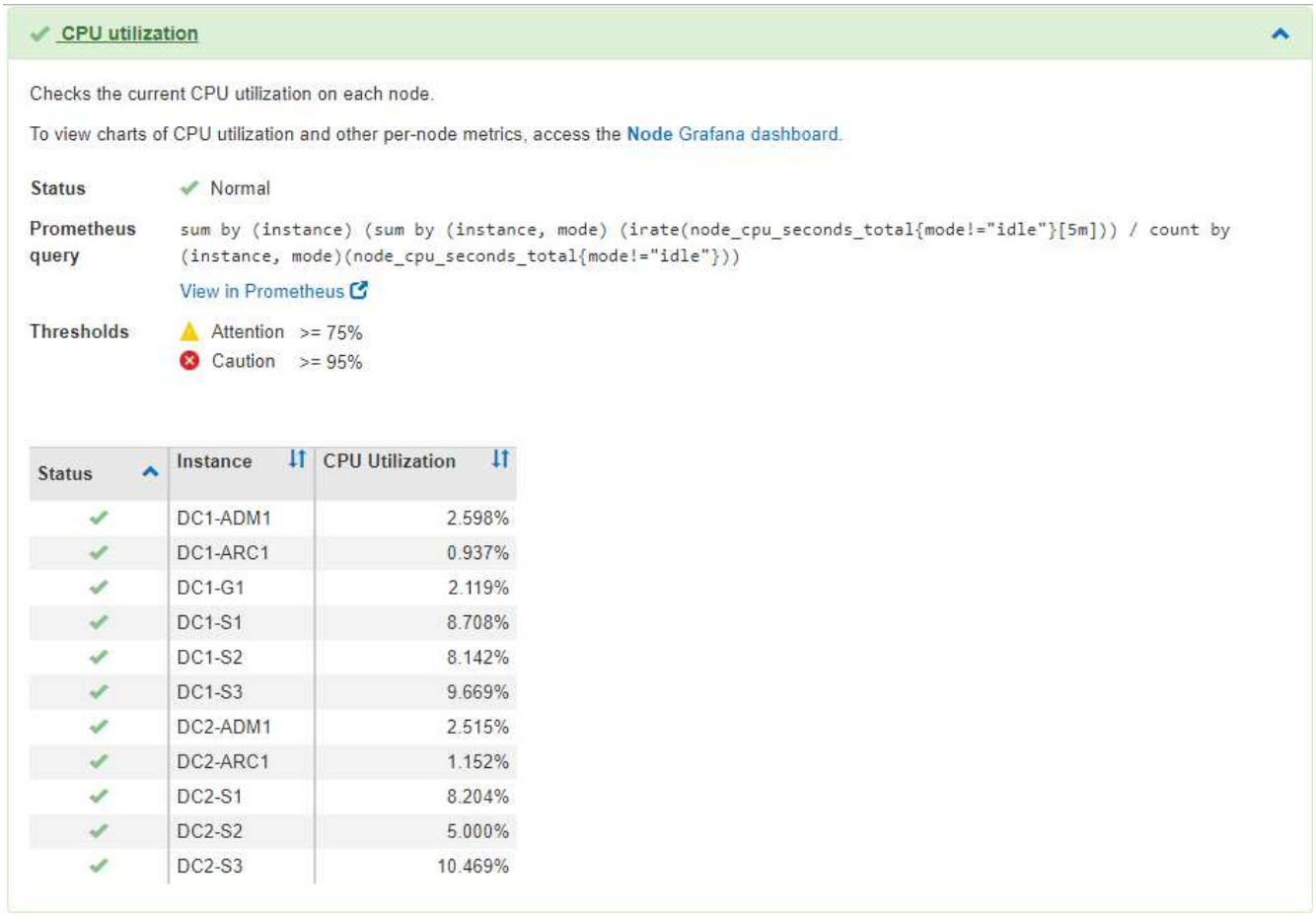
2. Pour en savoir plus sur un diagnostic spécifique, cliquez n'importe où dans la ligne.

   Des détails sur le diagnostic et ses résultats actuels s'affichent. Les informations suivantes sont répertoriées :

   - **Etat** : état actuel de ce diagnostic : normal, attention ou attention.
   - **Requête Prometheus** : si utilisé pour le diagnostic, l'expression Prometheus qui a été utilisée pour générer les valeurs d'état. (Une expression Prometheus n'est pas utilisée pour tous les diagnostics.)
   - **Seuils** : si disponibles pour le diagnostic, les seuils définis par le système pour chaque état de diagnostic anormal. (Les valeurs de seuil ne sont pas utilisées pour tous les diagnostics.)

     ⓘ Vous ne pouvez pas modifier ces seuils.

   - **Valeurs d'état** : tableau indiquant l'état et la valeur du diagnostic dans l'ensemble du système StorageGRID. Dans cet exemple, l'utilisation actuelle du processeur pour chaque nœud d'un système StorageGRID est indiquée. Toutes les valeurs de nœud sont inférieures aux seuils attention et mise en garde, de sorte que l'état général du diagnostic est Normal.



3. **Facultatif** : pour afficher les graphiques Grafana relatifs à ce diagnostic, cliquez sur le lien **Dashboard**.

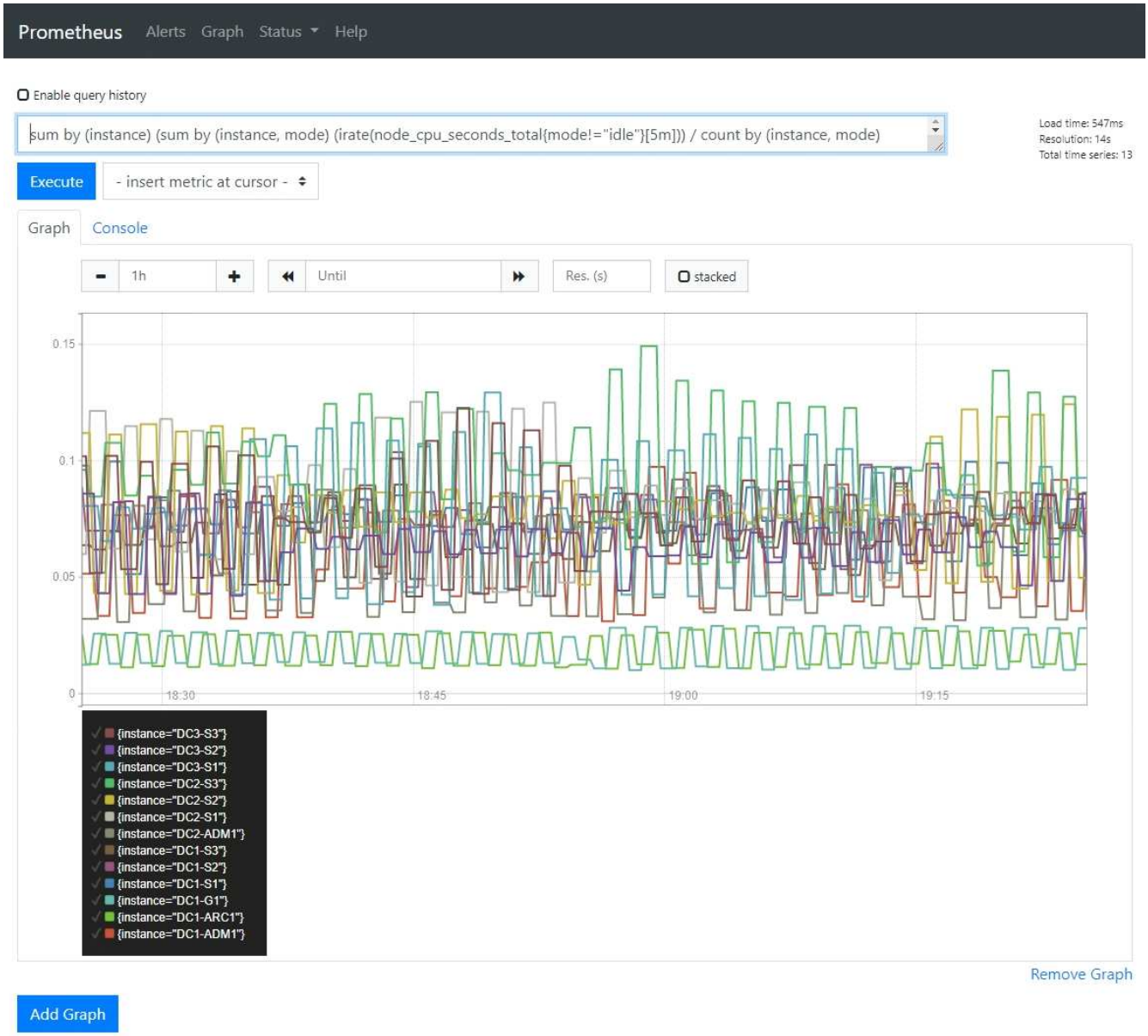
   Ce lien ne s'affiche pas pour tous les diagnostics.

   Le tableau de bord associé à Grafana s'affiche. Dans cet exemple, le tableau de bord des nœuds apparaît et affiche l'utilisation des CPU dans le temps pour ce nœud, ainsi que d'autres graphiques Grafana pour le nœud.

   Vous pouvez également accéder aux tableaux de bord pré-construits Grafana à partir de la section **support** > **Outils** > **Metrics**.

4. **Facultatif** : pour afficher un graphique de l'expression Prometheus au fil du temps, cliquez sur **Afficher dans Prometheus**.

   Un graphique Prometheus de l'expression utilisée dans le diagnostic s'affiche.



Informations associées

"L'examen des metrics de support"

"Metrics Prometheus couramment utilisés"

Création d'applications de surveillance personnalisées

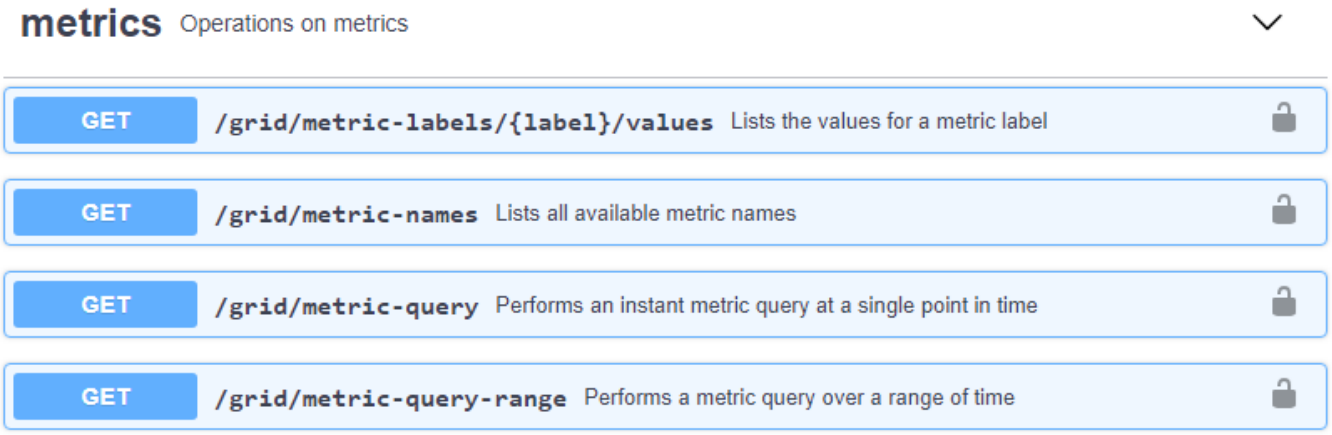
Vous pouvez créer des applications et des tableaux de bord de surveillance personnalisés à l'aide des metrics StorageGRID disponibles dans l'API de gestion du grid.

Si vous souhaitez contrôler les mesures qui ne s'affichent pas sur une page existante du Gestionnaire de grilles ou si vous souhaitez créer des tableaux de bord personnalisés pour StorageGRID, vous pouvez utiliser l'API de gestion des grilles pour interroger les metrics StorageGRID.

Vous pouvez également accéder directement à des metrics Prometheus à l'aide d'un outil de surveillance externe tel que Grafana. Pour utiliser un outil externe, vous devez télécharger ou générer un certificat de client

d'administration afin de permettre à StorageGRID d'authentifier l'outil pour la sécurité. Voir les instructions d'administration de StorageGRID.

Pour afficher les opérations de l'API de metrics, y compris la liste complète des metrics disponibles, accédez au Gestionnaire de grille et sélectionnez **aide** > **Documentation API** > **metrics**.



Les détails de la mise en œuvre d'une application de surveillance personnalisée dépassent le cadre de ce guide.

Informations associées

"Administrer StorageGRID"

Référence des alertes

Le tableau suivant répertorie toutes les alertes StorageGRID par défaut. Si nécessaire, vous pouvez créer des règles d'alerte personnalisées en fonction de votre approche de gestion du système.

Consultez des informations sur les metrics Prometheus les plus utilisés pour en savoir plus sur les metrics utilisés dans certaines de ces alertes.

Nom de l'alerte	Description et actions recommandées
Batterie de l'appareil expirée	La batterie du contrôleur de stockage de l'appareil a expiré. 1. Remplacer la batterie. Les étapes de retrait et de remplacement d'une batterie sont incluses dans la procédure de remplacement d'un contrôleur de stockage dans les instructions d'installation et de maintenance de l'appareil. ◦ "Dispositifs de stockage SG6000" ◦ "Appliances de stockage SG5700" ◦ "Appliances de stockage SG5600" 2. Si cette alerte persiste, contactez le support technique.

Nom de l’alerte	Description et actions recommandées
La batterie de l’appareil est défectueuse	La batterie du contrôleur de stockage de l’appareil est défectueuse. 1. Remplacer la batterie. Les étapes de retrait et de remplacement d’une batterie sont incluses dans la procédure de remplacement d’un contrôleur de stockage dans les instructions d’installation et de maintenance de l’appareil. ◦ "Dispositifs de stockage SG6000" ◦ "Appliances de stockage SG5700" ◦ "Appliances de stockage SG5600" 2. Si cette alerte persiste, contactez le support technique.
La capacité de la batterie de l’appareil est insuffisante	La capacité de la batterie du contrôleur de stockage de l’appareil est insuffisante. 1. Remplacer la batterie. Les étapes de retrait et de remplacement d’une batterie sont incluses dans la procédure de remplacement d’un contrôleur de stockage dans les instructions d’installation et de maintenance de l’appareil. ◦ "Dispositifs de stockage SG6000" ◦ "Appliances de stockage SG5700" ◦ "Appliances de stockage SG5600" 2. Si cette alerte persiste, contactez le support technique.
La batterie de l’appareil est presque déchargée	La batterie du contrôleur de stockage de l’appliance arrive à expiration. 1. Remplacez la batterie bientôt. Les étapes de retrait et de remplacement d’une batterie sont incluses dans la procédure de remplacement d’un contrôleur de stockage dans les instructions d’installation et de maintenance de l’appareil. ◦ "Dispositifs de stockage SG6000" ◦ "Appliances de stockage SG5700" ◦ "Appliances de stockage SG5600" 2. Si cette alerte persiste, contactez le support technique.

Nom de l’alerte	Description et actions recommandées
Batterie de l’appareil retirée	La batterie du contrôleur de stockage de l’appareil est manquante. 1. Installer une batterie. Les étapes de retrait et de remplacement d’une batterie sont incluses dans la procédure de remplacement d’un contrôleur de stockage dans les instructions d’installation et de maintenance de l’appareil. ◦ "Dispositifs de stockage SG6000" ◦ "Appliances de stockage SG5700" ◦ "Appliances de stockage SG5600" 2. Si cette alerte persiste, contactez le support technique.
Batterie de l’appareil trop chaude	La batterie du contrôleur de stockage de l’appareil est en surchauffe. 1. Déterminez s’il y a une autre alerte affectant ce nœud. Cette alerte est peut-être résolue lorsque vous résolvez l’autre alerte. 2. Rechercher les causes possibles de l’augmentation de la température, comme une panne du ventilateur ou du système CVC. 3. Si cette alerte persiste, contactez le support technique.
Erreur de communication du BMC de l’appliance	La communication avec le contrôleur de gestion de la carte mère (BMC) a été perdue. 1. Vérifiez que le contrôleur BMC fonctionne normalement. Sélectionnez **Nodes**, puis sélectionnez l’onglet **Hardware** pour le nœud de l’appliance. Recherchez le champ IP BMC du contrôleur de calcul et recherchez cette adresse IP. 2. Essayez de restaurer les communications BMC en plaçant le nœud en mode de maintenance, puis en mettant l’appliance hors tension puis sous tension. Consultez les instructions d’installation et de maintenance de votre appareil. ◦ "Dispositifs de stockage SG6000" ◦ "SG100 etamp ; appareils de services SG1000" 3. Si cette alerte persiste, contactez le support technique.

Nom de l’alerte	Description et actions recommandées
Échec du périphérique de sauvegarde du cache de l’appliance	Échec d’un périphérique de sauvegarde de cache persistant. 1. Déterminez s’il y a une autre alerte affectant ce nœud. Cette alerte est peut-être résolue lorsque vous résolvez l’autre alerte. 2. Contactez l’assistance technique.
Capacité insuffisante du périphérique de sauvegarde en cache de l’appliance	La capacité du périphérique de sauvegarde du cache est insuffisante.Contactez le support technique.
Dispositif de sauvegarde cache de l’appliance protégé en écriture	Un périphérique de sauvegarde de cache est protégé en écriture.Contactez le support technique.
La taille de la mémoire cache de l’appliance ne correspond pas	Les deux contrôleurs de l’appliance ont des tailles de cache différentes.Contactez l’assistance technique.
La température du châssis du contrôleur de calcul de l’appliance est trop élevée	La température du contrôleur de calcul d’une appliance StorageGRID a dépassé le seuil nominal. 1. Vérifier les composants matériels pour rechercher les conditions de surchauffe et suivre les actions recommandées : ◦ Si vous disposez d’un SG100, SG1000 ou SG6000, utilisez le BMC. ◦ Si vous disposez d’une appliance SG5600 ou SG5700, utilisez SANtricity System Manager. 2. Si nécessaire, remplacer l’organe. Consultez les instructions d’installation et de maintenance du matériel de votre appareil : ◦ "Dispositifs de stockage SG6000" ◦ "Appliances de stockage SG5700" ◦ "Appliances de stockage SG5600" ◦ "SG100 etamp ; appareils de services SG1000"

Nom de l’alerte	Description et actions recommandées
Température trop élevée du processeur du contrôleur de calcul de l’appliance	La température du processeur dans le contrôleur de calcul d’une appliance StorageGRID a dépassé le seuil nominal. 1. Vérifier les composants matériels pour rechercher les conditions de surchauffe et suivre les actions recommandées : ◦ Si vous disposez d’un SG100, SG1000 ou SG6000, utilisez le BMC. ◦ Si vous disposez d’une appliance SG5600 ou SG5700, utilisez SANtricity System Manager. 2. Si nécessaire, remplacer l’organe. Consultez les instructions d’installation et de maintenance du matériel de votre appareil : ◦ "Dispositifs de stockage SG6000" ◦ "Appliances de stockage SG5700" ◦ "Appliances de stockage SG5600" ◦ "SG100 etamp ; appareils de services SG1000"
Le contrôleur de calcul de l’appliance doit faire attention	Une défaillance matérielle a été détectée dans le contrôleur de calcul d’une appliance StorageGRID. 1. Rechercher des erreurs sur les composants matériels et suivre les actions recommandées : ◦ Si vous disposez d’un SG100, SG1000 ou SG6000, utilisez le BMC. ◦ Si vous disposez d’une appliance SG5600 ou SG5700, utilisez SANtricity System Manager. 2. Si nécessaire, remplacer l’organe. Consultez les instructions d’installation et de maintenance du matériel de votre appareil : ◦ "Dispositifs de stockage SG6000" ◦ "Appliances de stockage SG5700" ◦ "Appliances de stockage SG5600" ◦ "SG100 etamp ; appareils de services SG1000"

Nom de l'alerte	Description et actions recommandées
L'alimentation A du contrôleur de calcul de l'appliance présente un problème	L'alimentation A du contrôleur de calcul présente un problème. Cette alerte peut indiquer qu'elle est défectueuse ou qu'elle rencontre un problème de puissance. 1. Rechercher des erreurs sur les composants matériels et suivre les actions recommandées : ◦ Si vous disposez d'un SG100, SG1000 ou SG6000, utilisez le BMC. ◦ Si vous disposez d'une appliance SG5600 ou SG5700, utilisez SANtricity System Manager. 2. Si nécessaire, remplacer l'organe. Consultez les instructions d'installation et de maintenance du matériel de votre appareil : ◦ "Dispositifs de stockage SG6000" ◦ "Appliances de stockage SG5700" ◦ "Appliances de stockage SG5600" ◦ "SG100 etamp ; appareils de services SG1000"
L'alimentation B du contrôleur de calcul de l'appliance présente un problème	L'alimentation B du contrôleur de calcul présente un problème. Cette alerte peut indiquer que le bloc d'alimentation est défectueux ou qu'il présente un problème d'alimentation. 1. Rechercher des erreurs sur les composants matériels et suivre les actions recommandées : ◦ Si vous disposez d'un SG100, SG1000 ou SG6000, utilisez le BMC. ◦ Si vous disposez d'une appliance SG5600 ou SG5700, utilisez SANtricity System Manager. 2. Si nécessaire, remplacer l'organe. Consultez les instructions d'installation et de maintenance du matériel de votre appareil : ◦ "Dispositifs de stockage SG6000" ◦ "Appliances de stockage SG5700" ◦ "Appliances de stockage SG5600" ◦ "SG100 etamp ; appareils de services SG1000"

Nom de l’alerte	Description et actions recommandées
Service de surveillance du matériel de calcul de l’appliance bloqué	Le service qui surveille l’état du matériel de stockage a cessé de générer des rapports de données. 1. Vérifiez l’état du service eos-System-status dans le système d’exploitation de base. 2. Si le service est arrêté ou en état d’erreur, redémarrez-le. 3. Si cette alerte persiste, contactez le support technique.
Panne Fibre Channel de l’appliance détectée	La connexion Fibre Channel entre les contrôleurs de stockage et de calcul de l’appliance est problématique. 1. Recherchez des erreurs sur les composants matériels (**nœuds** > ***appliance node*** > **Hardware**). Si le statut de l’un des composants n’est pas « nominal », procédez comme suit : a. Vérifiez que les câbles Fibre Channel entre les contrôleurs sont correctement connectés. b. Assurez-vous que les câbles Fibre Channel sont exempts de plis excessifs. c. Vérifiez que les modules SFP+ sont correctement installés. **Remarque :** si ce problème persiste, le système StorageGRID risque de mettre la connexion problématique hors ligne automatiquement. 1. Au besoin, remplacer les composants. Consultez les instructions d’installation et de maintenance de votre appareil.
Défaillance du port HBA Fibre Channel de l’appliance	Un port HBA Fibre Channel est défectueux ou a échoué.Contactez le support technique.

Nom de l’alerte	Description et actions recommandées
Flash cache de l’appliance ne sont pas optimaux	Les disques utilisés pour la mise en cache SSD ne sont pas optimaux. 1. Remplacez les disques SSD cache. Consultez les instructions d’installation et d’entretien de l’appareil. ◦ "Dispositifs de stockage SG6000" ◦ "Appliances de stockage SG5700" ◦ "Appliances de stockage SG5600" 2. Si cette alerte persiste, contactez le support technique.
Interconnexion de l’appareil/boîtier de la batterie retiré	Le boîtier d’interconnexion/de batterie est manquant. 1. Remplacer la batterie. Les étapes de retrait et de remplacement d’une batterie sont incluses dans la procédure de remplacement d’un contrôleur de stockage dans les instructions d’installation et de maintenance de l’appareil. ◦ "Dispositifs de stockage SG6000" ◦ "Appliances de stockage SG5700" ◦ "Appliances de stockage SG5600" 2. Si cette alerte persiste, contactez le support technique.
Port d’appliance LACP manquant	Aucun port d’une appliance StorageGRID ne participe au lien LACP. 1. Vérifier la configuration du commutateur. Assurez-vous que l’interface est configurée dans le groupe d’agrégation de liens approprié. 2. Si cette alerte persiste, contactez le support technique.

Nom de l'alerte	Description et actions recommandées
L'alimentation générale de l'appareil est dégradée	La puissance d'un dispositif StorageGRID s'est déviée de la tension de fonctionnement recommandée. 1. Vérifier l'état des blocs d'alimentation A et B pour déterminer quelle alimentation fonctionne normalement et suivre les actions recommandées : ◦ Si vous disposez d'un SG100, SG1000 ou SG6000, utilisez le BMC. ◦ Si vous disposez d'une appliance SG5600 ou SG5700, utilisez SANtricity System Manager. 2. Si nécessaire, remplacer l'organe. Consultez les instructions d'installation et de maintenance du matériel de votre appareil : ◦ "Dispositifs de stockage SG6000" ◦ "Appliances de stockage SG5700" ◦ "Appliances de stockage SG5600" ◦ "SG100 etamp ; appareils de services SG1000"
Défaillance Du contrôleur de stockage De l'appliance	Le contrôleur de stockage A d'une appliance StorageGRID est en panne. 1. Utilisez SANtricity System Manager pour vérifier les composants matériels et suivez les actions recommandées. 2. Si nécessaire, remplacer l'organe. Consultez les instructions d'installation et de maintenance du matériel de votre appareil : ◦ "Dispositifs de stockage SG6000" ◦ "Appliances de stockage SG5700" ◦ "Appliances de stockage SG5600"

Nom de l'alerte	Description et actions recommandées
Défaillance du contrôleur B de stockage de l'appliance	Le contrôleur de stockage B d'une appliance StorageGRID est en panne. 1. Utilisez SANtricity System Manager pour vérifier les composants matériels et suivez les actions recommandées. 2. Si nécessaire, remplacer l'organe. Consultez les instructions d'installation et de maintenance du matériel de votre appareil : ◦ "Dispositifs de stockage SG6000" ◦ "Appliances de stockage SG5700" ◦ "Appliances de stockage SG5600"
Panne de disque du contrôleur de stockage de l'appliance	Un ou plusieurs disques d'une appliance StorageGRID sont défectueux ou non optimaux. 1. Utilisez SANtricity System Manager pour vérifier les composants matériels et suivez les actions recommandées. 2. Si nécessaire, remplacer l'organe. Consultez les instructions d'installation et de maintenance du matériel de votre appareil : ◦ "Dispositifs de stockage SG6000" ◦ "Appliances de stockage SG5700" ◦ "Appliances de stockage SG5600"
Problème matériel du contrôleur de stockage de l'appliance	Le logiciel SANtricity signale les besoins d'attention d'un composant d'une appliance StorageGRID. 1. Utilisez SANtricity System Manager pour vérifier les composants matériels et suivez les actions recommandées. 2. Si nécessaire, remplacer l'organe. Consultez les instructions d'installation et de maintenance du matériel de votre appareil : ◦ "Dispositifs de stockage SG6000" ◦ "Appliances de stockage SG5700" ◦ "Appliances de stockage SG5600"

Nom de l'alerte	Description et actions recommandées
Panne de l'alimentation Du contrôleur de stockage de l'appliance	L'alimentation A d'un dispositif StorageGRID s'est déviée de la tension de fonctionnement recommandée. 1. Utilisez SANtricity System Manager pour vérifier les composants matériels et suivez les actions recommandées. 2. Si nécessaire, remplacer l'organe. Consultez les instructions d'installation et de maintenance du matériel de votre appareil : ◦ "Dispositifs de stockage SG6000" ◦ "Appliances de stockage SG5700" ◦ "Appliances de stockage SG5600"
Panne de l'alimentation B du contrôleur de stockage de l'appliance	L'alimentation B d'un dispositif StorageGRID s'est déviée de la tension de fonctionnement recommandée. 1. Utilisez SANtricity System Manager pour vérifier les composants matériels et suivez les actions recommandées. 2. Si nécessaire, remplacer l'organe. Consultez les instructions d'installation et de maintenance du matériel de votre appareil : ◦ "Dispositifs de stockage SG6000" ◦ "Appliances de stockage SG5700" ◦ "Appliances de stockage SG5600"
Entretien du moniteur matériel de stockage de l'appliance bloqué	Le service qui surveille l'état du matériel de stockage a cessé de générer des rapports de données. 1. Vérifiez l'état du service eos-System-status dans le système d'exploitation de base. 2. Si le service est arrêté ou en état d'erreur, redémarrez-le. 3. Si cette alerte persiste, contactez le support technique.

Nom de l’alerte	Description et actions recommandées
Dégradation des tiroirs de stockage de l’appliance	L’état de l’un des composants du tiroir de stockage d’une appliance de stockage est dégradé. 1. Utilisez SANtricity System Manager pour vérifier les composants matériels et suivez les actions recommandées. 2. Si nécessaire, remplacer l’organe. Consultez les instructions d’installation et de maintenance du matériel de votre appareil : ◦ "Dispositifs de stockage SG6000" ◦ "Appliances de stockage SG5700" ◦ "Appliances de stockage SG5600"
Température de l’appareil dépassée	La température nominale ou maximale du contrôleur de stockage de l’appareil a été dépassée. 1. Déterminez s’il y a une autre alerte affectant ce nœud. Cette alerte est peut-être résolue lorsque vous résolvez l’autre alerte. 2. Rechercher les causes possibles de l’augmentation de la température, comme une panne du ventilateur ou du système CVC. 3. Si cette alerte persiste, contactez le support technique.
Capteur de température de l’appareil retiré	Un capteur de température a été déposé. Contactez l’assistance technique.
Erreur du compacteur automatique Cassandra	Le compacteur automatique Cassandra a rencontré une erreur.il existe un compacteur automatique Cassandra sur tous les nœuds de stockage et gère la taille de la base de données Cassandra pour le remplacement et la suppression de charges de travail lourdes. Même si ce problème persiste, certaines charges de travail connaissent une consommation de métadonnées élevée et inattendue. 1. Déterminez s’il y a une autre alerte affectant ce nœud. Cette alerte est peut-être résolue lorsque vous résolvez l’autre alerte. 2. Contactez l’assistance technique.

Nom de l’alerte	Description et actions recommandées
Indicateurs du compacteur automatique Cassandra obsolètes	Les mesures qui décrivent le compacteur automatique Cassandra sont obsolètes. Il existe sur tous les nœuds de stockage un compacteur automatique Cassandra et gère la taille de la base de données Cassandra pour le remplacement et la suppression des charges de travail lourdes. Même si cette alerte est conservée, certaines charges de travail subiront une consommation élevée des métadonnées inattendue. 1. Déterminez s’il y a une autre alerte affectant ce nœud. Cette alerte est peut-être résolue lorsque vous résolvez l’autre alerte. 2. Contactez l’assistance technique.
Erreur de communication Cassandra	Les nœuds qui exécutent le service Cassandra rencontrent des problèmes de communication. Cette alerte indique qu’un objet interfère avec les communications nœud à nœud. Un problème réseau peut se présenter ou le service Cassandra est peut-être arrêté sur un ou plusieurs nœuds de stockage. 1. Déterminez s’il existe une autre alerte affectant un ou plusieurs nœuds de stockage. Cette alerte est peut-être résolue lorsque vous résolvez l’autre alerte. 2. Recherchez un problème réseau affectant un ou plusieurs nœuds de stockage. 3. Sélectionnez **support** > **Outils** > **topologie de grille**. 4. Pour chaque noeud de stockage de votre système, sélectionnez **SSM** > **Services**. Assurez-vous que le statut du service Cassandra est "` en cours d’exécution." 5. Si Cassandra n’est pas en cours d’exécution, suivez les étapes de démarrage ou de redémarrage d’un service dans les instructions de récupération et de maintenance. 6. Si toutes les instances du service Cassandra sont en cours d’exécution et que l’alerte n’est pas résolue, contactez le support technique. "Maintenance et récupération"

Nom de l’alerte	Description et actions recommandées
Compression Cassandra surchargée	Le processus de compaction Cassandra est surchargé.si le processus de compaction est surchargé, les performances de lecture peuvent être dégradées et la mémoire RAM peut être consommée. Le service Cassandra peut également ne plus répondre ou tomber en panne. 1. Redémarrez le service Cassandra en suivant les étapes de redémarrage d’un service dans les instructions de récupération et de maintenance. 2. Si cette alerte persiste, contactez le support technique. "Maintenance et récupération"
Les metrics de réparation de Cassandra sont obsolètes	Les mesures qui décrivent les tâches de réparation de Cassandra sont obsolètes. Si cette condition persiste pendant plus de 48 heures, les requêtes client, telles que les listes de compartiments, peuvent afficher les données supprimées. 1. Redémarrez le nœud. Dans le Gestionnaire de grille, accédez à **noeuds**, sélectionnez le noeud et sélectionnez l’onglet tâches. 2. Si cette alerte persiste, contactez le support technique.
La progression de la réparation de Cassandra est lente	L’avancement des réparations des bases de données Cassandra est lente.lorsque les réparations des bases de données sont lentes, la cohérence des opérations de Cassandra est entravée. Si cette condition persiste pendant plus de 48 heures, les requêtes client, telles que les listes de compartiments, peuvent afficher les données supprimées. 1. Vérifiez que tous les nœuds de stockage sont en ligne et qu’il n’y a pas d’alerte liée à la mise en réseau. 2. Surveillez cette alerte pendant 2 jours maximum pour voir si le problème est résolu par lui-même. 3. Si les réparations de la base de données continuent à se poursuivre lentement, contacter le support technique.

Nom de l’alerte	Description et actions recommandées
Le service de réparation Cassandra n’est pas disponible	Le service de réparation Cassandra n’est pas disponible.le service de réparation Cassandra existe sur tous les nœuds de stockage et offre des fonctions de réparation critiques pour la base de données Cassandra. Si cette condition persiste pendant plus de 48 heures, les requêtes client, telles que les listes de compartiments, peuvent afficher les données supprimées. 1. Sélectionnez **support** > **Outils** > **topologie de grille**. 2. Pour chaque noeud de stockage de votre système, sélectionnez **SSM** > **Services**. Vérifiez que le service Cassandra Reaper est en cours d’exécution. 3. Si Cassandra Reaper n’est pas en cours d’exécution, suivez les étapes pour démarrer ou redémarrer un service dans les instructions de récupération et de maintenance. 4. Si toutes les instances du service Cassandra Reaper sont en cours d’exécution et que l’alerte n’est pas résolue, contactez le support technique. "Maintenance et récupération"
Erreur de connectivité de Cloud Storage Pool	Le contrôle de l’état des pools de stockage cloud a détecté une ou plusieurs nouvelles erreurs. 1. Accédez à la section Cloud Storage pools de la page Storage pools. 2. Consultez la colonne dernière erreur pour déterminer quel pool de stockage cloud a une erreur. 3. Voir les instructions de gestion des objets avec la gestion du cycle de vie des informations. "Gestion des objets avec ILM"

Nom de l’alerte	Description et actions recommandées
Bail DHCP expiré	Le bail DHCP sur une interface réseau a expiré.si le bail DHCP a expiré, suivez les actions recommandées : 1. Assurez-vous que la connectivité est présente entre ce nœud et le serveur DHCP de l’interface affectée. 2. Assurez-vous que des adresses IP sont disponibles pour être affectées dans le sous-réseau affecté sur le serveur DHCP. 3. Assurez-vous qu’il existe une réservation permanente pour l’adresse IP configurée dans le serveur DHCP. Vous pouvez également utiliser l’outil StorageGRID change IP pour attribuer une adresse IP statique en dehors du pool d’adresses DHCP. Reportez-vous aux instructions de récupération et d’entretien. "Maintenance et récupération"
La location DHCP expire bientôt	La location DHCP sur une interface réseau expire bientôt. Pour empêcher l’expiration du bail DHCP, suivez les actions recommandées : 1. Assurez-vous que la connectivité est présente entre ce nœud et le serveur DHCP de l’interface affectée. 2. Assurez-vous que des adresses IP sont disponibles pour être affectées dans le sous-réseau affecté sur le serveur DHCP. 3. Assurez-vous qu’il existe une réservation permanente pour l’adresse IP configurée dans le serveur DHCP. Vous pouvez également utiliser l’outil StorageGRID change IP pour attribuer une adresse IP statique en dehors du pool d’adresses DHCP. Reportez-vous aux instructions de récupération et d’entretien. "Maintenance et récupération"

Nom de l’alerte	Description et actions recommandées
Serveur DHCP indisponible	Le serveur DHCP est indisponible.le nœud StorageGRID ne peut pas contacter votre serveur DHCP. Le bail DHCP de l’adresse IP du nœud ne peut pas être validé. 1. Assurez-vous que la connectivité est présente entre ce nœud et le serveur DHCP de l’interface affectée. 2. Assurez-vous que des adresses IP sont disponibles pour être affectées dans le sous-réseau affecté sur le serveur DHCP. 3. Assurez-vous qu’il existe une réservation permanente pour l’adresse IP configurée dans le serveur DHCP. Vous pouvez également utiliser l’outil StorageGRID change IP pour attribuer une adresse IP statique en dehors du pool d’adresses DHCP. Reportez-vous aux instructions de récupération et d’entretien. "Maintenance et récupération"
Les E/S du disque sont très lentes	Des E/S de disque très lentes peuvent affecter les performances du StorageGRID. 1. Si le problème est lié à un nœud d’appliance de stockage, utilisez SANtricity System Manager pour rechercher des disques défectueux, des disques avec erreurs prévues ou des réparations de disques en cours. Vérifiez également l’état des liaisons Fibre Channel ou SAS entre le calcul de l’appliance et les contrôleurs de stockage pour voir si des liaisons sont en panne ou si les taux d’erreur sont excessifs. 2. Vérifiez le système de stockage qui héberge les volumes de ce nœud pour déterminer, et corriger, la cause première des opérations d’E/S lentes 3. Si cette alerte persiste, contactez le support technique. Les nœuds affectés peuvent désactiver les services et redémarrer afin d’éviter d’affecter les performances globales de la grille. Lorsque la condition à l’origine est éliminée et que ces nœuds détectent les performances d’E/S standard, ils retournent automatiquement leur service complet.

Nom de l'alerte	Description et actions recommandées
Échec de la notification par e-mail	Impossible d'envoyer la notification par e-mail pour une alerte.cette alerte est déclenchée lorsqu'une notification par e-mail d'alerte échoue ou qu'un e-mail test (envoyé à partir de la page **alertes** > **Configuration e-mail**) ne peut pas être envoyé. 1. Connectez-vous à Grid Manager à partir du nœud d'administration répertorié dans la colonne **site/nœud** de l'alerte. 2. Accédez à la page **alertes** > **Configuration de la messagerie**, vérifiez les paramètres et modifiez-les si nécessaire. 3. Cliquez sur **Envoyer E-mail de test** et vérifiez la boîte de réception d'un destinataire de test pour l'e-mail. Une nouvelle instance de cette alerte peut être déclenchée si l'e-mail de test ne peut pas être envoyé. 4. Si l'e-mail de test n'a pas pu être envoyé, vérifiez que votre serveur de messagerie est en ligne. 5. Si le serveur fonctionne, sélectionnez **support** > **Outils** > **Logs**, puis collectez le journal du noeud Admin. Spécifiez une période qui est 15 minutes avant et après l'heure de l'alerte. 6. Extrayez l'archive téléchargée et examinez le contenu de `prometheus.log` (`_/GID<gid><time_stamp>/<site_node>/<time_stamp>/metrics/prometheus.log`). 7. Si vous ne parvenez pas à résoudre le problème, contactez le support technique.
Expiration des certificats configurés sur la page certificats client	Un ou plusieurs certificats configurés sur la page certificats client vont bientôt expirer. 1. Sélectionnez **Configuration** > **contrôle d'accès** > **certificats client**. 2. Sélectionnez un certificat qui expirera bientôt. 3. Sélectionnez **Modifier** pour télécharger ou générer un nouveau certificat. 4. Répétez ces étapes pour chaque certificat qui expirera bientôt. "Administrer StorageGRID"

Nom de l'alerte	Description et actions recommandées
Expiration du certificat de point final de l'équilibreur de charge	Un ou plusieurs certificats de noeud final de l'équilibreur de charge vont expirer. 1. Sélectionnez **Configuration** > **Paramètres réseau** > **points d'extrémité Load Balancer**. 2. Sélectionnez un noeud final dont le certificat expirera bientôt. 3. Sélectionnez **Edit Endpoint** pour télécharger ou générer un nouveau certificat. 4. Répétez ces étapes pour chaque noeud final dont le certificat a expiré ou celui qui expirera bientôt. Pour plus d'informations sur la gestion des terminaux de l'équilibreur de charge, reportez-vous aux instructions d'administration de StorageGRID. "Administrer StorageGRID"
Expiration du certificat de serveur pour l'interface de gestion	Le certificat de serveur utilisé pour l'interface de gestion est sur le point d'expirer. 1. Sélectionnez **Configuration** > **Paramètres réseau** > **certificats serveur**. 2. Dans la section certificat du serveur de l'interface de gestion, téléchargez un nouveau certificat. "Administrer StorageGRID"
Expiration du certificat du serveur pour les terminaux API de stockage	Le certificat de serveur utilisé pour accéder aux noeuds finaux de l'API de stockage est sur le point d'expirer. 1. Sélectionnez **Configuration** > **Paramètres réseau** > **certificats serveur**. 2. Dans la section certificat de serveur de noeuds finaux du service d'API de stockage d'objet, téléchargez un nouveau certificat. "Administrer StorageGRID"

Nom de l’alerte	Description et actions recommandées
Non-concordance de MTU du réseau de grid	Le paramètre MTU (maximum transmission Unit, MTU) pour l’interface réseau Grid (eth0) diffère considérablement sur les nœuds de la grille.les différences de paramètres MTU peuvent indiquer que certains réseaux eth0 sont configurés pour les trames jumbo, mais pas tous. Une différence de taille de MTU supérieure à 1000 peut entraîner des problèmes de performances du réseau. "Dépannage de l’alerte de non-concordance de MTU du réseau Grid"
Utilisation du segment de mémoire Java élevée	Un pourcentage élevé d’espace de tas Java est utilisé.si le segment de mémoire Java devient plein, les services de métadonnées peuvent devenir indisponibles et les demandes client peuvent échouer. 1. Examinez l’activité ILM sur le tableau de bord. Cette alerte peut être résoudre elle-même lorsque la charge de travail ILM diminue. 2. Déterminez s’il y a une autre alerte affectant ce nœud. Cette alerte est peut-être résolue lorsque vous résolvez l’autre alerte. 3. Si cette alerte persiste, contactez le support technique.
Latence élevée pour les requêtes de métadonnées	Le temps moyen des requêtes de métadonnées Cassandra est trop long.une augmentation de la latence des requêtes peut être provoquée par une modification matérielle, comme le remplacement d’un disque ou un changement de charge de travail, comme une augmentation soudaine des inges. 1. Déterminez s’il y a eu des changements de matériel ou de charge de travail en fonction de l’augmentation de la latence de la requête. 2. Si vous ne parvenez pas à résoudre le problème, contactez le support technique.

Nom de l’alerte	Description et actions recommandées
Échec de synchronisation de la fédération d’identités	Impossible de synchroniser des groupes fédérés et des utilisateurs à partir du référentiel d’identité. 1. Vérifiez que le serveur LDAP configuré est en ligne et disponible. 2. Vérifiez les paramètres de la page Fédération des identités. Confirmer que toutes les valeurs sont actuelles. Consultez la section « Configuration d’un référentiel d’identité fédéré » dans les instructions d’administration de StorageGRID. 3. Cliquez sur **Tester la connexion** pour valider les paramètres du serveur LDAP. 4. Si vous ne pouvez pas résoudre le problème, contactez le support technique. "Administrer StorageGRID"

Nom de l’alerte	Description et actions recommandées
Placement ILM impossible à atteindre	Une instruction de placement dans une règle ILM ne peut pas être obtenue pour certains objets.cette alerte indique qu’un nœud requis par une instruction de placement est indisponible ou qu’une règle ILM est mal configurée. Par exemple, une règle peut indiquer plus de copies répliquées qu’il n’y a de nœuds de stockage. 1. Assurez-vous que tous les nœuds sont en ligne. 2. Si tous les nœuds sont en ligne, vérifiez les instructions de placement dans toutes les règles ILM utilisées par la politique ILM active. Vérifiez qu’il existe des instructions valides pour tous les objets. Voir les instructions de gestion des objets avec la gestion du cycle de vie des informations. 3. Si nécessaire, mettez à jour les paramètres des règles et activez une nouvelle stratégie. Un jour peut être nécessaire pour que l’alerte soit claire. 4. Si le problème persiste, contactez le support technique. Cette alerte peut s’afficher pendant une mise à niveau et peut persister 1 jour après la fin de la mise à niveau. Lorsque cette alerte est déclenchée par une mise à niveau, elle s’efface par elle-même. "Gestion des objets avec ILM"

Nom de l’alerte	Description et actions recommandées
Analyse ILM trop longue	Le temps nécessaire pour analyser, évaluer les objets et appliquer ILM est trop long.si la durée estimée pour mener à bien une analyse ILM complète de tous les objets est trop longue (voir **période d’analyse - estimée** sur le tableau de bord), la politique ILM active peut ne pas être appliquée aux objets récemment ingérés. Il est possible que les modifications de la politique ILM ne soient pas appliquées aux objets existants. 1. Déterminez s’il y a une autre alerte affectant ce nœud. Cette alerte est peut-être résolue lorsque vous résolvez l’autre alerte. 2. Vérifiez que tous les nœuds de stockage sont en ligne. 3. Réduire temporairement le trafic client. Par exemple, dans Grid Manager, sélectionnez **Configuration** > **Paramètres réseau** > **Classification du trafic**, puis créez une stratégie limitant la bande passante ou le nombre de requêtes. 4. Si les E/S du disque ou le CPU sont surchargés, essayez de réduire la charge ou d’augmenter la ressource. 5. Si nécessaire, mettez à jour les règles ILM pour utiliser le placement synchrone (par défaut pour les règles créées après StorageGRID 11.3). 6. Si cette alerte persiste, contactez le support technique. "Administrer StorageGRID"

Nom de l'alerte	Description et actions recommandées
Taux d'analyse ILM faible	La vitesse d'analyse ILM est définie sur moins de 100 objets/seconde.cette alerte indique qu'un utilisateur a modifié la vitesse d'analyse ILM de votre système à moins de 100 objets/seconde (par défaut : 400 objets/seconde). Il se peut que la politique ILM active ne soit pas appliquée aux objets récemment ingérées. Les modifications ultérieures de la politique ILM ne seront pas appliquées aux objets existants. 1. Déterminez si une modification temporaire a été apportée à la fréquence d'analyse ILM dans le cadre d'une enquête de soutien en cours. 2. Contactez l'assistance technique. Ne modifiez jamais le taux d'analyse ILM sans contacter le support technique.
Expiration du certificat CA KMS	Le certificat de l'autorité de certification (CA) utilisé pour signer le certificat du serveur de gestion des clés (KMS) est sur le point d'expirer. 1. À l'aide du logiciel KMS, mettez à jour le certificat CA du serveur de gestion des clés. 2. Dans Grid Manager, sélectionnez **Configuration** > **Paramètres système** > **serveur de gestion des clés**. 3. Sélectionnez le KMS qui a un avertissement d'état de certificat. 4. Sélectionnez **Modifier**. 5. Sélectionnez **Suivant** pour passer à l'étape 2 (Télécharger le certificat du serveur). 6. Sélectionnez **Parcourir** pour télécharger le nouveau certificat. 7. Sélectionnez **Enregistrer**. "Administrer StorageGRID"

Nom de l'alerte	Description et actions recommandées
Expiration du certificat client KMS	Le certificat client d'un serveur de gestion des clés est sur le point d'expirer. 1. Dans Grid Manager, sélectionnez **Configuration** > **Paramètres système** > **serveur de gestion des clés**. 2. Sélectionnez le KMS qui a un avertissement d'état de certificat. 3. Sélectionnez **Modifier**. 4. Sélectionnez **Suivant** pour passer à l'étape 3 (Téléchargement de certificats client). 5. Sélectionnez **Parcourir** pour télécharger le nouveau certificat. 6. Sélectionnez **Parcourir** pour télécharger la nouvelle clé privée. 7. Sélectionnez **Enregistrer**. "Administrer StorageGRID"
Echec du chargement de la configuration DES KMS	La configuration du serveur de gestion des clés existe mais n'a pas pu être chargée. 1. Déterminez s'il y a une autre alerte affectant ce nœud. Cette alerte est peut-être résolue lorsque vous résolvez l'autre alerte. 2. Si cette alerte persiste, contactez le support technique.
Erreur de connectivité KMS	Un nœud d'appliance n'a pas pu se connecter au serveur de gestion des clés de son site. 1. Dans Grid Manager, sélectionnez **Configuration** > **Paramètres système** > **serveur de gestion des clés**. 2. Vérifiez que les entrées de port et de nom d'hôte sont correctes. 3. Vérifiez que le certificat du serveur, le certificat client et la clé privée du certificat client sont corrects et n'ont pas expiré. 4. Assurez-vous que les paramètres de pare-feu permettent au nœud de l'appliance de communiquer avec le KMS spécifié. 5. Corrigez tout problème de réseau ou DNS. 6. Si vous avez besoin d'aide ou si cette alerte persiste, contactez le support technique.

Nom de l'alerte	Description et actions recommandées
Nom de la clé de cryptage KMS introuvable	Le serveur de gestion des clés configuré ne dispose pas d'une clé de chiffrement correspondant au nom fourni. 1. Vérifiez que le KMS attribué au site utilise le nom correct pour la clé de chiffrement et toutes les versions antérieures. 2. Si vous avez besoin d'aide ou si cette alerte persiste, contactez le support technique.
Echec de la rotation de la clé de chiffrement KMS	Tous les volumes de l'appliance ont été décryptés, mais un ou plusieurs volumes n'ont pas pu tourner vers la dernière clé.contactez le support technique.
LES KMS ne sont pas configurés	Aucun serveur de gestion des clés n'existe pour ce site. 1. Dans Grid Manager, sélectionnez **Configuration** > **Paramètres système** > **serveur de gestion des clés**. 2. Ajoutez un KMS pour ce site ou ajoutez un KMS par défaut. "Administrer StorageGRID"
La clé KMS n'a pas réussi à décrypter un volume d'appliance	Impossible de décrypter un ou plusieurs volumes sur une appliance dont le chiffrement de nœud est activé avec la clé KMS actuelle. 1. Déterminez s'il y a une autre alerte affectant ce nœud. Cette alerte est peut-être résolue lorsque vous résolvez l'autre alerte. 2. Assurez-vous que le serveur de gestion des clés (KMS) dispose de la clé de chiffrement configurée et des versions précédentes de clés. 3. Si vous avez besoin d'aide ou si cette alerte persiste, contactez le support technique.
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. 1. À l'aide du logiciel KMS, mettez à jour le certificat du serveur pour le serveur de gestion des clés. 2. Si vous avez besoin d'aide ou si cette alerte persiste, contactez le support technique. "Administrer StorageGRID"

Nom de l’alerte	Description et actions recommandées
Grande file d’attente d’audit	La file d’attente des messages d’audit est pleine. 1. Vérifier la charge sur le système—s’il y a eu un nombre important de transactions, l’alerte doit se résoudre au fil du temps et vous pouvez ignorer l’alerte. 2. Si l’alerte persiste et augmente la gravité, affichez un graphique de la taille de la file d’attente. Si ce chiffre augmente régulièrement au fil des heures ou des jours, la charge d’audit a probablement dépassé la capacité d’audit du système. 3. Réduisez le taux de fonctionnement du client ou diminuez le nombre de messages d’audit consignés en modifiant le niveau d’audit pour les écritures client et les lectures client sur erreur ou sur Désactivé (**Configuration** > **surveillance** > **Audit**). "Examiner les journaux d’audit"
Capacité du disque du journal d’audit faible	L’espace disponible pour les journaux d’audit est faible. 1. Surveillez cette alerte pour voir si le problème résout par lui-même et que l’espace disque devient disponible à nouveau. 2. Contactez le support technique si l’espace disponible continue de diminuer.
Mémoire de nœud faible disponibilité	La quantité de RAM disponible sur un nœud est faible.la quantité de RAM disponible faible peut indiquer une modification de la charge de travail ou une fuite de mémoire avec un ou plusieurs nœuds. 1. Surveillez cette alerte pour voir si le problème résout seul. 2. Si la mémoire disponible tombe en dessous du seuil d’alerte majeur, contactez le support technique.

Nom de l'alerte	Description et actions recommandées
Faible espace libre pour le pool de stockage	L'espace disponible pour stocker les données d'objet dans un pool de stockage est faible. 1. Sélectionnez **ILM** > **pools de stockage**. 2. Sélectionnez le pool de stockage répertorié dans l'alerte, puis sélectionnez **Afficher les détails**. 3. Déterminez les endroits où la capacité de stockage supplémentaire est requise. Vous pouvez ajouter des nœuds de stockage à chaque site du pool de stockage ou ajouter des volumes de stockage (LUN) à un ou plusieurs nœuds de stockage existants. 4. Exécutez une procédure d'extension pour augmenter la capacité de stockage. "Développez votre grille"
Mémoire insuffisante sur les nœuds installés	La quantité de mémoire installée sur un nœud est faible.augmentez la quantité de RAM disponible pour la machine virtuelle ou l'hôte Linux. Vérifiez la valeur de seuil de l'alerte majeure pour déterminer la configuration minimale par défaut requise pour un nœud StorageGRID. Reportez-vous aux instructions d'installation de votre plate-forme : • "Installez Red Hat Enterprise Linux ou CentOS" • "Installez Ubuntu ou Debian" • "Installez VMware"

Nom de l'alerte	Description et actions recommandées
Faibles capacités de stockage de métadonnées	L'espace disponible pour le stockage des métadonnées d'objet est faible.**alerte critique** 1. Arrêtez d'ingérer des objets. 2. Ajoutez immédiatement des nœuds de stockage dans une procédure d'extension. **Alerte majeure** Ajoutez immédiatement des nœuds de stockage dans une procédure d'extension. **Alerte mineure** 1. Surveillez la vitesse d'utilisation de l'espace des métadonnées de l'objet. Sélectionnez **Nodes** > ***Storage Node*** > **Storage** et affichez le graphique stockage utilisé - métadonnées d'objet. 2. Ajout de nœuds de stockage dans une procédure d'extension Dès que possible. Une fois que de nouveaux nœuds de stockage sont ajoutés, le système rééquilibre automatiquement les métadonnées d'objet sur tous les nœuds de stockage. L'alarme est supprimée. "Dépannage de l'alerte de stockage de métadonnées faible" "Développez votre grille"
Capacité disque de metrics faible	L'espace disponible pour la base de données de metrics est faible. 1. Surveillez cette alerte pour voir si le problème résout par lui-même et que l'espace disque devient disponible à nouveau. 2. Contactez le support technique si l'espace disponible continue de diminuer.
Faible stockage des données objet	L'espace disponible pour le stockage des données d'objet est faible.effectuez une procédure d'extension. Vous pouvez ajouter des volumes de stockage (LUN) à des nœuds de stockage existants ou ajouter de nouveaux nœuds de stockage. "Dépannage de l'alerte de stockage de données d'objet faible" "Développez votre grille"

Nom de l’alerte	Description et actions recommandées
Capacité du disque racine faible	L’espace disponible pour le disque racine est faible. 1. Surveillez cette alerte pour voir si le problème résout par lui-même et que l’espace disque devient disponible à nouveau. 2. Contactez le support technique si l’espace disponible continue de diminuer.
Faible capacité des données système	L’espace disponible pour les données système StorageGRID sur le système de fichiers /var/local est faible. 1. Surveillez cette alerte pour voir si le problème résout par lui-même et que l’espace disque devient disponible à nouveau. 2. Contactez le support technique si l’espace disponible continue de diminuer.
Erreur de connectivité réseau du nœud	Des erreurs se sont produites lors du transfert des données entre nodes.Network erreurs de connectivité peuvent être résolues sans intervention manuelle. Contactez le support technique si les erreurs ne sont pas corrigées. "Dépannage de l’alarme d’erreur de réception réseau (NRER)"
Erreur de trame de réception du réseau du nœud	Un pourcentage élevé des trames réseau reçues par un nœud a rencontré des erreurs. Cette alerte peut indiquer un problème matériel, par exemple un câble défectueux ou un émetteur-récepteur défectueux à l’une des extrémités de la connexion Ethernet. 1. Si vous utilisez une appliance, essayez de remplacer chaque émetteur-récepteur SFP+ ou SFP28 et chaque câble, un à la fois, afin de voir si l’alerte disparaît. 2. Si cette alerte persiste, contactez le support technique.

Nom de l’alerte	Description et actions recommandées
Nœud non synchronisé avec le serveur NTP	L’heure du nœud n’est pas synchronisée avec le serveur NTP (Network Time Protocol). 1. Vérifiez que vous avez spécifié au moins quatre serveurs NTP externes, chacun fournissant une référence Strum 3 ou supérieure. 2. Vérifier que tous les serveurs NTP fonctionnent normalement. 3. Vérifiez les connexions aux serveurs NTP. Assurez-vous qu’ils ne sont pas bloqués par un pare-feu.
Nœud non verrouillé avec le serveur NTP	Le nœud n’est pas verrouillé sur un serveur NTP (Network Time Protocol). 1. Vérifiez que vous avez spécifié au moins quatre serveurs NTP externes, chacun fournissant une référence Strum 3 ou supérieure. 2. Vérifier que tous les serveurs NTP fonctionnent normalement. 3. Vérifiez les connexions aux serveurs NTP. Assurez-vous qu’ils ne sont pas bloqués par un pare-feu.
Le réseau de nœuds de l’appliance n’est pas défaillant	Un ou plusieurs périphériques réseau sont en panne ou déconnectés. Cette alerte indique qu’une interface réseau (eth) pour un nœud installé sur une machine virtuelle ou un hôte Linux n’est pas accessible. Contactez l’assistance technique.

Nom de l’alerte	Description et actions recommandées
Objets perdus	Un ou plusieurs objets ont été perdus dans la grille.cette alerte peut indiquer que les données ont été définitivement perdues et ne peuvent pas être récupérées. 1. Examiner immédiatement cette alerte. Vous devrez peut-être prendre des mesures pour éviter d’autres pertes de données. Vous pouvez également restaurer un objet perdu si vous prenez une action d’invite. "Dépannage des données d’objet perdues ou manquantes" 2. Lorsque le problème sous-jacent est résolu, réinitialiser le compteur : a. Sélectionnez **support** > **Outils** > **topologie de grille**. b. Pour le nœud de stockage qui a déclenché l’alerte, sélectionnez ***site*** > ***grid node*** > **LDR** > **Data Store** > **Configuration** > **main**. c. Sélectionnez **Réinitialiser le nombre d’objets perdus** et cliquez sur **appliquer les modifications**.
Services de plateforme non disponibles	Trop peu de nœuds de stockage avec le service RSM sont en cours d’exécution ou disponibles sur un site.Assurez-vous que la majorité des nœuds de stockage disposant du service RSM sur le site affecté sont en cours d’exécution et qu’ils ne sont pas en état d’erreur. Consultez la section « Dépannage des services de plate-forme » dans les instructions d’administration de StorageGRID. "Administrer StorageGRID"

Nom de l’alerte	Description et actions recommandées
Interruption de la liaison de l’appliance de services sur le port réseau d’administration 1	Le port réseau Admin 1 de l’appliance est arrêté ou déconnecté. 1. Vérifiez le câble et la connexion physique au port réseau Admin 1. 2. Résoudre tout problème de connexion. Consultez les instructions d’installation et de maintenance du matériel de votre appareil. 3. Si ce port est déconnecté à cet effet, désactivez cette règle. Dans Grid Manager, sélectionnez **alertes** > **règles d’alerte**, sélectionnez la règle et cliquez sur **Modifier la règle**. Décochez ensuite la case **Enabled**. ◦ "SG100 etamp ; appareils de services SG1000" ◦ "Désactivation d’une règle d’alerte"
Liaison de l’appliance de services sur le réseau d’administration (ou le réseau client)	L’interface de l’appliance vers le réseau Admin (eth1) ou le réseau client (eth2) est désactivée ou déconnectée. 1. Vérifiez les câbles, les SFP et les connexions physiques au réseau StorageGRID. 2. Résoudre tout problème de connexion. Consultez les instructions d’installation et de maintenance du matériel de votre appareil. 3. Si ce port est déconnecté à cet effet, désactivez cette règle. Dans Grid Manager, sélectionnez **alertes** > **règles d’alerte**, sélectionnez la règle et cliquez sur **Modifier la règle**. Décochez ensuite la case **Enabled**. ◦ "SG100 etamp ; appareils de services SG1000" ◦ "Désactivation d’une règle d’alerte"

Nom de l'alerte	Description et actions recommandées
La liaison de l'appliance de services est inactive sur les ports réseau 1, 2, 3 ou 4	Les ports réseau 1, 2, 3 ou 4 de l'appareil sont en panne ou déconnectés. 1. Vérifiez les câbles, les SFP et les connexions physiques au réseau StorageGRID. 2. Résoudre tout problème de connexion. Consultez les instructions d'installation et de maintenance du matériel de votre appareil. 3. Si ce port est déconnecté à cet effet, désactivez cette règle. Dans Grid Manager, sélectionnez **alertes > règles d'alerte**, sélectionnez la règle et cliquez sur **Modifier la règle**. Décochez ensuite la case **Enabled**. ◦ "SG100 etamp ; appareils de services SG1000" ◦ "Désactivation d'une règle d'alerte"
Dégradation de la connectivité du stockage de l'appliance de services	L'un des deux disques SSD d'une appliance de services est défectueux ou n'est plus synchronisé avec l'autre.la fonctionnalité de l'appliance n'est pas affectée, mais vous devez résoudre le problème immédiatement. En cas de défaillance des deux disques, l'appliance ne fonctionnera plus. 1. Dans Grid Manager, sélectionnez **noeuds > *services appliance*, puis sélectionnez l'onglet matériel**. 2. Consultez le message dans le champ **Storage RAID mode**. 3. Si le message affiche la progression d'une opération de resynchronisation, attendez la fin de l'opération, puis confirmez que l'alerte a été résolue. Un message de resynchronisation indique que le disque SSD a été remplacé récemment ou qu'il est en cours de resynchronisation pour une autre raison. 4. Si le message indique qu'un des disques SSD est défectueux, remplacez le disque défectueux dans les plus brefs délais. Pour obtenir des instructions sur le remplacement d'un lecteur d'un appareil de services, reportez-vous au guide d'installation et de maintenance des appareils SG100 et SG1000. "SG100 etamp ; appareils de services SG1000"

Nom de l’alerte	Description et actions recommandées
Liaison du dispositif de stockage inactive sur le port réseau d’administration 1	Le port réseau Admin 1 de l’appliance est arrêté ou déconnecté. 1. Vérifiez le câble et la connexion physique au port réseau Admin 1. 2. Résoudre tout problème de connexion. Consultez les instructions d’installation et de maintenance du matériel de votre appareil. 3. Si ce port est déconnecté à cet effet, désactivez cette règle. Dans Grid Manager, sélectionnez **alertes** > **règles d’alerte**, sélectionnez la règle et cliquez sur **Modifier la règle**. Décochez ensuite la case **Enabled**. ◦ "Dispositifs de stockage SG6000" ◦ "Appliances de stockage SG5700" ◦ "Appliances de stockage SG5600" ◦ "Désactivation d’une règle d’alerte"
Lien du dispositif de stockage indisponible sur le réseau d’administration (ou le réseau client)	L’interface de l’appliance vers le réseau Admin (eth1) ou le réseau client (eth2) est désactivée ou déconnectée. 1. Vérifiez les câbles, les SFP et les connexions physiques au réseau StorageGRID. 2. Résoudre tout problème de connexion. Consultez les instructions d’installation et de maintenance du matériel de votre appareil. 3. Si ce port est déconnecté à cet effet, désactivez cette règle. Dans Grid Manager, sélectionnez **alertes** > **règles d’alerte**, sélectionnez la règle et cliquez sur **Modifier la règle**. Décochez ensuite la case **Enabled**. ◦ "Dispositifs de stockage SG6000" ◦ "Appliances de stockage SG5700" ◦ "Appliances de stockage SG5600" ◦ "Désactivation d’une règle d’alerte"

Nom de l'alerte	Description et actions recommandées
La liaison du dispositif de stockage est inactive sur les ports réseau 1, 2, 3 ou 4	Les ports réseau 1, 2, 3 ou 4 de l'appareil sont en panne ou déconnectés. 1. Vérifiez les câbles, les SFP et les connexions physiques au réseau StorageGRID. 2. Résoudre tout problème de connexion. Consultez les instructions d'installation et de maintenance du matériel de votre appareil. 3. Si ce port est déconnecté à cet effet, désactivez cette règle. Dans Grid Manager, sélectionnez **alertes** > **règles d'alerte**, sélectionnez la règle et cliquez sur **Modifier la règle**. Décochez ensuite la case **Enabled**. ◦ "Dispositifs de stockage SG6000" ◦ "Appliances de stockage SG5700" ◦ "Appliances de stockage SG5600" ◦ "Désactivation d'une règle d'alerte"
Dégradation de la connectivité du stockage de l'appliance de stockage	Un problème se produit au niveau d'une ou plusieurs connexions entre le contrôleur de calcul et le contrôleur de stockage. 1. Accédez à l'appareil pour vérifier les voyants des ports. 2. Si les voyants d'un port sont éteints, vérifiez que le câble est correctement branché. Au besoin, remplacez le câble. 3. Attendez jusqu'à cinq minutes. Si un second câble doit être remplacé, ne le débranchez pas pendant au moins 5 minutes. Dans le cas contraire, le volume root peut devenir en lecture seule, ce qui nécessite un redémarrage matériel. 4. Dans Grid Manager, sélectionnez **noeuds**. Sélectionnez ensuite l'onglet matériel du nœud qui a rencontré le problème. Vérifiez que la condition d'alerte a résolu.

Nom de l’alerte	Description et actions recommandées
Périphérique de stockage inaccessible	Impossible d’accéder à un périphérique de stockage.cette alerte indique qu’un volume ne peut pas être monté ou accédé en raison d’un problème avec un périphérique de stockage sous-jacent. 1. Vérifiez l’état de tous les périphériques de stockage utilisés pour le nœud : ◦ Si le nœud est installé sur une machine virtuelle ou un hôte Linux, suivez les instructions de votre système d’exploitation pour exécuter des diagnostics matériels ou effectuer une vérification du système de fichiers. ▪ "Installez Red Hat Enterprise Linux ou CentOS" ▪ "Installez Ubuntu ou Debian" ▪ "Installez VMware" ◦ Si le nœud est installé sur une appliance SG100, SG1000 ou SG6000, utilisez le contrôleur BMC. ◦ Si le nœud est installé sur une appliance SG5600 ou SG5700, utilisez SANtricity System Manager. 2. Si nécessaire, remplacer l’organe. Consultez les instructions d’installation et de maintenance du matériel de votre appareil. ◦ "Dispositifs de stockage SG6000" ◦ "Appliances de stockage SG5700" ◦ "Appliances de stockage SG5600"

Nom de l’alerte	Description et actions recommandées
Utilisation élevée du quota par les locataires	Un pourcentage élevé d’espace quota est utilisé. Si un locataire dépasse son quota, les nouvelles ingaux sont rejetées. Cette règle d’alerte est désactivée par défaut car elle peut générer un grand nombre de notifications. 1. Dans Grid Manager, sélectionnez **tenants**. 2. Trier la table par **quota Utilization**. 3. Sélectionnez un locataire dont l’utilisation des quotas est proche de 100 %. 4. Effectuez l’une des opérations suivantes ou les deux : ◦ Sélectionnez **Modifier** pour augmenter le quota de stockage du locataire. ◦ Informez le locataire que son taux d’utilisation des quotas est élevé.

Nom de l’alerte	Description et actions recommandées
Impossible de communiquer avec le nœud	Un ou plusieurs services ne répondent pas, ou le nœud ne peut pas être atteint.cette alerte indique qu’un nœud est déconnecté pour une raison inconnue. Par exemple, un service du nœud peut être arrêté, ou le nœud a perdu sa connexion réseau en raison d’une panne de courant ou d’une panne imprévue. Surveillez cette alerte pour voir si le problème résout seul. Si le problème persiste : 1. Déterminez s’il y a une autre alerte affectant ce nœud. Cette alerte est peut-être résolue lorsque vous résolvez l’autre alerte. 2. Vérifiez que tous les services de ce nœud sont en cours d’exécution. Si un service est arrêté, essayez de le démarrer. Reportez-vous aux instructions de récupération et d’entretien. 3. Vérifiez que l’hôte du nœud est sous tension. Si ce n’est pas le cas, démarrez l’hôte. Si plusieurs hôtes sont hors tension, reportez-vous aux instructions de récupération et de maintenance. 4. Déterminez s’il y a un problème de connectivité réseau entre ce nœud et le nœud d’administration. 5. Si vous ne parvenez pas à résoudre l’alerte, contactez le support technique. "Maintenance et récupération"
Redémarrage de nœud inattendu	Un nœud a été redémarré de manière inattendue au cours des 24 dernières heures. 1. Contrôle de cette alerte. L’alerte sera effacée après 24 heures. En revanche, si le nœud redémarre de nouveau de façon inattendue, cette alerte est déclenchée à nouveau. 2. Si vous ne parvenez pas à résoudre l’alerte, il se peut qu’il y ait une panne matérielle. Contactez l’assistance technique.

Nom de l'alerte	Description et actions recommandées
Objet corrompu non identifié détecté	Un fichier a été trouvé dans le stockage objet répliqué qui n'a pas pu être identifié en tant qu'objet répliqué. 1. Déterminez s'il y a des problèmes avec le stockage sous-jacent sur un nœud de stockage. Par exemple, exécutez des diagnostics matériels ou effectuez une vérification du système de fichiers. 2. Après avoir résolu des problèmes de stockage, exécutez une vérification au premier plan pour déterminer si des objets sont manquants et les remplacer si possible. 3. Contrôle de cette alerte. L'alerte s'efface après 24 heures, mais se déclenchera à nouveau si le problème n'a pas été résolu. 4. Si vous ne parvenez pas à résoudre l'alerte, contactez le support technique. "Exécution de la vérification de premier plan"

Informations connexes

"Metrics Prometheus couramment utilisés"

Metrics Prometheus couramment utilisés

Le service Prometheus sur les nœuds d'administration recueille les metrics de série chronologique des services sur tous les nœuds. Prometheus recueille plus d'un millier de metrics, mais un nombre relativement faible est requis pour surveiller les opérations StorageGRID les plus stratégiques.

Le tableau suivant répertorie les metrics Prometheus les plus couramment utilisés et fournit un mappage de chaque mesure avec l'attribut équivalent (utilisé dans le système d'alarme).

Vous pouvez consulter cette liste pour mieux comprendre les conditions des règles d'alerte par défaut ou pour définir les conditions des règles d'alerte personnalisées. Pour obtenir la liste complète des mesures, sélectionnez **aide** > **Documentation API**.

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

Les metrics Prometheus sont conservés pendant 31 jours.

Metrics Prometheus	Description
alertmanager_notifications_failed_total	Nombre total de notifications d'alerte ayant échoué.

Metrics Prometheus	Description
node_filesystem_dispo_octets	Quantité d'espace de système de fichiers disponible pour les utilisateurs non-racines en octets.
Node_Memory_MemAvailable_Bytes	Champ informations mémoire MemAvailable_Bytes.
node_network_carrier	Valeur de porteuse de /sys/class/net/<face>.
node_network_recy_errs_total	Statistiques de périphérique réseau Receive_errs.
node_network_transmit_errs_total	Statistiques de périphérique réseau transmit_errs.
storagegrid_panne_administrative	Le nœud n'est pas connecté à la grille pour une raison attendue. Par exemple, le nœud ou les services du nœud ont été normalement arrêtés, le nœud est en cours de redémarrage ou le logiciel est mis à niveau.
storagegrid_appliance_compute_controller_status	L'état du matériel du contrôleur de calcul d'une appliance.
disques_défaillants_appliance_storagegrid	Pour le contrôleur de stockage d'une appliance, le nombre de disques qui ne sont pas optimaux.
état_matériel_contrôleur_stockage_appliance_storagegrid	État global du matériel du contrôleur de stockage d'une appliance.
conteneurs_contenu_seaux_et_conteneurs_storagegrid	Le nombre total de compartiments S3 et de conteneurs Swift connus par ce nœud de stockage.
objets_contenu_storagegrid	Le nombre total d'objets de données S3 et Swift connus de ce nœud de stockage. Nombre n'est valide que pour les objets de données créés par les applications client qui communiquent avec le système via S3 ou Swift.
objet_contenu_storagegrid_perdu	Le nombre total d'objets détectés par ce service est manquant dans le système StorageGRID. Des mesures doivent être prises pour déterminer la cause de la perte et si la récupération est possible. "Dépannage des données d'objet perdues ou manquantes"
storagegrid_http_sessions_entrant_tenté	Nombre total de sessions HTTP ayant été tentées vers un noeud de stockage.

Metrics Prometheus	Description
storagegrid_http_sessions_entrant_actuellement_établi	Nombre de sessions HTTP actuellement actives (ouvertes) sur le nœud de stockage.
storagegrid_http_sessions_incoming_failed	Nombre total de sessions HTTP qui n'ont pas réussi à se terminer correctement, soit en raison d'une requête HTTP mal formée, soit en cas d'échec du traitement d'une opération.
storagegrid_http_sessions_entrant_réussi	Nombre total de sessions HTTP terminées avec succès.
objets_ilm_en_attente_arrière-plan	Le nombre total d'objets sur ce nœud en attente d'évaluation ILM à partir de l'analyse.
storagegrid_ilm_en_attente_client_évaluation_objets_par_seconde	Vitesse actuelle d'évaluation des objets par rapport à la règle ILM de ce nœud.
objet_client_attente_ilm_en_attente	Le nombre total d'objets de ce nœud attend l'évaluation ILM des opérations client (par exemple, ingestion).
objets_ilm_en_attente_total_storagegrid	Le nombre total d'objets en attente d'évaluation ILM.
ilm_scan_objets_par_seconde	Vitesse à laquelle les objets appartenant à ce nœud sont analysés et mis en file d'attente d'ILM.
storagegrid_ilm_scan_perce_estimé_minutes	Durée estimée d'une analyse ILM complète sur ce nœud. **Remarque :** Une analyse complète ne garantit pas que ILM a été appliquée à tous les objets appartenant à ce nœud.
storagegrid_load_balancer_cert_exexpiration_time	Le temps d'expiration du certificat de noeud final de l'équilibreur de charge en secondes depuis l'époque.
storagegrid_metadata_requêtes_moyenne_latence_millisecondes	Temps moyen requis pour exécuter une requête sur le magasin de métadonnées via ce service.
storagegrid_réseau_reçu_octets	Quantité totale de données reçues depuis l'installation.
octets_réseau_transmis_storagegrid	Quantité totale de données envoyées depuis l'installation.

Metrics Prometheus	Description
storagegrid_ntp_choisi_source_temps_offset_millisecondes	Décalage systématique du temps fourni par une source de temps choisie. Le décalage est introduit lorsque le délai d'accès à une source de temps n'est pas égal au temps requis pour que la source de temps atteigne le client NTP.
storagegrid_ntp_verrouillé	Le nœud n'est pas verrouillé sur un serveur NTP (Network Time Protocol).
storagegrid_s3_data_transferts_octets_ingérés	Quantité totale de données ingérées à partir des clients S3 pour ce nœud de stockage, depuis la dernière réinitialisation de l'attribut.
storagegrid_s3_data_transferts_octets_récupéré	Quantité totale de données récupérées par les clients S3 à partir de ce noeud de stockage depuis la dernière réinitialisation de l'attribut.
storagegrid_s3_operations_failed	Le nombre total d'opérations S3 ayant échoué (codes d'état HTTP 4xx et 5xx), à l'exclusion des opérations causées par l'échec d'autorisation S3.
opérations_storagegrid_s3_couronnées_succès	Nombre total d'opérations S3 réussies (code d'état HTTP 2xx).
opérations_storagegrid_s3_non autorisées	Nombre total d'opérations S3 ayant échoué à la suite d'une échec d'autorisation.
storagegrid_servercertificate_management_interface_cert_expiration_days	Nombre de jours avant l'expiration du certificat de l'interface de gestion.
storagegrid_servercertificate_storage_api_endpoints_cert_expiration_days	Nombre de jours avant l'expiration du certificat de l'API de stockage objet.
storagegrid_service_cpu_secondes	Durée cumulée pendant laquelle le CPU a été utilisé par ce service depuis l'installation.
charge_service_storagegrid	Pourcentage de temps CPU disponible actuellement utilisé par ce service. Indique le niveau d'occupation du service. Le temps CPU disponible dépend du nombre de CPU du serveur.
octets_usage_mémoire_service_storagegrid	La quantité de mémoire (RAM) actuellement utilisée par ce service. Cette valeur est identique à celle affichée par l'utilitaire Linux TOP sous RES.
octets_réseau_service_storagegrid_reçus_netapp	Quantité totale de données reçues par ce service depuis l'installation.

Metrics Prometheus	Description
octets_réseau_service_storagegrid_transmis_netapp	Quantité totale de données envoyées par ce service.
redémarrages_service_storagegrid	Nombre total de fois où le service a été redémarré.
storagegrid_service_runtime_seconds	Durée totale d'exécution du service depuis l'installation.
temps_disponibilité_service_storagegrid_secondes	Durée totale d'exécution du service depuis son dernier redémarrage.
storage_state_current_storagegrid	État actuel des services de stockage. Les valeurs d'attribut sont : • 10 = hors ligne • 15 = entretien • 20 = lecture seule • 30 = en ligne
état_stockage_storage_storagegrid	État actuel des services de stockage. Les valeurs d'attribut sont : • 0 = aucune erreur • 10 = en transition • 20 = espace libre insuffisant • 30 = Volume(s) indisponible • 40 = erreur
octets_métadonnées_utilisation_stockage_storagegrid	Estimation de la taille totale des données d'objet répliquées et codées d'effacement sur le nœud de stockage.
storage_utilisation_métadonnées_autorisés_storagegrid_octets	Espace total sur le volume 0 de chaque nœud de stockage autorisé pour les métadonnées d'objet. Cette valeur est toujours inférieure à l'espace réel réservé aux métadonnées sur un nœud, car une partie de l'espace réservé est requise pour les opérations essentielles de base de données (telles que la compaction et la réparation) et les futures mises à niveau matérielles et logicielles.l'espace autorisé pour les métadonnées de l'objet contrôle la capacité globale des objets.
octets_métadonnées_utilisation_stockage_storagegrid	Volume des métadonnées d'objet sur le volume de stockage 0, en octets.

Metrics Prometheus	Description
storage_utilisation_métadonnées_réservés_octets_storagegrid	Espace total sur le volume 0 de chaque nœud de stockage réellement réservé pour les métadonnées d'objet. Pour un nœud de stockage donné, l'espace réservé réel des métadonnées dépend de la taille du volume 0 pour le nœud et du paramètre espace réservé des métadonnées pour l'ensemble du système.
storage_usage_total_octets_espace_stockage_storagegrid	Quantité totale d'espace de stockage alloué à tous les magasins d'objets.
octets_stockage_utilisation_de_stockage_utilisables_storagegrid	Quantité totale d'espace de stockage objet restant. Calculé en ajoutant ensemble la quantité d'espace disponible pour tous les magasins d'objets du nœud de stockage.
storagegrid_swift_data_transfère_octets_ingérés	Quantité totale de données ingérées à partir des clients Swift vers ce nœud de stockage depuis la dernière réinitialisation de l'attribut.
storagegrid_swift_data_transferts_octets_récupéré	Quantité totale de données récupérées par les clients Swift à partir de ce noeud de stockage depuis la dernière réinitialisation de l'attribut.
storagegrid_swift_operations_failed	Nombre total d'opérations Swift ayant échoué (codes d'état HTTP 4xx et 5xx), à l'exclusion des opérations causées par l'échec de l'autorisation Swift.
storagegrid_swift_operations_successful	Nombre total d'opérations Swift réussies (code d'état HTTP 2xx).
storagegrid_swift_operations_non autorisé	Nombre total d'opérations Swift ayant échoué à la suite d'une erreur d'autorisation (codes d'état HTTP 401, 403, 405).
octets_données_utilisation_storagegrid_tenant	Taille logique de tous les objets pour le locataire.
nombre_d'objets_usage_storagegrid_tenant_storagegrid	Le nombre d'objets pour le locataire.
octets_quota_utilisation_storagegrid_tenant_octets	Quantité maximale d'espace logique disponible pour les objets du locataire. Si aucune mesure de quota n'est fournie, une quantité illimitée d'espace est disponible.

Référence des alarmes (système hérité)

Le tableau suivant répertorie toutes les alarmes par défaut héritées. Si une alarme est déclenchée, vous pouvez rechercher le code d'alarme dans ce tableau pour trouver les actions recommandées.

Bien que le système d'alarme existant continue d'être pris en charge, le système d'alerte offre des avantages significatifs et est plus facile à utiliser.

Code	Nom	Service	Action recommandée
ABRL	Relais d'attribut disponibles	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BSSM, BDDS	Rétablir la connectivité à un service (un service ADC) exécutant un service de relais d'attribut dès que possible. S'il n'y a pas de relais d'attribut connectés, le nœud de la grille ne peut pas signaler les valeurs d'attribut au service NMS. Ainsi, le service NMS ne peut plus surveiller l'état du service ou mettre à jour les attributs du service. Si le problème persiste, contactez le support technique.
ACMS	Services de métadonnées disponibles	BARC, BLDR, BCMN	Une alarme se déclenche lorsqu'un service LDR ou ARC perd la connexion à un service DDS. Dans ce cas, les transactions d'entrée ou de récupération ne peuvent pas être traitées. Si l'indisponibilité des services DDS n'est qu'un bref problème transitoire, les transactions peuvent être retardées. Vérifiez et restaurez les connexions à un service DDS pour effacer cette alarme et rétablir la fonctionnalité complète du service.

Code	Nom	Service	Action recommandée
ACTES	État du service NetApp Cloud Tiering	ARC	Disponible uniquement pour les nœuds d'archivage avec un type de Tiering cloud cible : simple Storage Service (S3). Si l'attribut ACT pour le nœud d'archivage est défini sur lecture seule activée ou lecture-écriture désactivée, vous devez définir l'attribut sur lecture-écriture activée. Si une alarme majeure est déclenchée en raison d'un échec de l'authentification, vérifiez les informations d'identification associées au compartiment de destination et mettez à jour les valeurs, si nécessaire. Si une alarme majeure est déclenchée pour une autre raison, contactez le support technique.
ADCA	État ADC	ADC	Si une alarme est déclenchée, sélectionnez **support** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***site*** > ***grid node*** > **ADC** > **Présentation** > **main** et **ADC** > **alarmes** > **main** pour déterminer la cause de l'alarme. Si le problème persiste, contactez le support technique.

Code	Nom	Service	Action recommandée
ADCE	État ADC	ADC	Si la valeur de l'état ADC est Veille, continuez à surveiller le service et si le problème persiste, contactez l'assistance technique. Si la valeur de l'état ADC est hors ligne, redémarrez le service. Si le problème persiste, contactez le support technique.

Code	Nom	Service	Action recommandée
AITE	État de récupération	BARC	Disponible uniquement pour les nœuds d'archivage avec un type cible de Tivoli Storage Manager (TSM). Si la valeur de Retrieve State est en attente de la cible, vérifiez le serveur middleware TSM et assurez-vous qu'il fonctionne correctement. Si le nœud d'archivage vient d'être ajouté au système StorageGRID, assurez-vous que la connexion du nœud d'archivage au système de stockage d'archives externe cible est correctement configurée. Si la valeur de l'état de récupération d'archives est hors ligne, essayez de mettre à jour l'état en ligne. Sélectionnez **support** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***site*** > ***grid node*** > **ARC** > **Retrieve** > **Configuration** > **main**, sélectionnez **Archive Retrieve State** > **Online**, puis cliquez sur **Apply Changes**. Si le problème persiste, contactez le support technique.

Code	Nom	Service	Action recommandée
AITU	État de récupération	BARC	Si la valeur de l'état de récupération est erreur cible, recherchez des erreurs dans le système de stockage d'archives externes ciblé. Si la valeur de l'état de récupération d'archives est session perdue, vérifiez le système de stockage d'archives externes ciblé pour vous assurer qu'il est en ligne et qu'il fonctionne correctement. Vérifiez la connexion réseau avec la cible. Si la valeur de l'état de récupération d'archives est erreur inconnue, contactez le support technique.
ALIS	Sessions d'attribut entrant	ADC	Si le nombre de sessions d'attribut entrantes sur un relais d'attribut augmente trop important, cela peut indiquer que le système StorageGRID est devenu déséquilibré. Dans des conditions normales, les sessions d'attribut doivent être réparties de manière uniforme entre les services ADC. Un déséquilibre peut entraîner des problèmes de performances. Si le problème persiste, contactez le support technique.

Code	Nom	Service	Action recommandée
ALOS	Sessions d’attribut sortant	ADC	Le service ADC a un nombre élevé de sessions d’attribut et est en train de devenir surchargé. Si cette alarme se déclenche, contactez le support technique.
ALUR	Référentiels d’attributs inaccessibles	ADC	Vérifiez la connectivité réseau avec le service NMS pour vous assurer que le service peut contacter le référentiel d’attributs. Si cette alarme se déclenche et que la connectivité réseau est correcte, contactez le support technique.

Code	Nom	Service	Action recommandée
AMQS	Messages d'audit en file d'attente	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BDDS	Si les messages d'audit ne peuvent pas être immédiatement transférés à un relais d'audit ou à un référentiel, ils sont stockés dans une file d'attente de disque. Si la file d'attente des disques est saturée, des pannes peuvent se produire. Pour vous permettre de répondre dans le temps afin d'éviter une panne, des alarmes AMQS sont déclenchées lorsque le nombre de messages dans la file d'attente du disque atteint les seuils suivants : • Remarque : plus de 100,000 messages • Mineur : au moins 500,000 messages • Majeur : au moins 2,000,000 messages • Critique : au moins 5,000,000 messages Si une alarme AMQS est déclenchée, vérifiez la charge sur le système --s'il y a eu un nombre important de transactions, l'alarme doit se résoudre au fil du temps. Dans ce cas, vous pouvez ignorer l'alarme. Si l'alarme persiste et augmente la gravité, affichez un graphique de la taille de la file d'attente. Si ce chiffre augmente régulièrement au fil des heures ou des jours, la charge d'audit a probablement dépassé la capacité d'audit du système. Réduisez le taux de fonctionnement du client ou diminuez le nombre de messages d'audit consignés en

Code	Nom	Service	Action recommandée
AOTE	État du magasin	BARC	Disponible uniquement pour les nœuds d'archivage avec un type cible de Tivoli Storage Manager (TSM). Si la valeur de l'état du magasin attend la cible, vérifiez le système de stockage d'archives externe et assurez-vous qu'il fonctionne correctement. Si le nœud d'archivage vient d'être ajouté au système StorageGRID, assurez-vous que la connexion du nœud d'archivage au système de stockage d'archives externe cible est correctement configurée. Si la valeur de l'état du magasin est hors ligne, vérifiez la valeur de l'état du magasin. Corrigez tout problème avant de remettre l'état du magasin en ligne.
AOTU	État du magasin	BARC	Si la valeur Etat de stockage est session perdue, vérifiez que le système de stockage d'archives externe est connecté et en ligne. Si la valeur erreur cible est définie, recherchez des erreurs dans le système de stockage d'archives externe. Si la valeur de l'état du stockage est erreur inconnue, contactez le support technique.

Code	Nom	Service	Action recommandée
APMS	Connectivité multivoie du stockage	SSM	Si l'alarme d'état multichemin apparaît en tant que « `Degraded' (sélectionnez **support** > **Outils** > **Grid Topology**, puis sélectionnez ***site*** > ***grid node*** > **SSM** > **Events**), procédez comme suit : 1. Branchez ou remplacez le câble qui n'affiche aucun voyant. 2. Attendez une à cinq minutes. Ne débranchez pas l'autre câble au moins cinq minutes après avoir branché le premier câble. Un débranchement trop précoce peut entraîner la lecture seule du volume racine, ce qui nécessite le redémarrage du matériel. 3. Retournez à la page **SSM** > **Ressources** et vérifiez que l'état "`Degraded'" Multipath a été modifié en ""nominal" dans la section Storage Hardware.

Code	Nom	Service	Action recommandée
ARCE	État DE L'ARC	ARC	Le service ARC dispose d'un état de veille jusqu'à ce que tous les composants ARC (réplication, stockage, récupération, cible) aient démarré. Il passe ensuite en ligne. Si la valeur de l'état ARC ne passe pas du mode Veille au mode en ligne, vérifier l'état des composants ARC. Si la valeur de l'état ARC est hors ligne, redémarrer le service. Si le problème persiste, contactez le support technique.
AROQ	Objets mis en file d'attente	ARC	Cette alarme peut être déclenchée si le périphérique de stockage amovible fonctionne lentement en raison de problèmes avec le système de stockage d'archives externes ciblé ou si plusieurs erreurs de lecture sont détectées. Vérifiez que le système de stockage d'archives externe ne présente pas d'erreurs et assurez-vous qu'il fonctionne correctement. Dans certains cas, cette erreur peut survenir en raison d'un taux élevé de demandes de données. Surveillez le nombre d'objets mis en file d'attente lorsque l'activité du système diminue.

Code	Nom	Service	Action recommandée
ARRF	Échecs de demande	ARC	Si une récupération à partir du système de stockage d'archives externe cible échoue, le nœud d'archivage retente l'extraction car la défaillance peut être due à un problème transitoire. Cependant, si les données de l'objet sont corrompues ou si elles ont été marquées comme étant définitivement indisponibles, la récupération n'échoue pas. En revanche, le nœud d'archivage tente continuellement la récupération et la valeur des échecs de demande continue d'augmenter. Cette alarme peut indiquer que le support de stockage contenant les données demandées est corrompu. Vérifiez le système de stockage d'archives externe pour diagnostiquer le problème. Si vous déterminez que les données d'objet ne sont plus dans l'archive, l'objet devra être supprimé du système StorageGRID. Pour plus d'informations, contactez le support technique. Une fois le problème qui a déclenché cette alarme résolu, réinitialisez le nombre de défaillances. Sélectionnez **support** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***site*** > ***grid node*** > **ARC** > **Retrieve** > **Configuration** > **main**, sélectionnez **Réinitialiser le nombre d'échecs de demande** et cliquez sur **appliquer les modifications**.

Code	Nom	Service	Action recommandée
ARRV	Échecs de vérification	ARC	Pour diagnostiquer et corriger ce problème, contactez le support technique. Une fois le problème qui a déclenché cette alarme résolu, réinitialisez le nombre de défaillances. Sélectionnez **support** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***site*** > ***grid node*** > **ARC** > **Retrieve** > **Configuration** > **main**, sélectionnez **Réinitialiser le nombre d'échecs de vérification** et cliquez sur **appliquer les changements**.
ARVF	Échecs de stockage	ARC	Cette alarme peut survenir en raison d'erreurs avec le système de stockage d'archives externes ciblé. Vérifiez que le système de stockage d'archives externe ne présente pas d'erreurs et assurez-vous qu'il fonctionne correctement. Une fois le problème qui a déclenché cette alarme résolu, réinitialisez le nombre de défaillances. Sélectionnez **support** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***site*** > ***grid node*** > **ARC** > **Retrieve** > **Configuration** > **main**, sélectionnez **Réinitialiser le nombre d'échecs de stockage** et cliquez sur **appliquer les changements**.

Code	Nom	Service	Action recommandée
ASXP	Partages d'audit	AMS	Une alarme est déclenchée si la valeur des partages d'audit est inconnue. Cette alarme peut indiquer un problème d'installation ou de configuration du nœud d'administration. Si le problème persiste, contactez le support technique.
AUMA	Statut AMS	AMS	Si la valeur de l'état AMS est erreur de connectivité DB, redémarrez le nœud de la grille. Si le problème persiste, contactez le support technique.
AUME	État AMS	AMS	Si la valeur de l'état AMS est Veille, continuez à surveiller le système StorageGRID. Si le problème persiste, contactez le support technique. Si la valeur de l'état AMS est hors ligne, redémarrez le service. Si le problème persiste, contactez le support technique.
AUXS	Audit de l'état d'exportation	AMS	Si une alarme se déclenche, corrigez le problème sous-jacent, puis redémarrez le service AMS. Si le problème persiste, contactez le support technique.

Code	Nom	Service	Action recommandée
BADD	Nombre de disques défaillants du contrôleur de stockage	SSM	Cette alarme se déclenche lorsqu'un ou plusieurs disques d'une appliance StorageGRID sont défectueux ou non optimaux. Remplacez les disques si nécessaire.
BASF	Identificateurs d'objet disponibles	CMN	Lorsqu'un système StorageGRID est provisionné, le service CMN reçoit un nombre fixe d'identifiants d'objets. Cette alarme se déclenche lorsque le système StorageGRID commence à épuiser sa fourniture d'identifiants d'objets. Pour attribuer davantage d'identifiants, contactez le support technique.

Code	Nom	Service	Action recommandée
BASSES	Identificateur de l'état d'allocation de bloc	CMN	Par défaut, une alarme est déclenchée lorsque les identificateurs d'objet ne peuvent pas être attribués car le quorum ADC ne peut pas être atteint. L'allocation de bloc d'identificateur sur le service CMN requiert un quorum (50 % + 1) des services ADC pour être connectés et en ligne. Si le quorum n'est pas disponible, le service CMN ne peut pas allouer de nouveaux blocs d'identification tant que le quorum ADC n'est pas rétabli. En cas de perte du quorum ADC, il n'y a généralement aucun impact immédiat sur le système StorageGRID (les clients peuvent toujours récupérer et récupérer le contenu), car la quantité d'identifiants d'un mois environ est mise en cache ailleurs dans le réseau ; Cependant, si la condition persiste, le système StorageGRID perdra la possibilité d'ingérer un nouveau contenu. Si une alarme est déclenchée, recherchez la raison de la perte du quorum ADC (par exemple, il peut s'agir d'une défaillance du réseau ou du nœud de stockage) et prenez des mesures correctives. Si le problème persiste, contactez le support technique.

Code	Nom	Service	Action recommandée
BRDT	Température du châssis du contrôleur de calcul	SSM	Une alarme est déclenchée si la température du contrôleur de calcul d'une appliance StorageGRID dépasse le seuil nominal. Vérifier si les composants matériels et les problèmes environnementaux sont en surchauffe. Si nécessaire, remplacer l'organe.
POINT DE FIN	Décalage	BADC, BLDR, BNMS, BAMS, BCLB, BCMN, BARC	Une alarme se déclenche si l'heure d'entretien (secondes) diffère sensiblement de l'heure du système d'exploitation. Dans des conditions normales, le service doit se resynchroniser. Si le temps d'entretien dépasse trop loin du temps du système d'exploitation, le fonctionnement du système peut être affecté. Vérifiez que la source de temps du système StorageGRID est correcte. Si le problème persiste, contactez le support technique.

Code	Nom	Service	Action recommandée
BTSE	État de l'horloge	BADC, BLDR, BNMS, BAMS, BCLB, BCMN, BARC	Une alarme se déclenche si l'heure du service n'est pas synchronisée avec l'heure suivie par le système d'exploitation. Dans des conditions normales, le service doit se resynchroniser. Si le temps dérive trop loin du temps du système d'exploitation, le fonctionnement du système peut être affecté. Vérifiez que la source de temps du système StorageGRID est correcte. Si le problème persiste, contactez le support technique.
CAHP	Pourcentage d'utilisation du tas Java	DDS	Une alarme se déclenche si Java ne parvient pas à effectuer la collecte des déchets à un rythme qui permet au système de disposer d'un espace suffisant pour fonctionner correctement. Une alarme peut indiquer une charge de travail d'utilisateur dépassant les ressources disponibles sur le système pour le magasin de métadonnées DDS. Vérifiez l'activité ILM dans le tableau de bord ou sélectionnez **support** > **Outils** > **topologie de grille**, puis sélectionnez ***site*** > ***grid node*** > **DDS** > **Ressources** > **Présentation** > **main**. Si le problème persiste, contactez le support technique.
CAIH	Nombre de destinations d'ingestion disponibles	CLB	Cette alarme est obsolète.

Code	Nom	Service	Action recommandée
CAQH	Nombre de destinations disponibles	CLB	Cette alarme disparaît lorsque les problèmes sous-jacents des services LDR disponibles sont corrigés. Assurez-vous que le composant HTTP des services LDR est en ligne et fonctionne normalement. Si le problème persiste, contactez le support technique.

Code	Nom	Service	Action recommandée
CASA	État de la banque de données	DDS	Une alarme est déclenchée si le magasin de métadonnées Cassandra n'est plus disponible. Vérifier l'état de Cassandra : 1. Sur le nœud de stockage, connectez-vous en tant qu'administrateur et `su` Pour s'identifier à l'aide du mot de passe indiqué dans le fichier Passwords.txt. 2. Entrez : `service cassandra status` 3. Si Cassandra n'est pas en cours d'exécution, redémarrez-le : `service cassandra restart` Cette alarme peut également indiquer que le magasin de métadonnées (base de données Cassandra) pour un nœud de stockage nécessite une reconstruction. "Dépannage de l'alarme Services : état - Cassandra (SVST)" Si le problème persiste, contactez le support technique.

Code	Nom	Service	Action recommandée
CASSE	État du magasin de données	DDS	Cette alarme est déclenchée lors de l'installation ou de l'extension pour indiquer qu'un nouveau magasin de données rejoint la grille.
CCES	Sessions entrantes - établies	CLB	Cette alarme est déclenchée si 20,000 sessions HTTP ou plus sont actuellement actives (ouvertes) sur le nœud passerelle. Si un client dispose de trop de connexions, il se peut que vous ayez constaté des échecs de connexion. Vous devez réduire la charge de travail.
CCNE	Matériel de calcul	SSM	Cette alarme est déclenchée si l'état du matériel du contrôleur de calcul d'une appliance StorageGRID nécessite une intervention.

Code	Nom	Service	Action recommandée
CDLP	Espace utilisé pour les métadonnées (en %)	DDS	Cette alarme se déclenche lorsque l'espace effectif des métadonnées (CEMS) atteint 70 % (alarme mineure), 90 % (alarme majeure) et 100 % (alarme critique). Si cette alarme atteint le seuil de 90 %, un avertissement s'affiche sur le tableau de bord dans Grid Manager. Vous devez effectuer une procédure d'extension pour ajouter de nouveaux nœuds de stockage dès que possible. Voir les instructions d'extension d'une grille StorageGRID. Si cette alarme atteint le seuil de 100 %, vous devez arrêter d'ingérer immédiatement des objets et ajouter des nœuds de stockage. Cassandra exige un certain espace pour effectuer les opérations essentielles telles que le compactage et la réparation. Ces opérations seront affectées si les métadonnées de l'objet utilisent plus de 100 % de l'espace autorisé. Des résultats indésirables peuvent survenir. **Remarque** : contactez le support technique si vous ne pouvez pas ajouter de nœuds de stockage. Une fois que de nouveaux nœuds de stockage sont ajoutés, le système rééquilibre automatiquement les métadonnées d'objet sur tous les nœuds de stockage. L'alarme est supprimée.
			"Dépannage de l'alerte de

Code	Nom	Service	Action recommandée
CLBA	Statut CLB	CLB	Si une alarme est déclenchée, sélectionnez **support** > **Outils** > **topologie de grille**, puis sélectionnez ***site*** > ***grid node*** > **CLB** > **Présentation** > **main** et **CLB** > **alarmes** > **main** pour déterminer la cause de l'alarme et résoudre le problème. Si le problème persiste, contactez le support technique.
CLBE	Etat CLB	CLB	Si la valeur de CLB State est Veille, continuez à surveiller la situation et si le problème persiste, contactez le support technique. Si l'état est hors ligne et qu'il n'y a aucun problème matériel connu du serveur (par exemple, le serveur est débranché) ou un temps d'arrêt programmé, redémarrez le service. Si le problème persiste, contactez le support technique.

Code	Nom	Service	Action recommandée
CMNA	État CMN	CMN	Si la valeur de l'état CMN est erreur, sélectionnez **support** > **Outils** > **topologie de grille**, puis sélectionnez ***site*** > ***grid node*** > **CMN** > **Présentation** > **main** et **CMN** > **alarmes** > **main** pour déterminer la cause de l'erreur et résoudre le problème. Une alarme est déclenchée et la valeur de l'état CMN est pas de CMN en ligne lors d'une actualisation matérielle du nœud d'administration principal lorsque les CMN sont commutés (la valeur de l'ancien état CMN est en attente et la nouvelle est en ligne). Si le problème persiste, contactez le support technique.
CPRC	Capacité restante	NMS	Une alarme se déclenche si la capacité restante (nombre de connexions disponibles pouvant être ouvertes à la base de données NMS) est inférieure à la gravité configurée pour l'alarme. Si une alarme est déclenchée, contactez le support technique.
CPSA	Alimentation a du contrôleur de calcul	SSM	Une alarme est déclenchée en cas de problème au niveau de l'alimentation A du contrôleur de calcul d'une appliance StorageGRID. Si nécessaire, remplacer l'organe.

Code	Nom	Service	Action recommandée
CPSB	Alimentation B du contrôleur de calcul	SSM	Une alarme est déclenchée en cas de problème au niveau de l'alimentation B du contrôleur de calcul d'une appliance StorageGRID. Si nécessaire, remplacer l'organe.
CPUT	Température du processeur du contrôleur de calcul	SSM	Une alarme est déclenchée si la température du CPU du contrôleur de calcul d'une appliance StorageGRID dépasse le seuil nominal. Si le nœud de stockage est une appliance StorageGRID, le système StorageGRID indique que le contrôleur nécessite une intervention. Vérifier si les composants matériels et les problèmes d'environnement sont en surchauffe. Si nécessaire, remplacer l'organe.
DNST	État DNS	SSM	Une fois l'installation terminée, une alarme DNST est déclenchée dans le service SSM. Une fois que le DNS est configuré et que les nouvelles informations de serveur atteignent tous les nœuds de la grille, l'alarme est annulée.

Code	Nom	Service	Action recommandée
ECCD	Fragments corrompus détectés	LDR	Une alarme se déclenche lorsque le processus de vérification en arrière-plan détecte un fragment codé d'effacement corrompu. Si un fragment corrompu est détecté, une tentative de reconstruction du fragment est effectuée. Réinitialisez les fragments corrompus détectés et copie les attributs perdus à zéro et surveillez-les pour voir si les comptages sont à nouveau affichés. Si le nombre de pannes persiste, le stockage sous-jacent du nœud de stockage peut être problématique. Une copie des données d'objet avec code d'effacement n'est pas considérée comme manquante tant que le nombre de fragments perdus ou corrompus n'enfreint pas la tolérance aux pannes du code d'effacement. Il est donc possible d'avoir un fragment corrompu et de pouvoir récupérer l'objet. Si le problème persiste, contactez le support technique.
ECST	État de vérification	LDR	Cette alarme indique l'état actuel du processus de vérification en arrière-plan des données d'objet avec code d'effacement sur ce nœud de stockage. Une alarme majeure est déclenchée en cas d'erreur dans le processus de vérification en arrière-plan.

Code	Nom	Service	Action recommandée
FONPN	Ouvrez les descripteurs de fichier	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BSSM, BDDS	Le FOPN peut devenir grand pendant l’activité de pointe. S’il ne diminue pas pendant des périodes de ralentissement d’activité, contacter le support technique.
HSTE	État HTTP	BLDR	Voir les actions recommandées pour HSTU.

Code	Nom	Service	Action recommandée
HSTU	Statut HTTP	BLDR	Les HSTE et HSTU sont liés au protocole HTTP pour tout le trafic LDR, y compris le trafic S3, Swift et autre trafic StorageGRID interne. Une alarme indique que l'une des situations suivantes s'est produite : • Le protocole HTTP a été mis hors ligne manuellement. • L'attribut HTTP de démarrage automatique a été désactivé. • Le service LDR est en cours de fermeture. L'attribut Auto-Start HTTP est activé par défaut. Si ce paramètre est modifié, HTTP peut rester hors ligne après un redémarrage. Si nécessaire, attendez que le service LDR redémarre. Sélectionnez **support** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***Storage Node*** > **LDR** > **Configuration**. Si le protocole HTTP est hors ligne, placez-le en ligne. Vérifiez que l'attribut Auto-Start HTTP est activé. Si le protocole HTTP reste hors ligne, contactez le support technique.

Code	Nom	Service	Action recommandée
HTA	Démarrage automatique HTTP	LDR	Spécifie si les services HTTP doivent démarrer automatiquement au démarrage. Il s'agit d'une option de configuration spécifiée par l'utilisateur.
IRSU	État de la réplication entrante	BLDR, BARC	Une alarme indique que la réplication entrante a été désactivée. Confirmer les paramètres de configuration : sélectionnez **support** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***site*** > ***grid node*** > **LDR** > **Replication** > **Configuration** > **main**.
LATA	Latence moyenne	NMS	Vérifiez les problèmes de connectivité. Vérifiez l'activité du système pour confirmer qu'il y a une augmentation de l'activité du système. Une augmentation de l'activité système entraînera une augmentation de l'activité des données d'attribut. Cette augmentation de l'activité entraînera un retard dans le traitement des données d'attribut. Il peut s'agir d'une activité normale du système et se subside. Rechercher des alarmes multiples. Une augmentation des temps de latence moyens peut être indiquée par un nombre excessif d'alarmes déclenchées. Si le problème persiste, contactez le support technique.

Code	Nom	Service	Action recommandée
LDRE	Etat LDR	LDR	Si la valeur de l'Etat LDR est en attente, continuez à suivre la situation et si le problème persiste, contactez l'assistance technique. Si la valeur de LDR State est hors ligne, redémarrez le service. Si le problème persiste, contactez le support technique.
PERDU	Objets perdus	DDS, LDR	Déclenché lorsque le système StorageGRID ne parvient pas à extraire une copie de l'objet demandé à partir de n'importe quel emplacement du système. Avant le déclenchement d'une alarme PERDUE (objets perdus), le système tente de récupérer et de remplacer un objet manquant ailleurs dans le système. Les objets perdus représentent une perte de données. L'attribut objets perdus est incrémenté chaque fois que le nombre d'emplacements d'un objet passe à zéro sans que le service DDS purge automatiquement le contenu pour satisfaire la stratégie ILM. Rechercher immédiatement les alarmes PERDUES (objets PERDUS). Si le problème persiste, contactez le support technique. "Dépannage des données d'objet perdues ou manquantes"

Code	Nom	Service	Action recommandée
MCEP	Expiration du certificat de l'interface de gestion	CMN	Déclenché lorsque le certificat utilisé pour accéder à l'interface de gestion est sur le point d'expirer. 1. Accédez à **Configuration** > **certificats de serveur**. 2. Dans la section certificat du serveur de l'interface de gestion, téléchargez un nouveau certificat. "Administrer StorageGRID"
MINQ	Notifications par e-mail en file d'attente	NMS	Vérifiez les connexions réseau des serveurs hébergeant le service NMS et le serveur de messagerie externe. Vérifiez également que la configuration du serveur de messagerie est correcte. "Configuration des paramètres du serveur de messagerie pour les alarmes (système hérité)"

Code	Nom	Service	Action recommandée
MINUTES	Statut des notifications par e-mail	BNMS	Une alarme mineure se déclenche si le service NMS ne parvient pas à se connecter au serveur de messagerie. Vérifiez les connexions réseau des serveurs hébergeant le service NMS et le serveur de messagerie externe. Vérifiez également que la configuration du serveur de messagerie est correcte. "Configuration des paramètres du serveur de messagerie pour les alarmes (système hérité)"
MLLE	État du moteur d'interface NMS	BNMS	Une alarme se déclenche si le moteur d'interface NMS du nœud d'administration qui collecte et génère du contenu d'interface est déconnecté du système. Cochez Server Manager pour déterminer si l'application individuelle du serveur est en panne.
NANG	Paramètre de négociation automatique du réseau	SSM	Vérifiez la configuration de la carte réseau. Le paramètre doit correspondre aux préférences de vos routeurs et commutateurs réseau. Un réglage incorrect peut avoir un impact important sur les performances du système.

Code	Nom	Service	Action recommandée
NUP	Paramètre duplex réseau	SSM	Vérifiez la configuration de la carte réseau. Le paramètre doit correspondre aux préférences de vos routeurs et commutateurs réseau. Un réglage incorrect peut avoir un impact important sur les performances du système.
NLNK	Détection de la liaison réseau	SSM	Vérifiez les connexions des câbles réseau sur le port et au niveau du commutateur. Vérifiez les configurations du routeur, du commutateur et de la carte réseau. Redémarrez le serveur. Si le problème persiste, contactez le support technique.
NRER	Erreurs de réception	SSM	Les causes suivantes peuvent être des alarmes NRER : • Correction d'erreur de marche avant (FEC) non compatible • Le port du commutateur et la MTU de la carte réseau ne correspondent pas • Taux d'erreur de liaison élevés • Dépassement de la mémoire tampon de la sonnerie NIC "Dépannage de l'alarme d'erreur de réception réseau (NRER)"

Code	Nom	Service	Action recommandée
NRLY	Relais d'audit disponibles	BADC, BARC, BCLB, BCMN, BLDR, BNMS, BDDS	Si les relais d'audit ne sont pas connectés aux services ADC, les événements d'audit ne peuvent pas être signalés. Elles sont mises en file d'attente et indisponibles aux utilisateurs jusqu'à ce que la connexion soit restaurée. Rétablir la connectivité avec un service ADC dès que possible. Si le problème persiste, contactez le support technique.
NSCA	Etat NMS	NMS	Si la valeur de NMS Status est DB Connectivity Error, redémarrez le service. Si le problème persiste, contactez le support technique.
NSCE	Etat NMS	NMS	Si la valeur de l'état NMS est Veille, continuez à surveiller et si le problème persiste, contactez le support technique. Si la valeur de l'état NMS est hors ligne, redémarrez le service. Si le problème persiste, contactez le support technique.
NSPD	Vitesse	SSM	Cela peut être dû à des problèmes de connectivité réseau ou de compatibilité des pilotes. Si le problème persiste, contactez le support technique.

Code	Nom	Service	Action recommandée
NTBR	Espace libre	NMS	Si une alarme est déclenchée, vérifiez la rapidité d'utilisation de la base de données. Une chute soudaine (par opposition à un changement progressif dans le temps) indique une condition d'erreur. Si le problème persiste, contactez le support technique. Le réglage du seuil d'alarme vous permet de gérer de manière proactive les besoins de stockage supplémentaire. Si l'espace disponible atteint un seuil bas (voir seuil d'alarme), contactez le support technique pour modifier l'allocation de la base de données.

Code	Nom	Service	Action recommandée
NTRE	Erreurs de transmission	SSM	Ces erreurs peuvent être résolues sans être réinitialisées manuellement. S'ils ne sont pas clairs, vérifiez le matériel réseau. Vérifiez que le matériel et le pilote de la carte sont correctement installés et configurés pour fonctionner avec vos routeurs et commutateurs réseau. Une fois le problème sous-jacent résolu, réinitialiser le compteur. Sélectionnez **support** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***site*** > ***grid node*** > **SSM** > **Resources** > **Configuration** > **main**, sélectionnez **Réinitialiser le nombre d'erreurs de transmission** et cliquez sur **appliquer les modifications**.
NTFQ	Décalage de fréquence NTP	SSM	Si le décalage de fréquence dépasse le seuil configuré, il y a probablement un problème matériel avec l'horloge locale. Si le problème persiste, contactez l'assistance technique pour organiser un remplacement.
NTPL	Verrouillage NTP	SSM	Si le démon NTP n'est pas verrouillé sur une source de temps externe, vérifiez la connectivité réseau aux sources de temps externes désignées, leur disponibilité et leur stabilité.

Code	Nom	Service	Action recommandée
NTOF	Décalage horaire NTP	SSM	Si le décalage dépasse le seuil configuré, il y a probablement un problème matériel avec l'oscillateur de l'horloge locale. Si le problème persiste, contactez l'assistance technique pour organiser un remplacement.
NTSJ	Jitter de la source horaire choisie	SSM	Cette valeur indique la fiabilité et la stabilité de la source de temps que NTP sur le serveur local utilise comme référence. Si une alarme est déclenchée, cela peut indiquer que l'oscillateur de la source de temps est défectueux ou qu'il y a un problème avec la liaison WAN à la source de temps.
NTSU	État NTP	SSM	Si la valeur de l'état NTP n'est pas en cours d'exécution, contactez le support technique.
OPST	État général de l'alimentation	SSM	Une alarme se déclenche si l'alimentation d'un appareil StorageGRID diffère de la tension de fonctionnement recommandée. Vérifier l'état du bloc d'alimentation A ou B pour déterminer quelle alimentation fonctionne normalement. Si nécessaire remplacer l'alimentation.

Code	Nom	Service	Action recommandée
OQRT	Objets en quarantaine	LDR	Une fois les objets restaurés automatiquement par le système StorageGRID, les objets mis en quarantaine peuvent être supprimés du répertoire de quarantaine. 1. Sélectionnez **support** > **Outils** > **topologie de grille**. 2. Sélectionnez **site** > **Storage Node** > **LDR** > **Verification** > **Configuration** > **main**. 3. Sélectionnez **Supprimer les objets en quarantaine**. 4. Cliquez sur **appliquer les modifications**. Les objets mis en quarantaine sont supprimés et le nombre est remis à zéro.

Code	Nom	Service	Action recommandée
ORSU	État de la réplication sortante	BLDR, BARC	Une alarme indique que la réplication sortante n'est pas possible : le stockage est dans un état où les objets ne peuvent pas être récupérés. Une alarme se déclenche si la réplication sortante est désactivée manuellement. Sélectionnez **support** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***site*** > ***grid node*** > **LDR** > **Replication** > **Configuration**. Une alarme est déclenchée si le service LDR n'est pas disponible pour la réplication. Sélectionnez **support** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***site*** > ***grid node*** > **LDR** > **Storage**.
SLF	État du tiroir	SSM	Une alarme est déclenchée si l'état de l'un des composants du tiroir de stockage d'une appliance de stockage est dégradé. Les composants des tiroirs de stockage incluent les IOM, les ventilateurs, les alimentations et les tiroirs disques.si cette alarme se déclenche, consultez les instructions de maintenance de votre appliance.

Code	Nom	Service	Action recommandée
PMEM	Utilisation de la mémoire de service (pourcentage)	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BSSM, BDDS	Peut avoir une valeur supérieure à y% RAM, où y représente le pourcentage de mémoire utilisé par le serveur. Les chiffres inférieurs à 80 % sont normaux. Plus de 90 % sont considérés comme un problème. Si l'utilisation de la mémoire est élevée pour un seul service, surveillez la situation et recherchez. Si le problème persiste, contactez le support technique.
PSAS	État de l'alimentation Électrique A	SSM	Une alarme se déclenche si l'alimentation A d'un appareil StorageGRID diffère de la tension de fonctionnement recommandée. Si nécessaire remplacer l'alimentation A.
PSB	État de l'alimentation B	SSM	Une alarme se déclenche si l'alimentation B d'un appareil StorageGRID diffère de la tension de fonctionnement recommandée. Si nécessaire remplacer l'alimentation B.

Code	Nom	Service	Action recommandée
RTTD	État de Tivoli Storage Manager	BARC	Disponible uniquement pour les nœuds d'archivage avec un type cible de Tivoli Storage Manager (TSM). Si la valeur de l'état Tivoli Storage Manager est hors ligne, vérifiez l'état de Tivoli Storage Manager et résolvez les problèmes éventuels. Remettre le composant en ligne. Sélectionnez **support** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***site*** > ***grid node*** > **ARC** > **cible** > **Configuration** > **main**, sélectionnez **Tivoli Storage Manager State** > **Online**, puis cliquez sur **appliquer les modifications**.

Code	Nom	Service	Action recommandée
RTU	Statut de Tivoli Storage Manager	BARC	Disponible uniquement pour les nœuds d'archivage avec un type cible de Tivoli Storage Manager (TSM). Si la valeur de l'état de Tivoli Storage Manager est erreur de configuration et que le nœud d'archivage vient d'être ajouté au système StorageGRID, assurez-vous que le serveur middleware TSM est correctement configuré. Si la valeur de l'état de Tivoli Storage Manager est échec de la connexion ou échec de la connexion, essayez de nouveau, vérifiez la configuration réseau sur le serveur middleware TSM et la connexion réseau entre le serveur middleware TSM et le système StorageGRID. Si la valeur de l'état de Tivoli Storage Manager est échec de l'authentification ou échec de l'authentification, reconnexion, le système StorageGRID peut se connecter au serveur middleware TSM, mais ne peut pas authentifier la connexion. Vérifiez que le serveur middleware TSM est configuré avec l'utilisateur, le mot de passe et les autorisations appropriés, puis redémarrez le service. Si la valeur de Tivoli Storage Manager Status est session Failure (échec de session), une session établie a été perdue de manière inattendue. Vérifiez la connexion réseau entre le serveur middleware TSM et le

Code	Nom	Service	Action recommandée
RRF	Réplications entrantes — échec	BLDR, BARC	Une alarme de répétition entrante — une alarme de défaillance peut se produire pendant des périodes de charge élevée ou de perturbations temporaires du réseau. Une fois l'activité du système réduite, cette alarme doit être déclenchée. Si le nombre de réplications ayant échoué continue à augmenter, recherchez des problèmes réseau et vérifiez que les services LDR et ARC source et destination sont en ligne et disponibles. Pour réinitialiser le nombre, sélectionnez **support** > **Outils** > **topologie de grille**, puis sélectionnez ***site*** > ***grid node*** > **LDR** > **Replication** > **Configuration** > **main**. Sélectionnez **Réinitialiser le nombre d'échecs de réplication entrants**, puis cliquez sur **appliquer les modifications**.
RIRQ	Réplications entrantes — en file d'attente	BLDR, BARC	Des alarmes peuvent se produire en cas de charge élevée ou d'interruption temporaire du réseau. Une fois l'activité du système réduite, cette alarme doit être déclenchée. Si le nombre de réplications en file d'attente continue à augmenter, recherchez des problèmes réseau et vérifiez que les services LDR et ARC source et destination sont en ligne et disponibles.

Code	Nom	Service	Action recommandée
RORQ	Réplications sortantes — en file d'attente	BLDR, BARC	La file d'attente de réplication sortante contient des données d'objet copiées afin de satisfaire les règles ILM et les objets requis par les clients. Une alarme peut se produire suite à une surcharge du système. Attendez que l'alarme s'efface lorsque l'activité du système diminue. Si l'alarme se répète, ajoutez de la capacité en ajoutant des nœuds de stockage.
VICE-PRÉSIDENT SAVP	Espace utilisable total (pourcentage)	LDR	Si l'espace utilisable atteint un seuil minimal, options incluent l'extension du système StorageGRID ou le déplacement des données d'objet vers l'archivage via un nœud d'archivage.

Code	Nom	Service	Action recommandée
SCA	État	CMN	Si la valeur Etat de la tâche de grille active est erreur, recherchez le message de tâche de grille. Sélectionnez **support** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***site*** > ***grid node*** > **CMN** > **Grid Tasks** > **Overview** > **main**. Le message de tâche de grille affiche des informations sur l'erreur (par exemple, « échec de la vérification sur le nœud 12130011 »). Après avoir examiné et corrigé le problème, redémarrez la tâche de grille. Sélectionnez **support** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***site*** > ***grid node*** > **CMN** > **Grid Tasks** > **Configuration** > **main** et sélectionnez **actions** > **Exécuter**. Si la valeur Etat pour une tâche de grille en cours d'abandon est erreur, essayez à nouveau d'abandonner la tâche de grille. Si le problème persiste, contactez le support technique.

Code	Nom	Service	Action recommandée
SCEP	Expiration du certificat des terminaux du service d'API de stockage	CMN	Déclenché lorsque le certificat utilisé pour accéder aux terminaux de l'API de stockage arrive à expiration. 1. Accédez à **Configuration** > **certificats de serveur**. 2. Dans la section certificat de serveur de noeuds finaux du service d'API de stockage d'objet, téléchargez un nouveau certificat. "Administrer StorageGRID"
SCHR	État	CMN	Si la valeur Etat de la tâche de grille historique est abandonnée, recherchez la raison et exécutez à nouveau la tâche si nécessaire. Si le problème persiste, contactez le support technique.
SCSA	Contrôleur de stockage A	SSM	Une alarme est déclenchée en cas de problème au niveau du contrôleur de stockage A dans une appliance StorageGRID. Si nécessaire, remplacer l'organe.

Code	Nom	Service	Action recommandée
SCSB	Contrôleur de stockage B	SSM	Une alarme est déclenchée en cas de problème au niveau du contrôleur de stockage B dans une appliance StorageGRID. Si nécessaire, remplacer l'organe. Certains modèles d'appliance ne disposent pas d'un contrôleur de stockage B.
SHLH	Santé	LDR	Si la valeur de l'option Santé d'un magasin d'objets est erreur, vérifiez et corrigez : • problèmes avec le volume monté • erreurs du système de fichiers

Code	Nom	Service	Action recommandée
SLSA	Moyenne de charge CPU	SSM	Plus la valeur est élevée, plus le système est occupé. Si la moyenne de charge CPU persiste à une valeur élevée, le nombre de transactions dans le système doit être examiné afin de déterminer si cela est dû à une charge importante à ce moment-là. Afficher un tableau de la moyenne de charge de la CPU : sélectionnez **support** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***site*** > ***grid node*** > **SSM** > **Ressources** > **Rapports** > **graphiques**. Si la charge du système n'est pas importante et que le problème persiste, contactez le support technique.
SMST	Etat du moniteur de journal	SSM	Si la valeur de l'état de surveillance du journal n'est pas connectée pendant une période prolongée, contactez le support technique.

Code	Nom	Service	Action recommandée
SMTT	Nombre total d'événements	SSM	Si la valeur du total des événements est supérieure à zéro, vérifiez s'il existe des événements connus (tels que des défaillances réseau) pouvant en être la cause. Sauf si ces erreurs ont été effacées (c'est-à-dire que le nombre a été remis à 0), les alarmes Total Events peuvent être déclenchées. Lorsqu'un problème est résolu, réinitialisez le compteur pour effacer l'alarme. Sélectionnez **Nodes** > ***site*** > ***grid node*** > **Events** > **Reset Event counts**. Pour réinitialiser le nombre d'événements, vous devez disposer de l'autorisation Configuration de la page de topologie de la grille. Si la valeur de Total Events est égale à zéro ou si le nombre augmente et que le problème persiste, contactez le support technique.

Code	Nom	Service	Action recommandée
SNST	État	CMN	Une alarme indique qu'il y a un problème de stockage des lots de tâches de la grille. Si la valeur de l'état est erreur de point de contrôle ou si le quorum n'est pas atteint, confirmez qu'une majorité des services ADC sont connectés au système StorageGRID (50 % plus un) et patientez quelques minutes. Si le problème persiste, contactez le support technique.
SOSS	État du système d'exploitation de stockage	SSM	Une alarme se déclenche si le logiciel SANtricity indique qu'un composant d'une appliance StorageGRID présente un problème « nécessite une attention ». Sélectionnez **noeuds**. Sélectionnez ensuite **appliance Storage Node** > **Hardware**. Faites défiler vers le bas pour afficher l'état de chaque composant. Dans le logiciel SANtricity, vérifiez les autres composants de l'appliance pour isoler le problème.

Code	Nom	Service	Action recommandée
SSMA	État SSM	SSM	Si la valeur État SSM est erreur, sélectionnez **support** > **Outils** > **topologie de grille**, puis sélectionnez ***site*** > ***grid node*** > **SSM** > **Présentation** > **main** et **SSM** > **Présentation** > **Survol** > **alarmes** pour déterminer la cause de l'alarme. Si le problème persiste, contactez le support technique.
SSME	État SSM	SSM	Si la valeur de l'état SSM est Veille, continuez à surveiller et si le problème persiste, contactez le support technique. Si la valeur de l'état SSM est hors ligne, redémarrez le service. Si le problème persiste, contactez le support technique.

Code	Nom	Service	Action recommandée
SST	État du stockage	BLDR	Si la valeur de l'état de stockage est insuffisant espace utilisable, il n'y a plus de stockage disponible sur le nœud de stockage et les ingoses de données sont redirigées vers un autre nœud de stockage disponible. Les demandes de récupération peuvent continuer à être fournies à partir de ce nœud de grille. Un stockage supplémentaire doit être ajouté. Elle n'a aucun impact sur les fonctionnalités de l'utilisateur final, mais l'alarme persiste tant que du stockage supplémentaire n'est pas ajouté. Si la valeur de l'état du stockage est Volume(s) indisponible(s), une partie du stockage est indisponible. Le stockage et la récupération de ces volumes ne sont pas possibles. Vérifiez l'état du volume pour plus d'informations : sélectionnez **support** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***site*** > ***grid node*** > **LDR** > **Storage** > **Présentation** > **main**. L'état de santé du volume est répertorié sous magasins d'objets. Si la valeur de l'état de stockage est erreur, contactez le support technique. "Dépannage de l'alarme Storage Status (SSTS)"

Code	Nom	Service	Action recommandée
VST	État	SSM	Cette alarme s'efface lorsque d'autres alarmes liées à un service non opérationnel sont résolues. Suivez les alarmes de service source pour rétablir le fonctionnement. Sélectionnez **support** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***site*** > ***grid node*** > **SSM** > **Services** > **Présentation** > **main**. Lorsque l'état d'un service est indiqué comme non en cours d'exécution, son état est désactivé d'un point de vue administratif. L'état du service peut être indiqué comme étant en cours d'exécution pour les raisons suivantes : • Le service a été arrêté manuellement (`/etc/init.d/<service\> stop`). • Il y a un problème avec la base de données MySQL et Server Manager arrête le service MI. • Un nœud de grille a été ajouté, mais pas démarré. • Pendant l'installation, un nœud de grille n'est pas encore connecté au nœud d'administration. Si un service n'est pas en cours d'exécution, redémarrez-le (`/etc/init.d/<service\> restart`). Cette alarme peut également indiquer que le magasin de métadonnées (base de données Cassandra) pour un nœud de stockage

Code	Nom	Service	Action recommandée
TMEM	Mémoire installée	SSM	Les nœuds exécutés avec moins de 24 Gio de mémoire installée peuvent entraîner des problèmes de performances et l'instabilité du système. La quantité de mémoire installée sur le système doit être augmentée à au moins 24 Gio.
TPOP	Opérations en attente	ADC	Une file d'attente de messages peut indiquer que le service ADC est surchargé. Trop peu de services ADC peuvent être connectés au système StorageGRID. Dans un déploiement important, le service ADC peut nécessiter l'ajout de ressources de calcul, ou le système peut nécessiter des services ADC supplémentaires.
UMEM	Mémoire disponible	SSM	Si la RAM disponible est faible, déterminez s'il s'agit d'un problème matériel ou logiciel. S'il ne s'agit pas d'un problème matériel ou si la mémoire disponible est inférieure à 50 Mo (seuil d'alarme par défaut), contactez le support technique.
VMFI	Entrées disponibles	SSM	Cela indique que du stockage supplémentaire est nécessaire. Contactez l'assistance technique.

Code	Nom	Service	Action recommandée
VMFR	Espace disponible	SSM	Si la valeur de l'espace disponible est trop faible (voir seuils d'alarme), il faut examiner si des fichiers journaux ne sont pas proportionnels ou si des objets prennent trop d'espace disque (voir seuils d'alarme) qui doivent être réduits ou supprimés. Si le problème persiste, contactez le support technique.
VMST	État	SSM	Une alarme est déclenchée si la valeur État du volume monté est Inconnu. Une valeur Inconnu ou Offline peut indiquer que le volume ne peut pas être monté ou accessible en raison d'un problème avec le périphérique de stockage sous-jacent.
VPRI	Priorité de vérification	BLDR, BARC	Par défaut, la valeur de la priorité de vérification est adaptative. Si la priorité de vérification est définie sur élevée, une alarme est déclenchée car la vérification du stockage peut ralentir le fonctionnement normal du service.

Code	Nom	Service	Action recommandée
VSTU	État de vérification de l'objet	BLDR	Sélectionnez **support** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***site*** > ***grid node*** > **LDR** > **Storage** > **Présentation** > **main**. Vérifiez si le système d'exploitation ne présente aucun signe d'erreur de périphérique de bloc ou de système de fichiers. Si la valeur de l'état de vérification de l'objet est erreur inconnue, elle indique généralement un problème matériel ou système de fichiers de bas niveau (erreur d'E/S) qui empêche la tâche de vérification du stockage d'accéder au contenu stocké. Contactez l'assistance technique.
XAMS	Référentiels d'audit inaccessibles	BADC, BARC, BCLB, BCMN, BLDR, BNMS	Vérifiez la connectivité réseau au serveur hébergeant le nœud d'administration. Si le problème persiste, contactez le support technique.

Alarmes générant des notifications SNMP (système hérité)

Le tableau suivant répertorie les anciennes alarmes qui génèrent des notifications SNMP. Contrairement aux alertes, toutes les alarmes ne génèrent pas de notifications SNMP. Seules les alarmes répertoriées génèrent des notifications SNMP et uniquement à la gravité indiquée ou supérieure.

Bien que le système d'alarme existant continue d'être pris en charge, le système d'alerte offre des avantages significatifs et est plus facile à utiliser.

Code	Nom	Gravité
ACMS	Services de métadonnées disponibles	Primordial

Code	Nom	Gravité
AITE	État de récupération	Mineur
AITU	État de récupération	Majeur
AMQS	Messages d'audit en file d'attente	Avertissement
AOTE	État du magasin	Mineur
AOTU	État du magasin	Majeur
AROQ	Objets mis en file d'attente	Mineur
ARRF	Échecs de demande	Majeur
ARRV	Échecs de vérification	Majeur
ARVF	Échecs de stockage	Majeur
ASXP	Partages d'audit	Mineur
AUMA	Statut AMS	Mineur
AUXS	Audit de l'état d'exportation	Mineur
POINT DE FIN	Décalage	Avertissement
CAHP	Pourcentage d'utilisation du tas Java	Majeur
CAQH	Nombre de destinations disponibles	Avertissement
CASA	État de la banque de données	Majeur
CDLP	Espace utilisé pour les métadonnées (en %)	Majeur
CLBE	Etat CLB	Primordial
DNST	État DNS	Primordial
ECST	État de vérification	Majeur

Code	Nom	Gravité
HSTE	État HTTP	Majeur
HTA	Démarrage automatique HTTP	Avertissement
PERDU	Objets perdus	Majeur
MINQ	Notifications par e-mail en file d'attente	Avertissement
MINUTES	Statut des notifications par e-mail	Mineur
NANG	Paramètre de négociation automatique du réseau	Avertissement
NUP	Paramètre duplex réseau	Mineur
NLNK	Détection de la liaison réseau	Mineur
NRER	Erreurs de réception	Avertissement
NSPD	Vitesse	Avertissement
NTRE	Erreurs de transmission	Avertissement
NTFQ	Décalage de fréquence NTP	Mineur
NTPL	Verrouillage NTP	Mineur
NTOF	Décalage horaire NTP	Mineur
NTSJ	Jitter de la source horaire choisie	Mineur
NTSU	État NTP	Majeur
OPST	État général de l'alimentation	Majeur
ORSU	État de la réplication sortante	Avertissement
PSAS	État de l'alimentation Électrique A	Majeur
PSB	État de l'alimentation B	Majeur
RTTD	État de Tivoli Storage Manager	Avertissement

Code	Nom	Gravité
RTU	Statut de Tivoli Storage Manager	Majeur
VICE-PRÉSIDENT SAVP	Espace utilisable total (pourcentage)	Avertissement
SHLH	Santé	Avertissement
SLSA	Moyenne de charge CPU	Avertissement
SMTT	Nombre total d'événements	Avertissement
SNST	État	
SOSS	État du système d'exploitation de stockage	Avertissement
SST	État du stockage	Avertissement
VST	État	Avertissement
TMEM	Mémoire installée	Mineur
UMEM	Mémoire disponible	Mineur
VMST	État	Mineur
VPRI	Priorité de vérification	Avertissement
VSTU	État de vérification de l'objet	Avertissement

Référence des fichiers journaux

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

- "Journaux du logiciel StorageGRID"
- "Journaux de déploiement et de maintenance"
- "Journaux de logiciels tiers"
- "Sur le bycast.log"

Les tableaux de cette section sont fournis à titre de référence uniquement. Les journaux sont destinés au dépannage avancé par le support technique. Les techniques avancées qui impliquent la reconstruction de l'historique des problèmes à l'aide des journaux d'audit et des fichiers journaux d'application sont hors de portée de ce guide.

Pour accéder à ces journaux, vous pouvez collecter des fichiers journaux et des données système (**support** > **Outils** > **journaux**). Si le nœud d'administration principal n'est pas disponible ou ne peut pas atteindre un nœud spécifique, vous pouvez accéder aux journaux de chaque nœud de la grille comme suit :

1. Saisissez la commande suivante : `ssh admin@grid_node_IP`
2. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
3. Entrez la commande suivante pour passer à la racine : `su -`
4. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

Informations associées

"Collecte des fichiers journaux et des données système"

Journaux du logiciel StorageGRID

Les journaux StorageGRID vous permettent de résoudre les problèmes.

Journaux StorageGRID généraux

Nom du fichier	Remarques	Ci-après
`/var/local/log/bycast.log`	Le fichier `bycast.log` Est le fichier de dépannage StorageGRID principal. Le fichier `bycast-err.log` contient un sous-ensemble de `bycast.log` (Messages avec ERREUR de gravité et CRITIQUE). Des messages CRITIQUES sont également affichés dans le système. Sélectionnez **support** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***site*** > ***Node*** > **SSM** > **Events**.	Tous les nœuds

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

Journaux Server Manager

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

Journaux des services StorageGRID

Nom du fichier	Remarques	Ci-après
`/var/local/log/acct.errlog`		Nœuds de stockage exécutant le service ADC

Nom du fichier	Remarques	Ci-après
`/var/local/log/adc.errlog`	Contient le flux erreur standard (stderr) des services correspondants. Il y a un fichier journal par service. Ces fichiers sont généralement vides, sauf en cas de problème avec le service.	Nœuds de stockage exécutant le service ADC
`/var/local/log/ams.errlog`		Nœuds d'administration
`/var/local/log/arc.errlog`		Nœuds d'archivage
`/var/local/log/cassandra/system.log`	Informations pour le magasin de métadonnées (base de données Cassandra) pouvant être utilisées en cas de problème lors de l'ajout de nouveaux nœuds de stockage ou si la tâche de réparation nodetool cale.	Nœuds de stockage
`/var/local/log/cassandra-reaper.log`	Informations concernant le service Cassandra Reaper, qui répare les données de la base de données Cassandra.	Nœuds de stockage
`/var/local/log/cassandra-reaper.errlog`	Informations d'erreur pour le service Cassandra Reaper.	Nœuds de stockage
`/var/local/log/chunk.errlog`		Nœuds de stockage
`/var/local/log/clb.errlog`	Informations d'erreur pour le service CLB. **Note:** le service CLB est obsolète.	Nœuds de passerelle
`/var/local/log/cmn.errlog`		Nœuds d'administration
`/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/cts.errlog`	Ce fichier journal est créé uniquement si le type cible est **Cloud Tiering - simple Storage Service (S3).**	Nœuds d'archivage

Nom du fichier	Remarques	Ci-après
`/var/local/log/dds.errlog`		Nœuds de stockage
`/var/local/log/dmv.errlog`		Nœuds de stockage
`/var/local/log/dynip*`	Contient des journaux liés au service dynap, qui surveille la grille pour les modifications IP dynamiques et met à jour la configuration locale.	Tous les nœuds
`/var/local/log/grafana.log`	Journal associé au service Grafana, utilisé pour la visualisation des metrics dans Grid Manager.	Nœuds d'administration
`/var/local/log/hagroups.log`	Journal associé aux groupes haute disponibilité.	Nœuds d'administration et nœuds de passerelle
`/var/local/log/hagroups_events.log`	Suivi des changements d'état, tels que la transition de LA SAUVEGARDE vers LE MAÎTRE ou LE DÉFAUT.	Nœuds d'administration et nœuds de passerelle
`/var/local/log/idnt.errlog`		Nœuds de stockage exécutant le service ADC
`/var/local/log/jaeger.log`	Journal associé au service jaeger, qui est utilisé pour la collecte de traces.	Tous les nœuds
`/var/local/log/kstn.errlog`		Nœuds de stockage exécutant le service ADC
`/var/local/log/ldr.errlog`		Nœuds de stockage
`/var/local/log/miscd/*.log`	Contient des journaux pour le service MISCd (démon de contrôle du service d'information), qui fournit une interface pour interroger et gérer les services sur d'autres nœuds et pour gérer les configurations environnementales sur le nœud, comme interroger l'état des services s'exécutant sur d'autres nœuds.	Tous les nœuds

Nom du fichier	Remarques	Ci-après
`/var/local/log/nginx/*.log`	Contient des journaux pour le service nginx, qui agit comme un mécanisme d'authentification et de communication sécurisée pour divers services de réseau (comme Prometheus et Dynap) pour pouvoir communiquer avec les services sur d'autres nœuds via des API HTTPS.	Tous les nœuds
`/var/local/log/nginx-gw/*.log`	Contient des journaux des ports d'administration restreints sur les nœuds d'administration et pour le service Load Balancer, qui fournit l'équilibrage de la charge du trafic S3 et Swift entre les clients et les nœuds de stockage.	Nœuds d'administration et nœuds de passerelle
`/var/local/log/persistence*`	Contient les journaux du service Persistence, qui gère les fichiers sur le disque racine qui doivent persister au cours d'un redémarrage.	Tous les nœuds
`/var/local/log/prometheus.log`	Pour tous les nœuds, il contient le journal de service de l'exportateur de nœuds et le journal des services de metrics de l'outil d'exportation de nœuds. 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 de radeau.	Nœuds de stockage avec service RSM
`/var/local/log/rms.errlog`	Contient les journaux du service RSM (State machine Service) répliqué, qui est utilisé pour les services de plate-forme S3.	Nœuds de stockage avec service RSM
`/var/local/log/ssm.errlog`		Tous les nœuds

Nom du fichier	Remarques	Ci-après
`/var/local/log/update-s3vs-domains.log`	Contient des journaux relatifs aux mises à jour de traitement pour la configuration des noms de domaine hébergés sur des serveurs virtuels S3.consultez les instructions d'implémentation des applications client S3.	Nœuds d'administration et de passerelle
`/var/local/log/update-snmp-firewall.*`	Contiennent des journaux relatifs aux ports de pare-feu gérés pour SNMP.	Tous les nœuds
`/var/local/log/update-sysl.log`	Contient des journaux relatifs aux modifications apportées à la configuration syslog du système.	Tous les nœuds
`/var/local/log/update-traffic-classes.log`	Contient des journaux relatifs aux modifications apportées à la configuration des classificateurs de trafic.	Nœuds d'administration et de passerelle
`/var/local/log/update-utcn.log`	Contient des journaux liés au mode réseau client non fiable sur ce nœud.	Tous les nœuds

Journaux NMS

Nom du fichier	Remarques	Ci-après
`/var/local/log/nms.log`	• Capture des notifications à partir du Grid Manager et du tenant Manager. • Capture les événements liés au fonctionnement du service NMS, par exemple, le traitement des alarmes, les notifications par e-mail et les modifications de configuration. • Contient des mises à jour de bundle XML résultant des modifications de configuration effectuées dans le système. • Contient des messages d'erreur liés au sous-échantillonnage de l'attribut effectué une fois par jour. • Contient les messages d'erreur du serveur Web Java, par exemple les erreurs de génération de page et les erreurs HTTP Status 500.	Nœuds d'administration
`/var/local/log/nms.errlog`	Contient des messages d'erreur relatifs aux mises à niveau de la base de données MySQL. Contient le flux erreur standard (stderr) des services correspondants. Il y a un fichier journal par service. Ces fichiers sont généralement vides, sauf en cas de problème avec le service.	Nœuds 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

Informations associées

"Sur le bycast.log"

"Utilisation de S3"

Journaux de déploiement et de maintenance

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

Nom du fichier	Remarques	Ci-après
`/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 pendant les opérations d'extension. Contient un enregistrement des événements d'extension.	Nœuds de stockage
`/var/local/log/gdu-server.log`	Créé par le service GDU. Contient les événements liés aux procédures d'approvisionnement et de maintenance gérées par le nœud d'administration principal.	Nœud d'administration principal
`/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 logicielle. Contient un enregistrement des événements de mise à jour du logiciel.	Tous les nœuds

Journaux de logiciels tiers

Vous pouvez utiliser les journaux de logiciels tiers pour résoudre les problèmes.

Catégorie	Nom du fichier	Remarques	Ci-après
journaux apache2	`/var/local/log/apache2/access.log` `/var/local/log/apache2/error.log` `/var/local/log/apache2/other_vhosts_access.log`	Fichiers journaux pour apache2.	Nœuds d'administration
Archivage	`/var/local/log/dsierror.log`	Informations d'erreur pour les API client TSM.	Nœuds d'archivage

Catégorie	Nom du fichier	Remarques	Ci-après

MySQL	/var/local/log/mysql.err'
	
	`/var/local/log/mysql.err`
	`/var/local/log/mysql-slow.log`
		Fichiers journaux générés par MySQL.
		
		Le fichier mysql.err capture les erreurs de base de données et les événements tels que les démarrages et les arrêts.
		
		Le fichier mysql-slow.log (le journal de requête lente) capture les instructions SQL qui ont pris plus de 10 secondes à exécuter.
			Nœuds d'administration

Système d'exploitation	`/var/local/log/messages`	Ce répertoire contient les fichiers journaux du système d'exploitation. Les erreurs contenues dans ces journaux s'affichent également dans Grid Manager. Sélectionnez **support** > **Outils** > **topologie de grille**. Sélectionnez ensuite **Topology** > ***site*** > ***Node*** > **SSM** > **Events**.	Tous les nœuds

NTP	`/var/local/log/ntp.log`
	
	`/var/lib/ntp/var/log/ntpstats/`
		Le `/var/local/log/ntp.log` Contient le fichier journal des messages d'erreur NTP.
		
		Le `/var/lib/ntp/var/log/ntpstats/` Le répertoire contient les statistiques de synchronisation NTP.
		
		`loopstats` enregistre les informations statistiques de filtre en boucle.
		
		`peerstats` enregistre les statistiques homologues.
			Tous les nœuds

Catégorie	Nom du fichier	Remarques	Ci-après
Samba	`/var/local/log/samba/`	Le répertoire des journaux Samba comprend un fichier journal pour chaque processus Samba (smb, nmb et winbind) et chaque nom d'hôte/IP du client.	Nœud d'administration configuré pour exporter le partage d'audit via CIFS

Sur le bycast.log

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

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

Rotation des fichiers pour bycast.log

Lorsque 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`. Lorsque le nouveau `bycast.log` Atteint 1 Go, `bycast.log.1` est renommé et compressé pour devenir `bycast.log.2.gz`, et `bycast.log` est renommé `bycast.log.1`.

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

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

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

Informations associées

"Collecte des fichiers journaux et des données système"

Messages en bycast.log

Messages dans `bycast.log` Sont écrits par l'ADE (ADE). ADE est l'environnement d'exécution utilisé par les services de chaque nœud de la grille.

Voici un exemple de message ADE :

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

Les messages ADE contiennent les informations suivantes :

Segment de message	Valeur dans l'exemple
ID de nœud	12455685
ID processus ADE	0357819531
Nom du module	SVMR
Identifiant du message	EVHR
Heure système UTC	2019-05-05T27T17:10:29.784677 (AAAA-MM-DDTHH:MM:SS.UUUUUUUU)
Niveau de gravité	ERREUR
Numéro de suivi interne	0906
Messagerie	SVMR : le bilan de santé du volume 3 a échoué avec la raison « tout »

Gravité des messages en bycast.log

Les messages dans `bycast.log` des niveaux de sévérité sont attribués.

Par exemple :

- **AVIS** — un événement qui devrait être enregistré s'est produit. La plupart des messages du journal sont à ce niveau.
- **AVERTISSEMENT** — une condition inattendue s'est produite.
- **ERREUR** — Une erreur majeure s'est produite qui aura une incidence sur les opérations.
- **CRITIQUE** — une condition anormale s'est produite qui a arrêté les opérations normales. Vous devez immédiatement corriger la condition sous-jacente. Les messages critiques sont également affichés dans le Grid Manager. Sélectionnez **support** > **Outils** > **topologie de grille**. Sélectionnez ensuite **site** > **nœud** > **SSM** > **événements**.

Codes d'erreur dans bycast.log

La plupart des messages d'erreur dans `bycast.log` contient 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 signalé.

Code d’erreur	Signification
CAN	Pas d’erreur
GERR	Inconnu
ANNUL	Annulée
ABRT	Abandonné
TOUT	Délai dépassé
INVL	Non valide
NFND	Introuvable
VERS	Version
CONF	Configuration
ECHEC	Échec
CIPD	Incomplet
L’A FAIT	L’a fait
SUNV	Service indisponible

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

Numéro de l’erreur	Code d’erreur	Signification
001	EPERM	Opération non autorisée
002	RÉF	Ce fichier ou répertoire n’est pas disponible
003	ESRCH	Pas de tel processus
004	EINTA	Appel système interrompu
005	EIO	Erreur d’E/S.
006	ENXIO	Ce périphérique ou cette adresse n’est pas disponible

Numéro de l’erreur	Code d’erreur	Signification
007	E2BIG	Liste d’arguments trop longue
008	ENOEXEC	Erreur de format Exec
009	EBADF	Numéro de fichier incorrect
010	ECHILD	Aucun processus enfant
011	EAGAIN	Réessayez
012	ENOMEM	Mémoire insuffisante
013	EACCES	Autorisation refusée
014	PAR DÉFAUT	Adresse incorrecte
015	ENOTBLK	Dispositif de blocage requis
016	EBUSY	Périphérique ou ressource occupé
017	EEXIST	Le fichier existe déjà
018	EXDEV	Liaison interpériphérique
019	ENV	Aucun appareil de ce type
020	ENOTDIR	Pas un répertoire
021	EISDIR	Est un répertoire
022	EINVAL	Argument non valide
023	PAGE D’ACCUEIL	Dépassement de la table de fichiers
024	EMFILE	Trop de fichiers ouverts
025	EN COURS	Pas une machine à écrire
026	ETXTBBY	Fichier texte occupé
027	EFBIG	Fichier trop volumineux

Numéro de l’erreur	Code d’erreur	Signification
028	ENOSPC	Il n’y a plus d’espace sur l’appareil
029	ESPIPE	Recherche illégale
030	EROFS	Système de fichiers en lecture seule
031	ALINK	Trop de liens
032	EPIPE	Tuyau cassé
033	ÉDOM	Argument mathématique hors domaine de la fonction
034	ERANGE	Résultat mathématique non représentativité
035	EDEADLE	L’impasse de la ressource se produirait
036	ENAMETOOLONG	Nom de fichier trop long
037	ENOLCK	Aucun verrouillage d’enregistrement disponible
038	ENOSYS	Fonction non implémentée
039	ENOTEMPTY	Répertoire non vide
040	ELOP	Trop de liens symboliques rencontrés
041		
042	ENOMSG	Aucun message du type souhaité
043	EIDRM	Identificateur supprimé
044	ECHNG	Numéro de canal hors plage
045	EL2NSYNC	Niveau 2 non synchronisé
046	EL3HLT	Niveau 3 arrêté

Numéro de l’erreur	Code d’erreur	Signification
047	EL3RST	Remise à zéro du niveau 3
048	ELNRNG	Numéro de liaison hors plage
049	EUNATCH	Pilote de protocole non connecté
050	ENOCSI	Aucune structure CSI disponible
051	EL2HLT	Niveau 2 arrêté
052	EBADE	Échange non valide
053	ADR	Descripteur de demande non valide
054	EXFULL	Exchange complet
055	ENOANO	Pas d’anode
056	EBADRQC	Code de demande non valide
057	EBADSLT	Emplacement non valide
058		
059	EBFONT	Format de fichier de police incorrect
060	ENOSTR	Le périphérique n’est pas un flux
061	ENODATA	Aucune donnée disponible
062	ETIME	Temporisation expirée
063	ENOSR	Ressources hors flux
064	ENONET	La machine n’est pas sur le réseau
065	ENOPKG	Package non installé
066	EREMOTE	L’objet est distant
067	LIAISON	Le lien a été rompu

Numéro de l’erreur	Code d’erreur	Signification
068	EADV	Erreur de publicité
069	ESRMNT	Erreur Srmount
070	ECOMM	Erreur de communication sur l’envoi
071	EPROTO	Erreur de protocole
072	EMULTIIHOP	Multihop tenté
073	EDOTTDOT	Erreur spécifique RFS
074	EBADMSG	Pas un message de données
075	EOVERFLOW	Valeur trop élevée pour le type de données défini
076	ENOTUNIQ	Nom non unique sur le réseau
077	EDFD	Descripteur de fichier dans un état incorrect
078	SOUS-GROUPE	Adresse distante modifiée
079	ELIBACC	Impossible d’accéder à une bibliothèque partagée requise
080	ELIBBAD	Accès à une bibliothèque partagée endommagée
081	ELIBSCN	
082	ELIBMAX	Tentative de liaison dans trop de bibliothèques partagées
083	ELIBEXEC	Impossible d’effectuer directement l’exec d’une bibliothèque partagée
084	EILSEQ	Séquence d’octets non autorisée
085	SYSTÈME	L’appel système interrompu doit être redémarré

Numéro de l’erreur	Code d’erreur	Signification
086	ESTRPIPE	Erreur de tuyau de flux
087	EUSERS	Trop d’utilisateurs
088	ENOTSOCK	Fonctionnement de la prise femelle sur non prise femelle
089	EDESTADDRREQ	Adresse de destination requise
090	EMSGSIZE	Message trop long
091	EPROTOTYPE	Type de protocole incorrect pour le socket
092	EN OPTION	Protocole non disponible
093	EPROTONOSUPPORT	Protocole non pris en charge
094	ESOCKNOSUPPORT	Type de socket non pris en charge
095	EOPNOTSUPP	Opération non prise en charge sur le terminal de transport
096	EPFNOSUPPORT	Famille de protocoles non prise en charge
097	EAFNOSUPPORT	Famille d’adresses non prise en charge par le protocole
098	EADDDRINUSE	Adresse déjà utilisée
099	EADDRNOTAVAIL	Impossible d’attribuer l’adresse demandée
100	EN-TÊTE	Le réseau ne fonctionne pas
101	ENETUNREACH	Le réseau est inaccessible
102	ENETRESET	La connexion au réseau a été interrompue en raison d’une réinitialisation
103	ECONNABORTED	Le logiciel a provoqué l’abandon de la connexion

Numéro de l’erreur	Code d’erreur	Signification
104	ECONRESET	Réinitialisation de la connexion par poste
105	ENOBUFS	Aucun espace tampon disponible
106	EISCONN	Terminal de transport déjà connecté
107	ENOTCONN	Le terminal de transport n’est pas connecté
108	ESHUTDOWN	Impossible d’envoyer après l’arrêt du terminal de transport
109	ETOONYREFS	Trop de références : impossible d’épissure
110	ETIMDOUT	La connexion a expiré
111	ECONREFUSED	Connexion refusée
112	EHOSTDOWN	L’hôte n’est pas en panne
113	EHOSTUNREACH	Aucune route vers l’hôte
114	EALREADY	Opération déjà en cours
115	EINPROGRESS	Opération en cours
116		
117	EUCLEAN	La structure doit être nettoyée
118	ENOTNAM	Pas un fichier de type nommé XENIX
119	ENAVAIL	Aucun sémaphores XENIX n’est disponible
120	EISNAM	Est un fichier de type nommé
121	EREMOTIO	Erreur d’E/S distante
122	EDUQUOT	Quota dépassé

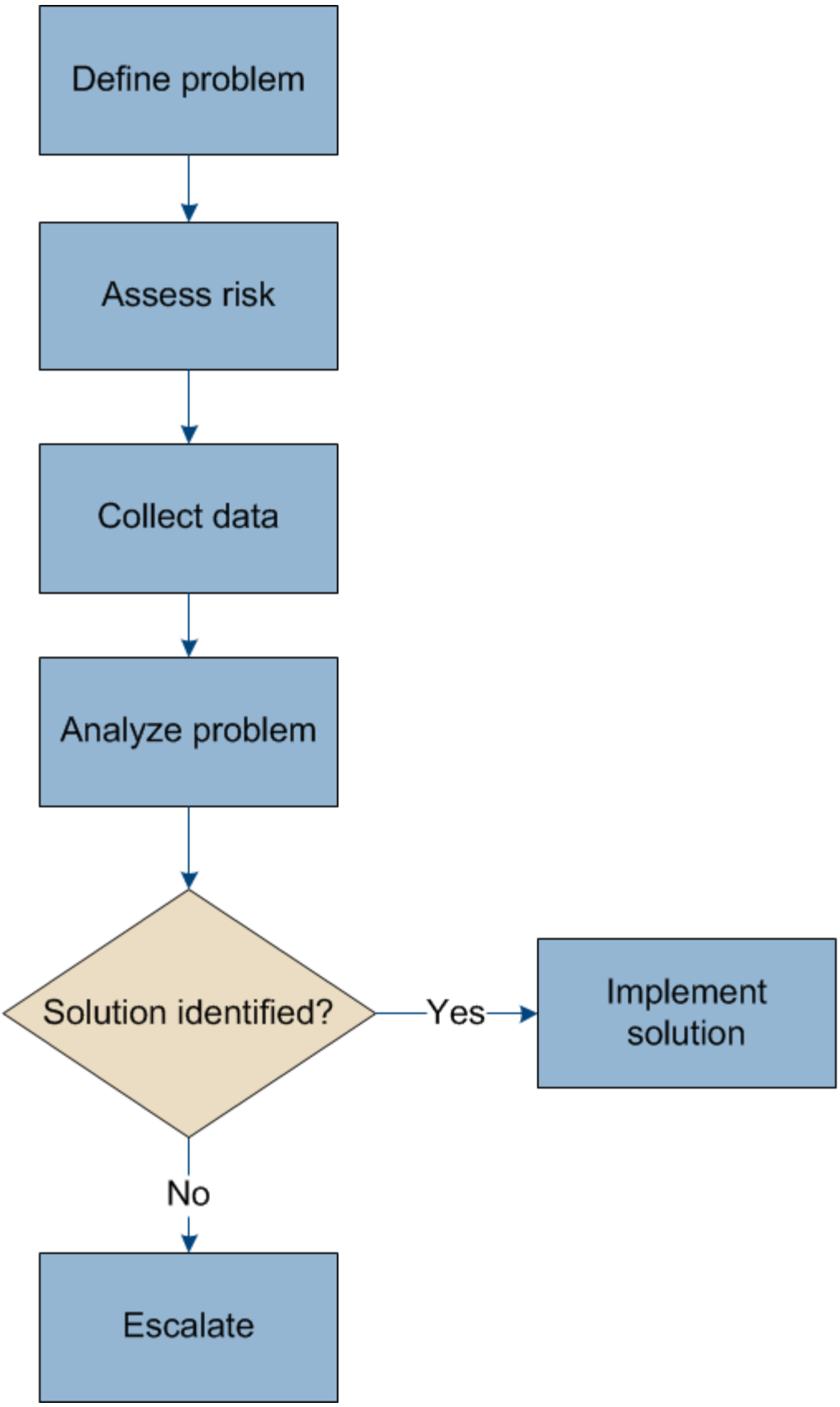
Numéro de l’erreur	Code d’erreur	Signification
123	ENOMEDIUM	Aucun support trouvé
124	EMEDIUMTYPE	Type de support incorrect
125	ECANCELED	Opération annulée
126	ENOKAY	Clé requise non disponible
127	EKEYEXPIRED	La clé a expiré
128	EKEYREVOKED	La clé a été révoquée
129	EKEYREJECTED	La clé a été rejetée par le service
130	EOWNERDEAD	Pour des mutexes robustes : le propriétaire est mort
131	ENOTREOVERABLE	Pour les mutexes robustes : état non récupérable

Dépanner un système StorageGRID

Si vous rencontrez un problème avec un système StorageGRID, consultez les conseils et les instructions de cette section pour déterminer et résoudre le problème.

Présentation de la détection des problèmes

Si vous rencontrez un problème lors de l’administration d’un système StorageGRID, vous pouvez utiliser le processus décrit dans cette figure pour identifier et analyser le problème. Dans de nombreux cas, vous pouvez résoudre vous-même les problèmes que vous rencontrez, mais vous devrez peut-être réaffecter quelques problèmes au support technique.



Définition du problème

La première étape pour résoudre un problème est de définir clairement le problème.

Ce tableau fournit des exemples de types d'informations que vous pouvez collecter pour définir un problème :

Question	Exemple de réponse
Que fait ou ne fait pas le système StorageGRID ? Quels sont ses symptômes ?	Les applications client signale que les objets ne peuvent pas être ingérées sur StorageGRID.
Quand le problème a-t-il démarré ?	L'ingestion d'objet a d'abord été refusée à environ 14:50 le 8 janvier 2020.
Comment avez-vous remarqué le problème pour la première fois ?	Notifié par la demande du client. Vous avez également reçu des notifications par e-mail d'alerte.
Le problème se produit-il de manière cohérente ou seulement parfois ?	Le problème est en cours.
Si le problème se produit régulièrement, quelles sont les étapes à suivre	Un problème se produit à chaque fois qu'un client tente d'ingérer un objet.
Si le problème se produit par intermittence, quand cela se produit-il? Notez l'heure de chaque incident que vous connaissez.	Le problème n'est pas intermittent.
Avez-vous déjà vu ce problème ? À quelle fréquence avez-vous eu ce problème par le passé ?	C'est la première fois que j'ai vu cette question.

Évaluation du risque et de l'impact sur le système

Une fois le problème défini, évaluez les risques et l'impact sur le système StorageGRID. Par exemple, la présence d'alertes critiques ne signifie pas nécessairement que le système ne fournit pas de services de base.

Ce tableau récapitule l'impact du problème exemple sur les opérations du système :

Question	Exemple de réponse
Le système StorageGRID est-il en mesure d'ingérer du contenu ?	Non
Les applications client peuvent-elles récupérer du contenu ?	Certains objets peuvent être récupérés et d'autres ne peuvent pas être récupérés.
Les données sont-elles menacées ?	Non
La capacité à mener des activités est-elle gravement affectée ?	Oui, car les applications client ne peuvent pas stocker d'objets sur le système StorageGRID et les données ne peuvent pas être récupérées de manière cohérente.

Collecte des données

Une fois que vous avez défini le problème et évalué ses risques et son impact, collectez des données pour analyse. Le type de données les plus utiles à recueillir dépend de la nature du problème.

Type de données à collecter	Pourquoi collecter ces données	Instructions
Créer le calendrier des modifications récentes	Toute modification de votre système StorageGRID, de sa configuration ou de son environnement peut provoquer un nouveau comportement.	• Création d'un calendrier des modifications récentes
Examinez les alertes et les alarmes	Les alertes et les alarmes peuvent vous aider à déterminer rapidement la cause première d'un problème en fournissant des indications importantes sur les problèmes sous-jacents qui pourraient l'être. Consultez la liste des alertes et alarmes en cours pour voir si StorageGRID a identifié la cause principale d'un problème pour vous. Pour en savoir plus, consultez les alertes et les alarmes déclenchées par le passé.	• "Affichage des alertes en cours" • "Affichage des anciennes alarmes" • "Affichage des alertes résolues" • "Vérification des alarmes historiques et de la fréquence des alarmes (système hérité)"
Contrôle des événements	Les événements incluent les événements d'erreur système ou de panne pour un nœud, y compris les erreurs telles que les erreurs réseau. Surveiller les événements pour en savoir plus sur les problèmes ou obtenir de l'aide pour les résoudre.	• "Affichage de l'onglet événements" • "Contrôle des événements"
Identifier les tendances à l'aide de rapports graphiques et textuels	Les tendances peuvent donner des indications précieuses sur le moment où les problèmes sont apparus et vous aider à comprendre la rapidité à laquelle les choses évoluent.	• "Utilisation de graphiques et de rapports"
Établir les lignes de base	Collectez des informations sur les niveaux normaux de différentes valeurs opérationnelles. Ces valeurs de référence, ainsi que les écarts par rapport à ces lignes de base, peuvent fournir des indices précieux.	• Établir des lignes de base
Tests d'entrée et de récupération	Pour résoudre les problèmes de performance liés à l'entrée et à la récupération, utilisez un poste de travail pour stocker et récupérer des objets. Comparez les résultats obtenus avec ceux observés lors de l'utilisation de l'application client.	• "Surveillance et PERFORMANCES ACCRUES"

Type de données à collecter	Pourquoi collecter ces données	Instructions
Examiner les messages d'audit	Examinez les messages d'audit afin de suivre les opérations StorageGRID en détail. Les détails dans les messages d'audit peuvent être utiles pour le dépannage de nombreux types de problèmes, y compris les problèmes de performance.	• "Vérification des messages d'audit"
Vérifier l'emplacement des objets et l'intégrité du stockage	En cas de problèmes de stockage, vérifiez que les objets sont placés à l'endroit où vous vous attendez. Vérifiez l'intégrité des données d'objet sur un nœud de stockage.	"Surveillance des opérations de vérification d'objets".
Collecte de données pour le support technique	L'assistance technique peut vous demander de collecter des données ou de passer en revue des informations spécifiques pour résoudre les problèmes.	• "Collecte des fichiers journaux et des données système" • "Déclenchement manuel de l'un des messages AutoSupport" • "L'examen des metrics de support"

Création d'un calendrier des modifications récentes

En cas de problème, vous devriez considérer ce qui a changé récemment et quand ces changements se sont produits.

- Toute modification de votre système StorageGRID, de sa configuration ou de son environnement peut provoquer un nouveau comportement.
- Un calendrier des modifications peut vous aider à identifier les changements susceptibles d'être responsables d'un problème, ainsi que la manière dont chaque changement pourrait avoir affecté son développement.

Créez un tableau des dernières modifications apportées à votre système, qui contient des informations sur la date à laquelle chaque modification a eu lieu, ainsi que des informations pertinentes sur la modification, telles que les autres événements survenus pendant que la modification a été en cours :

Heure de la modification	Type de modification	Détails
Par exemple : • Quand avez-vous démarré la restauration du nœud ? • Quand la mise à niveau logicielle s'est-elle terminée ? • Avez-vous interrompu le processus ?	Que s'est-il passé ? Qu'avez-vous fait ?	Documentez toute information pertinente concernant la modification. Par exemple : • Détails des modifications du réseau. • Quel correctif a été installé. • Changement des workloads clients. Assurez-vous de noter si plusieurs changements ont eu lieu en même temps. Par exemple, ce changement a-t-il été effectué pendant qu'une mise à niveau était en cours ?

Exemples de changements récents importants

Voici quelques exemples de changements potentiellement importants :

- Le système StorageGRID a-t-il été récemment installé, étendu ou récupéré ?
- Le système a-t-il été mis à niveau récemment ? Un correctif a-t-il été appliqué ?
- Du matériel a-t-il été réparé ou modifié récemment ?
- La règle ILM a-t-elle été mise à jour ?
- La charge de travail client a-t-elle changé ?
- L'application client ou son comportement a-t-il changé ?
- Avez-vous modifié des équilibreurs de charge, ou ajouté ou supprimé un groupe haute disponibilité de nœuds d'administration ou de nœuds de passerelle ?
- Certaines tâches lancées peuvent-elles prendre un certain temps ? Voici quelques exemples :
  - Récupération d'un noeud de stockage défaillant
  - Désaffectation des nœuds de stockage
- Des modifications ont-elles été apportées à l'authentification utilisateur, par exemple l'ajout d'un locataire ou la modification de la configuration LDAP ?
- La migration des données a-t-elle lieu ?
- Les services de plateforme ont-ils été récemment activés ou modifiés ?
- La conformité a-t-elle été activée récemment ?
- Les pools de stockage cloud ont-ils été ajoutés ou supprimés ?
- La compression du stockage ou le chiffrement ont-ils été modifiés ?
- L'infrastructure réseau a-t-elle été modifiée ? Par exemple, VLAN, routeurs ou DNS.
- Des modifications ont-elles été apportées aux sources NTP ?
- Des modifications ont-elles été apportées aux interfaces réseau Grid, Admin ou client ?
- Des modifications de configuration ont-elles été apportées au nœud d'archivage ?

- Le système StorageGRID ou son environnement a-t-il subi d'autres modifications ?

Établir des lignes de base

Vous pouvez établir des lignes de base pour votre système en enregistrant les niveaux normaux de différentes valeurs opérationnelles. À l'avenir, vous pourrez comparer les valeurs actuelles à ces lignes de base afin de détecter et de résoudre les valeurs anormales.

Propriété	Valeur	Comment obtenir
Consommation de stockage moyenne	Go utilisés/jour Pourcentage consommé/jour	Accédez à Grid Manager. Sur la page nœuds, sélectionnez la totalité de la grille ou d'un site et accédez à l'onglet stockage. Dans le graphique stockage utilisé - données d'objet, recherchez une période où la ligne est assez stable. Passez le curseur de la souris sur le graphique pour estimer la quantité de stockage consommée chaque jour Vous pouvez collecter ces informations pour l'intégralité du système ou pour un data Center spécifique.
Consommation moyenne des métadonnées	Go utilisés/jour Pourcentage consommé/jour	Accédez à Grid Manager. Sur la page nœuds, sélectionnez la totalité de la grille ou d'un site et accédez à l'onglet stockage. Dans le graphique stockage utilisé - métadonnées d'objet, recherchez une période où la ligne est assez stable. Passez le curseur de la souris sur le graphique pour estimer la quantité de stockage de métadonnées consommée chaque jour Vous pouvez collecter ces informations pour l'intégralité du système ou pour un data Center spécifique.
Vitesse des opérations S3/Swift	Opérations/seconde	Accédez au tableau de bord dans Grid Manager. Dans la section opérations de protocole, affichez les valeurs du taux S3 et du taux Swift. Pour afficher les taux et les nombres d'entrée et de récupération pour un site ou un nœud spécifique, sélectionnez **noeuds** > ***site ou noeud de stockage*** > **objets**. Placez le curseur sur le tableau d'ingestion et de récupération pour S3 ou Swift.
Échec des opérations S3/Swift	Exploitation	Sélectionnez **support** > **Outils** > **topologie de grille**. Dans l'onglet Présentation de la section opérations d'API, affichez la valeur des opérations S3 - FAILED ou opérations Swift - FAILED.
Évaluation des règles ILM	Objets/seconde	Dans la page noeuds, sélectionnez ***grid*** > **ILM**. Dans le graphique ILM Queue, recherchez une période où la ligne est assez stable. Placez le curseur sur le graphique pour estimer une valeur de référence pour **taux d'évaluation** pour votre système.

Propriété	Valeur	Comment obtenir
Taux d'analyse ILM	Objets/seconde	Sélectionnez **Nodes** > ***grid*** > **ILM**. Dans le graphique ILM Queue, recherchez une période où la ligne est assez stable. Placez le curseur sur le graphique pour estimer une valeur de référence pour **Scan rate** pour votre système.
Objets mis en file d'attente à partir des opérations client	Objets/seconde	Sélectionnez **Nodes** > ***grid*** > **ILM**. Dans le graphique ILM Queue, recherchez une période où la ligne est assez stable. Placez le 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*** > **objets**. Dans le tableau requêtes, affichez la valeur de la latence moyenne.

Analyse des données

Utilisez les informations que vous recueillez pour déterminer la cause du problème et les solutions potentielles.

L'analyse dépend du problème, mais en général :

- Localiser les points de défaillance et les goulets d'étranglement à l'aide des alarmes.
- Reconstruire l'historique des problèmes à l'aide de l'historique des alarmes et des graphiques.
- Utiliser les tableaux pour rechercher des anomalies et comparer la situation du problème avec le fonctionnement normal.

Liste de contrôle des informations de réaffectation

Si vous ne pouvez pas résoudre le problème par vous-même, contactez le support technique. Avant de contacter le support technique, collectez les informations du tableau ci-dessous pour faciliter la résolution de votre problème.

✔	Élément	Remarques
	Énoncé du problème	Quels sont les symptômes du problème ? Quand le problème a-t-il démarré ? Cela se produit-il de manière cohérente ou intermittente ? Si elle est intermittente, à quelle heure s'est-elle produite ? "Définition du problème"

✔	Élément	Remarques
	Évaluation de l'impact	Quelle est la gravité du problème ? Quel est l'impact sur l'application client ? • Le client a-t-il déjà été connecté avec succès ? • Le client est-il en mesure d'ingérer, de récupérer et de supprimer des données ?
	ID du système StorageGRID	Sélectionnez **Maintenance** > **système** > **Licence**. L'ID système StorageGRID s'affiche dans le cadre de la licence actuelle.
	Version logicielle	Cliquez sur **aide** > **a propos** pour afficher la version StorageGRID.
	Personnalisation	Résumez le mode de configuration de votre système StorageGRID. Par exemple, énumérez les éléments suivants : • La grille utilise-t-elle la compression du stockage, le chiffrement du stockage ou la conformité ? • ILM effectue-t-il des objets répliqués ou soumis à un code d'effacement ? La ILM permet-elle la redondance des sites ? Les règles ILM utilisent-elles des comportements d'entrée stricts, équilibrés ou à double engagement ?
	Fichiers journaux et données système	Collecte des fichiers journaux et des données système pour votre système. Sélectionnez **support** > **Outils** > **journaux**. Vous pouvez collecter les journaux pour toute la grille ou pour certains nœuds. Si vous ne recueillez des journaux que pour les nœuds sélectionnés, veillez à inclure au moins un nœud de stockage disposant du service ADC. (Les trois premiers nœuds de stockage d'un site incluent le service ADC.) "Collecte des fichiers journaux et des données système"
	Informations de base	Collectez les informations de base relatives aux opérations d'entrée, aux opérations de récupération et à la consommation du stockage. "Établir des lignes de base"
	Chronologie des modifications récentes	Créez un calendrier qui résume les modifications récentes apportées au système ou à son environnement. "Création d'un calendrier des modifications récentes"

✔	Élément	Remarques
	Historique des efforts déployés pour diagnostiquer le problème	Si vous avez pris des mesures pour diagnostiquer ou résoudre vous-même le problème, assurez-vous d'enregistrer les mesures que vous avez prises et les résultats obtenus.

Informations associées

"Administrer StorageGRID"

Résolution des problèmes d'objet et de stockage

Vous pouvez effectuer plusieurs tâches pour déterminer la source des problèmes liés au stockage et à l'objet.

Confirmation de l'emplacement des données d'objet

En fonction du problème, vous pouvez confirmer l'emplacement de stockage des données d'objet. Par exemple, vous pouvez vérifier que la règle ILM fonctionne comme prévu et que les données d'objet sont stockées à l'emplacement prévu.

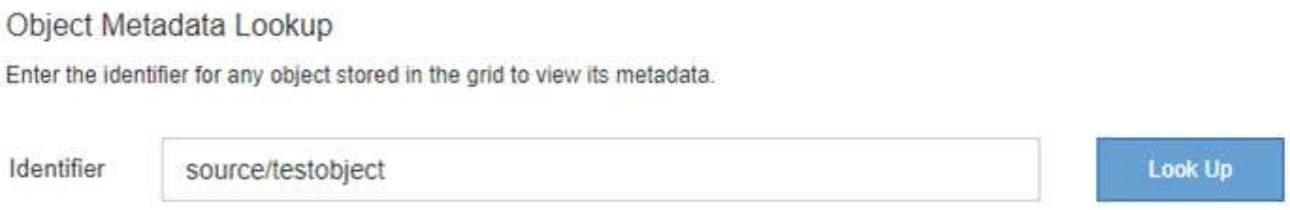
Ce dont vous avez besoin

- Vous devez disposer d'un identifiant d'objet, qui peut être l'un des suivants :
  - **UUID** : identifiant unique universel de l'objet. Saisissez l'UUID en majuscules.
  - **CBID** : identifiant unique de l'objet dans StorageGRID . Vous pouvez obtenir le CBID d'un objet à partir du journal d'audit. Saisissez le CBID en majuscules.
  - **Compartiment S3 et clé d'objet** : lors de l'ingestion d'un objet via l'interface S3, l'application client utilise une combinaison de compartiments et de clés d'objet pour stocker et identifier l'objet.
  - **Conteneur Swift et nom d'objet** : lorsqu'un objet est ingéré via l'interface Swift, l'application cliente utilise une combinaison de conteneur et de nom d'objet pour stocker et identifier l'objet.

Étapes

1. Sélectionnez **ILM** > **recherche de métadonnées d'objet**.
2. Saisissez l'identifiant de l'objet dans le champ **Identificateur**.

   Vous pouvez entrer un UUID, un CBID, un compartiment S3/une clé-objet ou un nom-objet/conteneur Swift.



3. Cliquez sur **chercher**.

   Les résultats de la recherche de métadonnées d'objet s'affichent. Cette page répertorie les types d'informations suivants :

- Les métadonnées du système, y compris l'ID d'objet (UUID), le nom de l'objet, le nom du conteneur, le nom ou l'ID du compte de locataire, la taille logique de l'objet, la date et l'heure de la première création de l'objet, ainsi que la date et l'heure de la dernière modification de l'objet.
- Toutes les paires de clé-valeur de métadonnées utilisateur personnalisées associées à l'objet.
- Pour les objets S3, toutes les paires de clé-valeur de balise d'objet associées à l'objet.
- Pour les copies d'objet répliquées, emplacement de stockage actuel de chaque copie.
- Pour les copies d'objets avec code d'effacement, l'emplacement de stockage actuel de chaque fragment.
- Pour les copies d'objet dans Cloud Storage Pool, l'emplacement de l'objet, notamment le nom du compartiment externe et l'identifiant unique de l'objet.
- Pour les objets segmentés et les objets multisegments, une liste de segments d'objet, y compris les identificateurs de segments et la taille des données. Pour les objets de plus de 100 segments, seuls les 100 premiers segments sont affichés.
- Toutes les métadonnées d'objet dans le format de stockage interne non traité. Ces métadonnées brutes incluent les métadonnées du système interne qui ne sont pas garanties de la version à la version.

  L'exemple suivant présente les résultats de la recherche de métadonnées d'objet pour un objet de test S3 stocké sous forme de deux copies répliquées.

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H$|TFbnQQ}|CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H$|TFboW28|CXG%

Raw Metadata


```
{
    "TYPE": "CTNT",
    "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
    "NAME": "testobject",
    "CBID": "0x8823DE7EC7C10416",
    "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
    "PPTH": "source",
    "META": {
        "BASE": {
            "PAWS": "2",
```


Informations associées

"Gestion des objets avec ILM"

"Utilisation de S3"

"Utiliser Swift"

Défaillances de stockage d'objets (volume de stockage)

Le stockage sous-jacent d'un nœud de stockage est divisé en magasins d'objets. Ces magasins d'objets sont des partitions physiques qui servent de points de montage pour le stockage du système StorageGRID. Les magasins d'objets sont également appelés volumes de stockage.

Vous pouvez afficher les informations de magasin d'objets pour chaque nœud de stockage. Les magasins d'objets sont affichés en bas de la page **Nodes** > ***Storage Node*** > **Storage**.

Disk Devices

Name	World Wide Name	I/O Load	Read Rate	Write Rate
croot(8:1,sda1)	N/A	1.62%	0 bytes/s	177 KB/s
cvloc(8:2,sda2)	N/A	17.28%	0 bytes/s	2 MB/s
sdc(8:16,sdb)	N/A	0.00%	0 bytes/s	11 KB/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	0 bytes/s
sds(8:48,sdd)	N/A	0.00%	0 bytes/s	0 bytes/s

Volumes

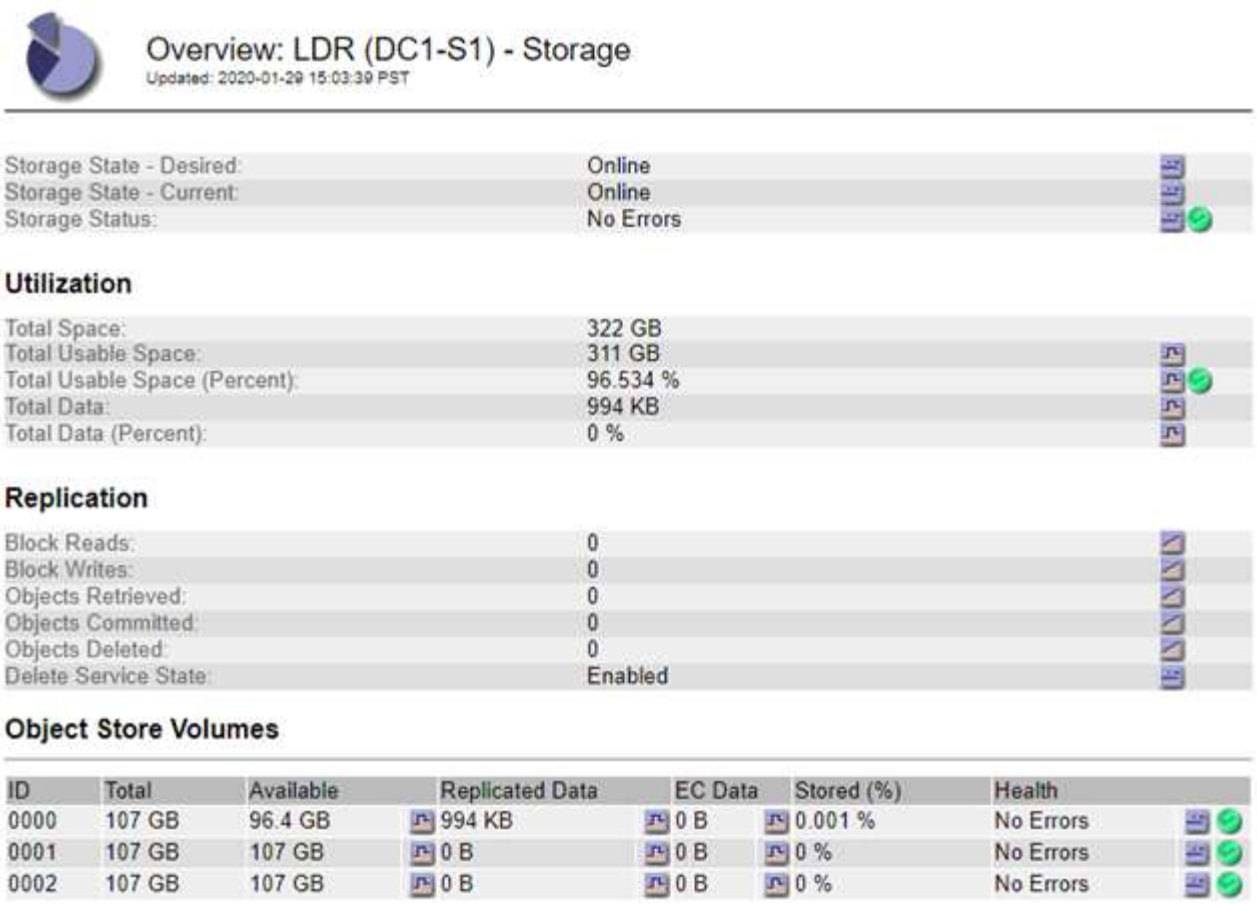
Mount Point	Device	Status	Size	Available	Write Cache Status
/	croot	Online	21.00 GB	14.25 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.39 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sds	Online	107.32 GB	107.18 GB	Enabled

Object Stores

ID	Size	Available	Replicated Data	EC Data	Object Data (%)	Health
0000	107.32 GB	96.45 GB	994.37 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

Pour plus de détails sur chaque nœud de stockage, procédez comme suit :

1. Sélectionnez **support** > **Outils** > **topologie de grille**.
2. Sélectionnez ***site*** > ***Storage Node*** > **LDR** > **Storage** > **Présentation** > **main**.



Selon la nature de la défaillance, des défaillances liées à un volume de stockage peuvent se refléter dans une alarme indiquant l'état du stockage ou l'état de santé d'un magasin d'objets. En cas de défaillance d'un volume de stockage, réparez le volume de stockage défectueux pour restaurer le nœud de stockage à son plein fonctionnement dès que possible. Si nécessaire, vous pouvez accéder à l'onglet **Configuration** et placer le nœud de stockage en lecture seule de sorte que le système StorageGRID puisse l'utiliser pour récupérer les données tout en préparant la récupération complète du serveur.

Informations associées

"Maintenance et récupération"

Vérification de l'intégrité des objets

Le système StorageGRID vérifie l'intégrité des données d'objet sur les nœuds de stockage, en vérifiant la présence d'objets corrompus et manquants.

Il existe deux processus de vérification : la vérification des antécédents et la vérification de premier plan. Elles travaillent ensemble pour assurer l'intégrité des données. La vérification en arrière-plan s'exécute automatiquement et vérifie en continu l'exactitude des données d'objet. La vérification de premier plan peut être déclenchée par un utilisateur, afin de 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 des copies corrompues de données d'objet et tente automatiquement de résoudre les problèmes qu'il trouve.

La vérification en arrière-plan vérifie l'intégrité des objets répliqués et des objets avec code d'effacement, comme suit :

- **Objets répliqués** : si le processus de vérification en arrière-plan trouve un objet répliqué corrompu, la copie corrompue est supprimée de son emplacement et mise en quarantaine ailleurs sur le noeud de stockage. Une nouvelle copie non corrompue est ensuite générée et placée pour satisfaire la politique ILM active. Il se peut que la nouvelle copie ne soit pas placée sur le nœud de stockage utilisé pour la copie d'origine.

> Les données d'objet corrompues sont mises en quarantaine au lieu d'être supprimées du système, de sorte qu'elles soient toujours accessibles. Pour plus d'informations sur l'accès aux données d'objet en quarantaine, contactez le support technique.

- **Objets avec code d'effacement** : si le processus de vérification en arrière-plan détecte qu'un fragment d'un objet avec code d'effacement est corrompu, StorageGRID tente automatiquement de reconstruire le fragment manquant en place sur le même nœud de stockage, en utilisant les données restantes et les fragments de parité. Si le fragment corrompu ne peut pas être reconstruit, l'attribut copies corrompues détectées (ECOR) est incrémenté d'un seul et une tentative est effectuée pour récupérer une autre copie de l'objet. Lorsque la récupération réussit, une évaluation du ILM est effectuée pour créer une copie de remplacement de l'objet avec code d'effacement.

  Le processus de vérification en arrière-plan vérifie uniquement les objets sur les nœuds de stockage. Elle ne vérifie pas les objets sur les nœuds d'archivage ou dans un pool de stockage cloud. Les objets doivent être âgés de plus de quatre jours pour être admissibles à la vérification des antécédents.

La vérification des antécédents s'exécute à un taux continu conçu pour ne pas interférer avec les activités ordinaires du système. Impossible d'arrêter la vérification de l'arrière-plan. Toutefois, vous pouvez augmenter le taux de vérification en arrière-plan pour vérifier plus rapidement le contenu d'un nœud de stockage si vous soupçonnez un problème.

Alertes et alarmes (anciennes) liées à la vérification des antécédents

Si le système détecte un objet corrompu qu'il ne peut pas corriger automatiquement (car 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** et l'alarme héritée PERDUE (objets perdus) sont déclenchées.

Modification du taux de vérification du bruit de fond

Vous pouvez modifier la vitesse à laquelle la vérification en arrière-plan vérifie les données d'objet répliquées sur un nœud de stockage si vous avez des problèmes d'intégrité des données.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

Vous pouvez modifier le taux de vérification pour la vérification en arrière-plan sur un nœud de stockage :

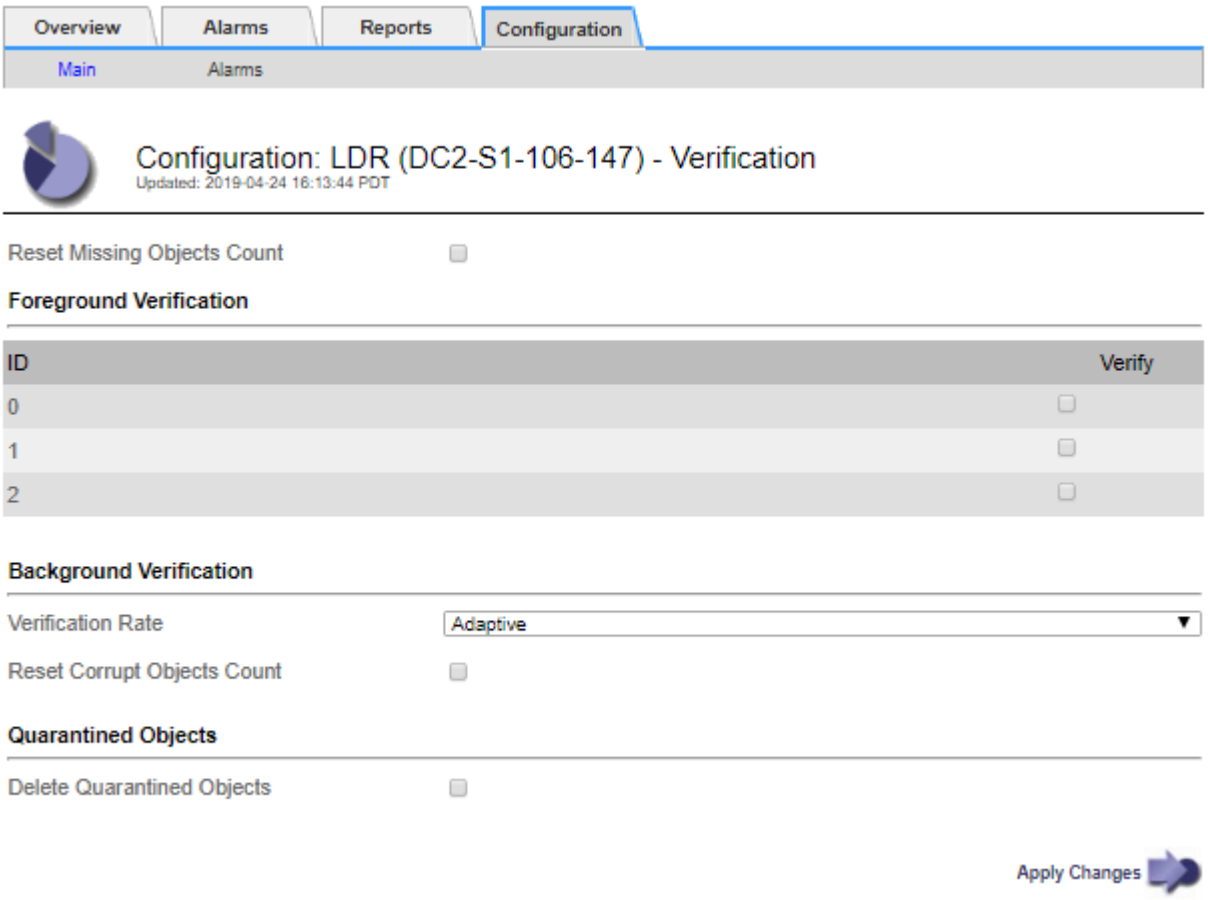
- Adaptatif : paramètre par défaut. La tâche est conçue pour vérifier à un maximum de 4 Mo/s ou 10 objets/s (selon la première limite dépassée).

- Élevé : la vérification du stockage s'effectue rapidement, à une vitesse qui peut ralentir les activités ordinaires des systèmes.

Utilisez le taux de vérification élevé uniquement si vous soupçonnez qu'une erreur matérielle ou logicielle pourrait avoir des données d'objet corrompues. Une fois la vérification de l'arrière-plan de priorité élevée terminée, le taux de vérification se réinitialise automatiquement sur Adaptive.

Étapes

1. Sélectionnez **support** > **Outils** > **topologie de grille**.
2. Sélectionnez ***Storage Node*** **> LDR > Verification**.
3. Sélectionnez **Configuration** > **main**.
4. Accédez à **LDR** > **Verification** > **Configuration** > **main**.
5. Sous Vérification de l'arrière-plan, sélectionnez **taux de vérification** > **taux élevé** ou **taux de vérification** > **adaptatif**.



Le réglage du taux de vérification sur élevé déclenche l'alarme VPRI (taux de vérification) héritée au niveau des notifications.

1. Cliquez sur **appliquer les modifications**.
2. Surveiller les résultats de la vérification en arrière-plan des objets répliqués.
   a. Accédez à **noeuds** > ***Storage Node*** > **objets**.
   b. Dans la section Vérification, surveillez les valeurs de **objets corrompus** et **objets corrompus non**

identifiés.

Si la vérification en arrière-plan trouve des données d'objet répliqué corrompues, la mesure **objets corrompus** est incrémentée et StorageGRID tente d'extraire l'identificateur d'objet des données, comme suit :

- Si l'identifiant d'objet peut être extrait, StorageGRID crée automatiquement une nouvelle copie des données de l'objet. La nouvelle copie peut être effectuée à tout emplacement du système StorageGRID conformément à la politique ILM active.
- Si l'identificateur d'objet ne peut pas être extrait (car il a été corrompu), la mesure **objets corrompus non identifiés** est incrémentée et l'alerte **objet corrompu non identifié détecté** est déclenchée.

c. Si des données d'objet répliqué corrompues sont trouvées, contactez le support technique pour déterminer la cause première de la corruption.

3. Surveillez les résultats de la vérification en arrière-plan des objets avec code d'effacement.

   Si la vérification en arrière-plan détecte des fragments corrompus de données d'objet codées par effacement, l'attribut fragments corrompus détectés est incrémenté. StorageGRID restaure en reconstruisant le fragment corrompu sur le même nœud de stockage.

   a. Sélectionnez **support** > **Outils** > **topologie de grille**.
   b. Sélectionnez ***Storage Node*** **> LDR > codage d'effacement**.
   c. Dans le tableau Résultats de la vérification, surveillez l'attribut fragments corrompus détectés (ECCD).

4. Une fois les objets corrompus automatiquement restaurés par le système StorageGRID, réinitialisez le nombre d'objets corrompus.
   a. Sélectionnez **support** > **Outils** > **topologie de grille**.
   b. Sélectionnez ***Storage Node*** **> LDR > Vérification > Configuration**.
   c. Sélectionnez **Réinitialiser le nombre d'objets corrompus**.
   d. Cliquez sur **appliquer les modifications**.
5. Si vous êtes sûr que les objets mis en quarantaine ne sont pas nécessaires, vous pouvez les supprimer.

> Si l'alerte **objets perdus** ou L'alarme héritée PERDUS (objets perdus) a été déclenchée, le support technique peut vouloir accéder aux objets mis en quarantaine pour aider à déboguer le problème sous-jacent ou à tenter la récupération des données.

1. Sélectionnez **support** > **Outils** > **topologie de grille**.
2. Sélectionnez ***Storage Node*** > **LDR** > **Verification** > **Configuration**.
3. Sélectionnez **Supprimer les objets en quarantaine**.
4. Cliquez sur **appliquer les modifications**.

La vérification de premier plan

La vérification avant-plan est un processus initié par l'utilisateur qui vérifie si toutes les données d'objet attendues existent sur un nœud de stockage. La vérification de premier plan est utilisée pour vérifier l'intégrité d'un périphérique de stockage.

Il s'agit d'une alternative plus rapide à la vérification en arrière-plan qui vérifie l'existence, mais pas l'intégrité, des données d'objet sur un nœud de stockage. Si la vérification au premier plan détecte que de nombreux

éléments sont manquants, il peut y avoir un problème avec tout ou partie d'un périphérique de stockage associé au nœud de stockage.

La vérification premier plan vérifie les données d'objet répliquées et les données d'objet avec code d'effacement, comme suit :

- **Objets répliqués** : si une copie de données d'objet répliqué est manquante, StorageGRID tente automatiquement de remplacer la copie à partir de copies stockées ailleurs dans le système. Le nœud de stockage exécute une copie existante via une évaluation ILM. Cette dernière détermine que la politique ILM actuelle n'est plus respectée pour cet objet, car la copie manquante n'existe plus à l'emplacement prévu. Une nouvelle copie est générée et placée pour satisfaire la politique ILM active du système. Cette nouvelle copie peut ne pas être placée au même emplacement que la copie manquante.
- **Objets avec code d'effacement** : si un fragment d'un objet avec code d'effacement est manquant, StorageGRID tente automatiquement de reconstruire le fragment manquant sur le même noeud de stockage en utilisant les fragments restants. Si le fragment manquant ne peut pas être reconstruit (parce que trop de fragments ont été perdus), l'attribut de copies corrompues détectées (ECOR) est incrémenté d'un. ILM tente ensuite de trouver une autre copie de l'objet qui peut ensuite servir à générer une nouvelle copie codée d'effacement.

  Si la vérification au premier plan identifie un problème de codage d'effacement sur un volume de stockage, la tâche de vérification au premier plan s'interrompt et un message d'erreur identifie le volume affecté. Vous devez effectuer une procédure de restauration pour tous les volumes de stockage concernés.

Si aucune autre copie d'un objet répliqué manquant ou d'un objet à code d'effacement corrompu n'est trouvée dans la grille, l'alerte **objets perdus** et l'alarme héritée PERDUE (objets perdus) sont déclenchées.

Exécution de la vérification de premier plan

La vérification de premier plan vous permet de vérifier l'existence de données sur un nœud de stockage. Des données d'objet manquantes peuvent indiquer qu'un problème existe avec le périphérique de stockage sous-jacent.

Ce dont vous avez besoin

- Vous avez vérifié que les tâches de grille suivantes ne sont pas en cours d'exécution :
  - Extension de grille : ajoutez un serveur (GEXP) lors de l'ajout d'un noeud de stockage
  - Le service de désaffectation des nœuds de stockage (LDCM) sur le même nœud de stockage si ces tâches de la grille sont en cours d'exécution, attendez qu'elles soient terminées ou relâchés.
- Vous avez vérifié que le stockage est en ligne. (Sélectionnez **support** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***Storage Node*** > **LDR** > **Storage** > **Overview** > **main**. Assurez-vous que **État de stockage - actuel** est en ligne.)
- Vous avez vérifié que les procédures de restauration suivantes ne sont pas exécutées sur le même nœud de stockage :
  - Restauration d'un volume de stockage défaillant
  - La récupération d'un nœud de stockage avec une vérification de premier plan de lecteur système ayant échoué ne fournit pas d'informations utiles tant que les procédures de récupération sont en cours.

Description de la tâche

Vérifications de premier plan des données d'objet répliqué manquantes et des données d'objet à code d'effacement manquantes :

- Si la vérification avant-plan détecte de grandes quantités de données d'objet manquantes, il est probable

que le stockage du nœud de stockage soit soumis à une étude et à une résolution.

- Si la vérification au premier plan détecte une erreur de stockage grave associée aux données avec code d'effacement, elle vous en informe. Vous devez effectuer la récupération du volume de stockage pour corriger l'erreur.

Vous pouvez configurer la vérification en premier plan pour vérifier tous les magasins d'objets d'un nœud de stockage ou uniquement des magasins d'objets spécifiques.

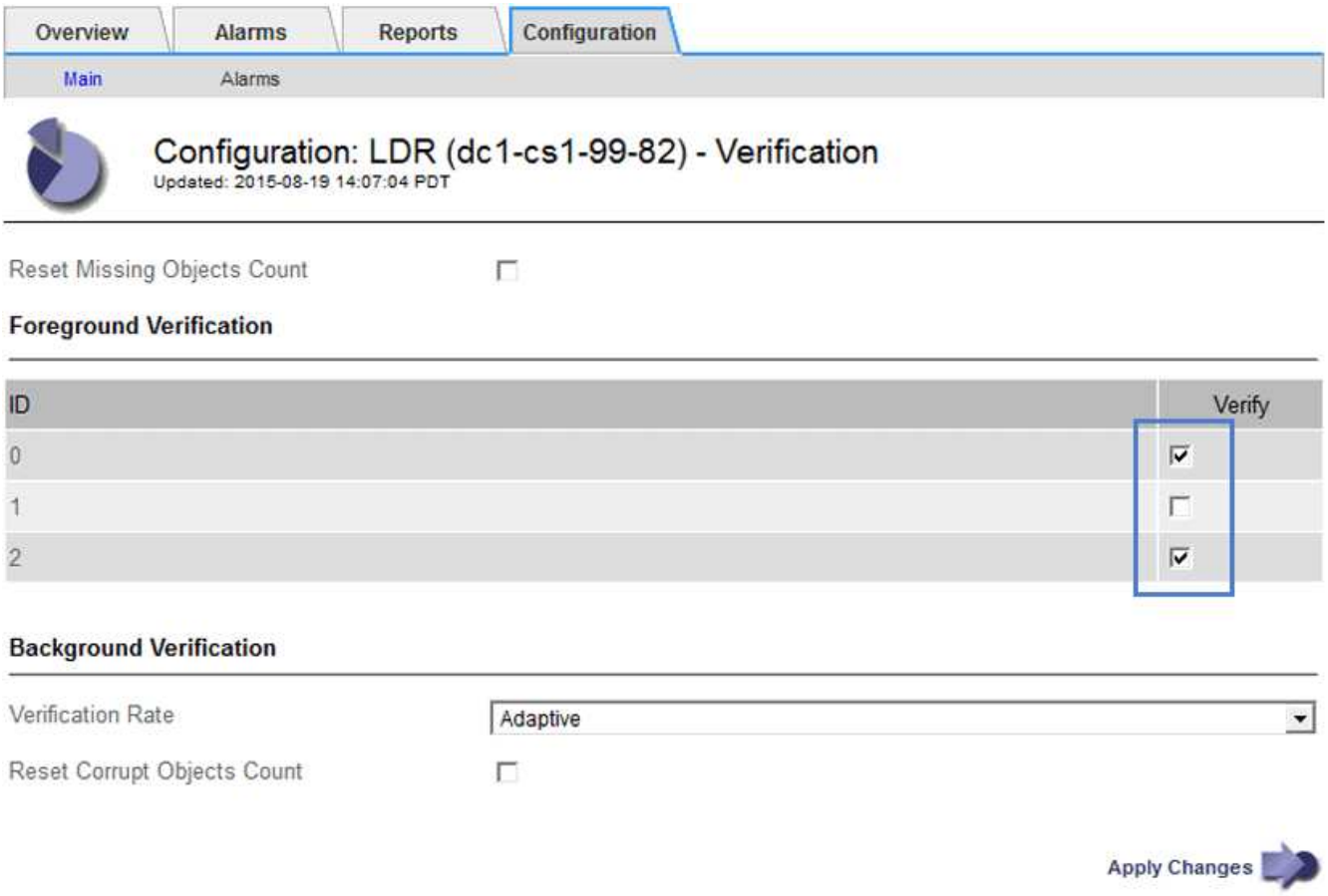
Si la vérification au premier plan trouve des données d'objet manquantes, le système StorageGRID tente de les remplacer. Si une copie de remplacement ne peut pas être effectuée, l'alarme OBJETS PERDUS peut être déclenchée.

La vérification par premier plan génère une tâche de grille de vérification par premier plan LDR qui, selon le nombre d'objets stockés sur un nœud de stockage, peut prendre plusieurs jours ou plusieurs semaines. Il est possible de sélectionner plusieurs nœuds de stockage en même temps, mais ces tâches de grille ne sont pas exécutées simultanément. Au lieu de cela, elles sont mises en file d'attente et s'exécutent l'une après l'autre jusqu'à la fin. Lorsque la vérification de premier plan est en cours sur un nœud de stockage, vous ne pouvez pas démarrer une autre tâche de vérification de premier plan sur ce même nœud de stockage, même si l'option de vérification de volumes supplémentaires peut sembler disponible pour le nœud de stockage.

Si un nœud de stockage autre que celui où la vérification de premier plan est exécutée passe hors ligne, la tâche de grille continue à s'exécuter jusqu'à ce que l'attribut **% Complete** atteigne 99.99 pour cent. L'attribut **% Complete** revient ensuite à 50 % et attend que le nœud de stockage revienne à l'état en ligne. Lorsque l'état du nœud de stockage revient en ligne, la tâche de grille de vérification hors-plan LDR se poursuit jusqu'à sa fin.

Étapes

1. Sélectionnez ***Storage Node*** > **LDR** > **Verification**.
2. Sélectionnez **Configuration** > **main**.
3. Sous **Vérification de premier plan**, cochez la case pour chaque ID de volume de stockage que vous voulez vérifier.



4. Cliquez sur **appliquer les modifications**.

   Attendez que la page se réactualise et se recharge automatiquement avant de quitter la page. Une fois les magasins d'objets actualisés, ils ne peuvent plus être sélectionnés sur ce nœud de stockage.

   Une tâche de grille de vérification de premier plan LDR est générée et exécutée jusqu'à ce qu'elle soit terminée, interrompue ou abandonnée.

5. Surveiller les objets manquants ou les fragments manquants :

   a. Sélectionnez ***Storage Node*** > **LDR** > **Verification**.

   b. Dans l'onglet vue d'ensemble sous **Résultats de vérification**, notez la valeur de **objets manquants détectés**.

      Remarque : la même valeur est signalée comme **objets perdus** sur la page noeuds. Accédez à **noeuds** > ***Storage Node***, puis sélectionnez l'onglet **objets**.

      Si le nombre de **objets manquants détectés** est important (s'il y a des centaines d'objets manquants), il y a probablement un problème avec le stockage du nœud de stockage. Contactez l'assistance technique.

   c. Sélectionnez ***Storage Node*** > **LDR** > **codage d'effacement**.

   d. Dans l'onglet vue d'ensemble sous **Résultats de vérification**, notez la valeur de **fragments manquants détectés**.

      Si le nombre de **fragments manquants détectés** est important (s'il y a des centaines de fragments manquants), il y a probablement un problème avec le stockage du nœud de stockage. Contactez

l'assistance technique.

Si la vérification au premier plan ne détecte pas un nombre important de copies d'objet répliquées manquantes ou un nombre significatif de fragments manquants, alors le stockage fonctionne normalement.

6. Surveiller l'achèvement de la tâche de grille de vérification de premier plan :
   a. Sélectionnez **support** > **Outils** > **topologie de grille**. Sélectionnez ensuite **site** > ***Admin Node*** > **CMN** > **Grid Task** > **Overview** > **main**.
   b. Vérifiez que la tâche de la grille de vérification de premier plan progresse sans erreur.

      Remarque : une alarme de niveau de notification est déclenchée sur l'état de la tâche de grille (SCAS) si la tâche de grille de vérification de premier plan est interrompue.

   c. Si la tâche de grille s'interrompt avec un `critical storage error`, récupérez le volume affecté, puis exécutez la vérification de premier plan sur les volumes restants pour rechercher d'autres erreurs.

      Attention : si la tâche de la grille de vérification de premier plan s'interrompt avec le message `Encountered a critical storage error in volume volID`, vous devez effectuer la procédure de récupération d'un volume de stockage défaillant. Reportez-vous aux instructions de récupération et d'entretien.

Une fois que vous avez terminé

Si vous avez toujours des préoccupations concernant l'intégrité des données, allez à **LDR** > **Verification** > **Configuration** > **main** et augmentez le taux de vérification en arrière-plan. La vérification en arrière-plan vérifie l'exactitude de toutes les données d'objet stockées et répare tout problème détecté. Trouver et réparer les problèmes le plus rapidement possible réduit le risque de perte de données.

Informations associées

"Maintenance et récupération"

Dépannage des données d'objet perdues ou manquantes

Les objets peuvent être récupérés pour plusieurs raisons, y compris les demandes de lecture provenant d'une application client, les vérifications en arrière-plan des données d'objet répliquées, les réévaluations ILM et la restauration des données d'objet lors de la restauration d'un nœud de stockage.

Le système StorageGRID utilise les informations d'emplacement dans les métadonnées d'un objet pour déterminer l'emplacement à partir duquel vous souhaitez récupérer l'objet. Si une copie de l'objet n'est pas trouvée à l'emplacement prévu, le système tente de récupérer une autre copie de l'objet à partir d'un autre emplacement du système, en supposant que la règle ILM contient une règle permettant de créer au moins deux copies de l'objet.

Si cette récupération réussit, le système StorageGRID remplace la copie manquante de l'objet. Dans le cas contraire, l'alerte **objets perdus** et l'alarme hérité PERDUS (objets perdus) sont déclenchées, comme suit :

- Pour les copies répliquées, si une autre copie ne peut pas être récupérée, l'objet est considéré comme perdu et l'alerte et l'alarme sont déclenchées.
- Pour les copies avec code d'effacement, si une copie ne peut pas être extraite de l'emplacement prévu, l'attribut ECOR (corrompues copies détectées) est incrémenté d'une seule fois avant qu'une tentative de récupération d'une copie à partir d'un autre emplacement soit effectuée. Si aucune autre copie n'est trouvée, l'alerte et l'alarme sont déclenchées.

Vous devez examiner immédiatement toutes les alertes **objets perdus** pour déterminer la cause principale de la perte et déterminer si l'objet peut toujours exister dans un nœud hors ligne ou actuellement indisponible, un nœud de stockage ou un nœud d'archivage.

Dans le cas où les données d'objet sans copie sont perdues, il n'y a pas de solution de récupération. Cependant, vous devez réinitialiser le compteur d'objets perdus pour empêcher les objets perdus connus de masquer les nouveaux objets perdus.

Informations associées

"Analyse des objets perdus"

"Réinitialisation du nombre d'objets perdus et manquants"

Analyse des objets perdus

Lorsque l'alarme **objets perdus** et l'alarme hérité PERDUS (objets perdus) sont déclenchées, vous devez examiner immédiatement. Collectez des informations sur les objets affectés et contactez le support technique.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.
- Vous devez avoir le `Passwords.txt` fichier.

Description de la tâche

L'alerte **objets perdus** et l'alarme PERDUE indiquent que StorageGRID estime qu'il n'y a pas de copie d'un objet dans la grille. Les données ont peut-être été définitivement perdues.

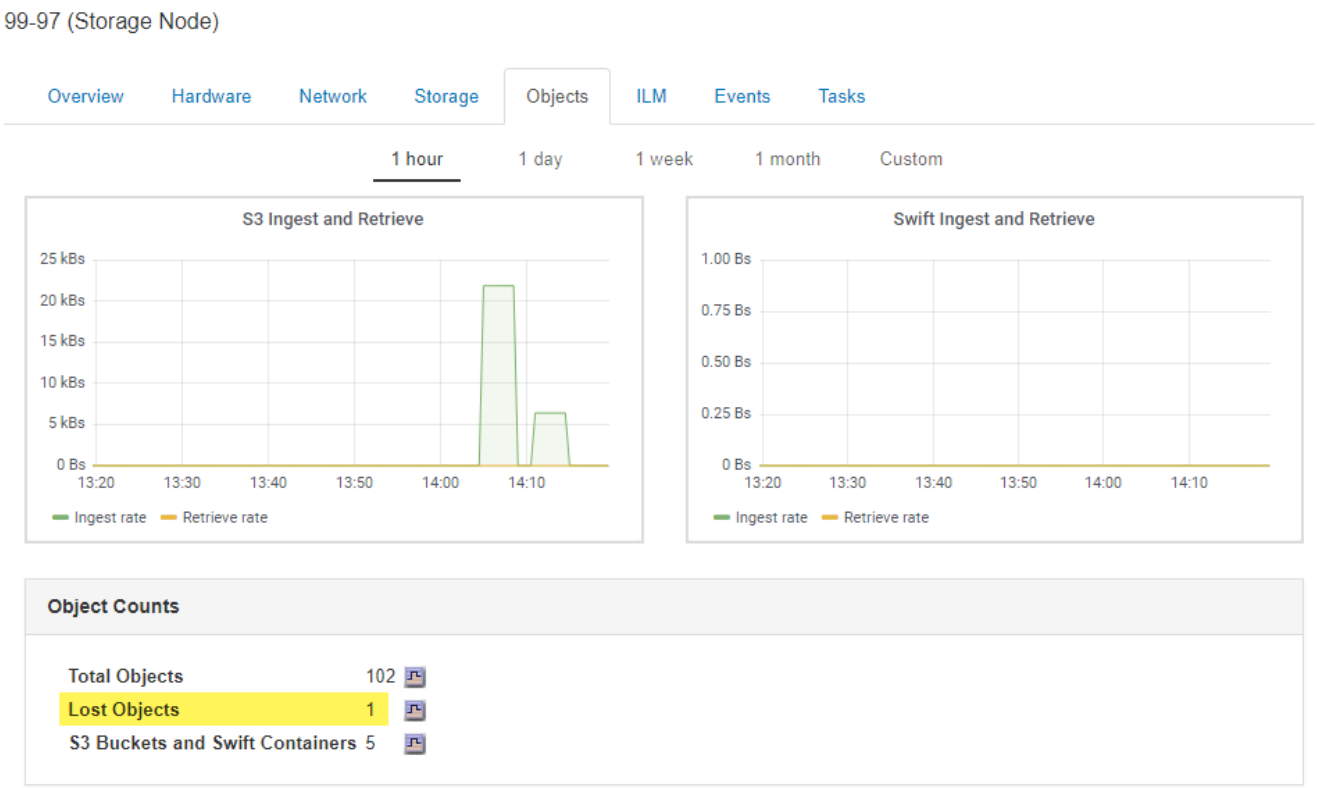
Recherchez immédiatement les alarmes ou les alertes relatives aux objets perdus. Vous devrez peut-être prendre des mesures pour éviter d'autres pertes de données. Dans certains cas, vous pourrez peut-être restaurer un objet perdu si vous prenez une action d'invite.

Le nombre d'objets perdus est visible dans le gestionnaire de grille.

Étapes

1. Sélectionnez **noeuds**.
2. Sélectionnez ***Storage Node*** > **objets**.
3. Vérifiez le nombre d'objets perdus affiché dans le tableau nombres d'objets.

   Ce nombre indique le nombre total d'objets que ce nœud de grille détecte comme manquant dans l'ensemble du système StorageGRID. La valeur est la somme des compteurs d'objets perdus du composant de stockage de données dans les services LDR et DDS.



4. À partir d'un nœud d'administration, accédez au journal d'audit pour déterminer l'identifiant unique (UUID) de l'objet qui a déclenché l'alerte **objets perdus** et l'alarme PERDUE :
   a. Connectez-vous au nœud grid :
      i. Saisissez la commande suivante : `ssh admin@grid_node_IP`
      ii. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
      iii. Entrez la commande suivante pour passer à la racine : `su -`
      iv. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier. Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.
   b. Accédez au répertoire dans lequel se trouvent les journaux d'audit. Entrez : `cd /var/local/audit/export/`
   c. Utilisez grep pour extraire les messages d'audit objet perdu (OLST). Entrez : `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. Utilisez le `ObjectByUUID` Commande permettant de rechercher l'objet par son identificateur (UUID), puis de déterminer si les données sont à risque.

   a. Telnet vers localhost 1402 pour accéder à la console LDR.

   b. Entrez : `/proc/OBRP/ObjectByUUID UUID_value`

      Dans ce premier exemple, l'objet avec `UUID 926026C4-00A4-449B-AC72-BCCA72DD1311` comporte deux emplacements répertoriés.

```
ade 12448208: /proc/OBRP > ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-
ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
            "ITME": "1581534970983000"
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    },
```

```
    "CLCO\(Locations\)": \[
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12448208",
            "VOLI\(Volume ID\)": "3222345473",
            "Object File Path":
"/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila\#3udu",
            "LTIM\(Location timestamp\)": "2020-02-
12T19:36:17.880569"
        \},
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12288733",
            "VOLI\(Volume ID\)": "3222345984",
            "Object File Path":
"/var/local/rangedb/0/p/19/11/00rH0%DkRt78Rrb\#3s;L",
            "LTIM\(Location timestamp\)": "2020-02-
12T19:36:17.934425"
        }
    ]
}
```

Dans le second exemple, l'objet avec `UUID 926026C4-00A4-449B-AC72-BCCA72DD1311` n'a aucun emplacement répertorié.

```
ade 12448208: / > /proc/OBRP/ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
            "ITME": "1581534970983000"
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    }
}
```

a. Examinez le résultat de /proc/OBRP/ObjectByUUID et prenez les mesures appropriées :

Les métadonnées	Conclusion
Aucun objet trouvé ("ERREUR":")	Si l'objet n'est pas trouvé, le message "ERREUR":" est renvoyé. Si l'objet n'est pas trouvé, vous pouvez ignorer l'alarme en toute sécurité. L'absence d'objet indique que l'objet a été supprimé intentionnellement.
Emplacements 0	Si des emplacements sont répertoriés dans la sortie, l'alarme objets perdus peut être un faux positif. Vérifiez que les objets existent. Utilisez l'ID de nœud et le chemin du fichier indiqués dans la sortie pour confirmer que le fichier objet se trouve à l'emplacement indiqué. (La procédure de recherche d'objets potentiellement perdus explique comment utiliser l'ID de nœud pour trouver le nœud de stockage correct.) "Recherche et restauration d'objets potentiellement perdus" Si les objets existent, vous pouvez réinitialiser le nombre d'objets perdus pour effacer l'alarme et l'alerte.
Emplacements = 0	Si aucun emplacement n'est répertorié dans le résultat, l'objet est potentiellement manquant. Vous pouvez essayer de trouver et de restaurer l'objet vous-même, ou vous pouvez contacter le support technique. "Recherche et restauration d'objets potentiellement perdus" L'assistance technique peut vous demander si une procédure de restauration du stockage est en cours. C'est-à-dire qu'une commande *repair-Data* a été émise sur un nœud de stockage, et la restauration est-elle toujours en cours ? Consultez les informations sur la restauration des données d'objet vers un volume de stockage dans les instructions de restauration et de maintenance.

Informations associées

"Maintenance et récupération"

"Examiner les journaux d'audit"

Recherche et restauration d'objets potentiellement perdus

Il est possible de trouver et de restaurer des objets qui ont déclenché une alarme objets perdus (PERDUS) et une alerte **objet perdu** et que vous avez identifié comme potentiellement perdus.

Ce dont vous avez besoin

- Vous devez avoir l'UUID de tout objet perdu, tel qu'il est identifié dans « enquête sur les objets perdus ».

- Vous devez avoir le `Passwords.txt` fichier.

Description de la tâche

Vous pouvez suivre cette procédure pour rechercher les copies répliquées de l'objet perdu ailleurs dans la grille. Dans la plupart des cas, l'objet perdu est introuvable. Toutefois, dans certains cas, vous pouvez trouver et restaurer un objet répliqué perdu si vous prenez une action rapide.

Pour obtenir de l'aide sur cette procédure, contactez le support technique.

Étapes

1. À partir d'un nœud d'administration, recherchez dans les journaux d'audit les emplacements d'objets possibles :
   a. Connectez-vous au nœud grid :
      i. Saisissez la commande suivante : `ssh admin@grid_node_IP`
      ii. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
      iii. Entrez la commande suivante pour passer à la racine : `su -`
      iv. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier. Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.
   b. Accédez au répertoire dans lequel se trouvent les journaux d'audit : `cd /var/local/audit/export/`
   c. Utilisez grep pour extraire les messages d'audit associés à l'objet potentiellement perdu et les envoyer vers un fichier de sortie. Entrez : `grep uuid-valueaudit_file_name > output_file_name`

      Par exemple :

      ```
      Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
      messages_about_lost_object.txt
      ```

   d. Utilisez grep pour extraire les messages d'audit emplacement perdu (LLST) de ce fichier de sortie. Entrez : `grep LLST output_file_name`

      Par exemple :

      ```
      Admin: # grep LLST messages_about_lost_objects.txt
      ```

      Un message d'audit LLST ressemble à cet exemple de message.

```
[AUDT:\[NOID\(UI32\):12448208\][CBIL(UI64):0x38186FE53E3C49A5]
[UUID(CSTR):"926026C4-00A4-449B-AC72-BCCA72DD1311"][LTYP(FC32):CLDI]
[PCLD\(CSTR\):"/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%\#3tN6"\]
[TSRC(FC32):SYST][RSLT(FC32):NONE][AVER(UI32):10][ATIM(UI64):
1581535134379225][ATYP(FC32):LLST][ANID(UI32):12448208][AMID(FC32):CL
SM]
[ATID(UI64):7086871083190743409]]
```

e. Recherchez le champ PCLD et LE champ NOID dans le message LLST.

Le cas échéant, la valeur de PCLD correspond au chemin complet du disque vers la copie de l'objet répliqué manquante. La valeur de NOID est l'ID de nœud du LDR dans lequel une copie de l'objet peut être trouvée.

Si vous trouvez un emplacement d'objet, vous pourrez peut-être restaurer l'objet.

f. Recherchez le nœud de stockage pour cet ID de nœud LDR.

Il existe deux façons d'utiliser l'ID de nœud pour trouver le nœud de stockage :

- Dans le Gestionnaire de grille, sélectionnez **support** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***Data Center*** > ***Storage Node*** > **LDR**. L'ID de nœud LDR se trouve dans le tableau Node information. Vérifiez les informations pour chaque nœud de stockage jusqu'à ce que vous trouviez celui qui héberge ce LDR.
- Téléchargez et décompressez le pack de récupération pour la grille. Il y a un répertoire *\docs* dans LEDIT package. Si vous ouvrez le fichier index.html, le récapitulatif des serveurs affiche tous les ID de nœud de tous les nœuds de la grille.

2. Déterminez si l'objet existe sur le nœud de stockage indiqué dans le message d'audit :

a. Connectez-vous au nœud grid :

i. Saisissez la commande suivante : `ssh admin@grid_node_IP`

ii. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

iii. Entrez la commande suivante pour passer à la racine : `su -`

iv. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

b. Déterminez si le chemin du fichier de l'objet existe.

Pour le chemin du fichier de l'objet, utilisez la valeur PCLD du message d'audit LLST.

Par exemple, entrez :

```
ls '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
```

Remarque : placez toujours le chemin du fichier d'objet entre guillemets dans des commandes pour échapper à tout caractère spécial.

- Si le chemin d'accès à l'objet est introuvable, il est perdu et ne peut pas être restauré à l'aide de cette procédure. Contactez l'assistance technique.
- Si le chemin d'accès à l'objet est trouvé, passez à l'étape Restaurez l'objet sur StorageGRID. Vous pouvez essayer de restaurer à nouveau l'objet trouvé dans StorageGRID.

1. Si le chemin d'accès à l'objet a été trouvé, essayez de restaurer l'objet sur StorageGRID :
   a. À partir du même nœud de stockage, modifiez la propriété du fichier objet afin qu'il puisse être géré par StorageGRID. Entrez : `chown ldr-user:bycast 'file_path_of_object'`
   b. Telnet vers localhost 1402 pour accéder à la console LDR. Entrez : `telnet 0 1402`
   c. Entrez : `cd /proc/STOR`
   d. Entrez : `Object_Found 'file_path_of_object'`

      Par exemple, entrez :

      ```
      Object_Found '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
      ```

      Émission du `Object\_Found` commande informe la grille de l'emplacement de l'objet. Il déclenche également la règle ILM active, qui crée des copies supplémentaires, comme spécifié dans la règle.

      Remarque : si le noeud de stockage sur lequel vous avez trouvé l'objet est hors ligne, vous pouvez copier l'objet sur n'importe quel noeud de stockage en ligne. Placez l'objet dans un répertoire /var/local/rangedb du noeud de stockage en ligne. Ensuite, émettez le `Object\_Found` commande utilisant ce chemin de fichier pour l'objet.

      - Si l'objet ne peut pas être restauré, le `Object\_Found` échec de la commande. Contactez l'assistance technique.
      - Si l'objet a été restauré avec succès dans StorageGRID, un message de réussite s'affiche. Par exemple :

        ```
        ade 12448208: /proc/STOR > Object_Found
        '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'

        ade 12448208: /proc/STOR > Object found succeeded.
        First packet of file was valid. Extracted key: 38186FE53E3C49A5
        Renamed '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6' to
        '/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila#3udu'
        ```

        Passez à l'étape Vérifiez que de nouveaux emplacements ont été créés

1. Si l'objet a été restauré dans StorageGRID, vérifiez que de nouveaux emplacements ont été créés.
   a. Entrez : `cd /proc/OBRP`
   b. Entrez : `ObjectByUUID UUID_value`

      L'exemple suivant montre qu'il existe deux emplacements pour l'objet avec l'UUID 926026C4-00A4-449B-AC72-BCCA72DD1311.

```
ade 12448208: /proc/OBRP > ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
            "ITME": "1581534970983000"
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    },
    "CLCO\(Locations\)": \[
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12448208",
            "VOLI\(Volume ID\)": "3222345473",
            "Object File Path":
"/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila\#3udu",
            "LTIM\(Location timestamp\)": "2020-02-12T19:36:17.880569"
        \},
```

```
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12288733",
            "VOLI\(Volume ID\)": "3222345984",
            "Object File Path":
"/var/local/rangedb/0/p/19/11/00rH0%DkRt78Rrb\#3s;L",
            "LTIM\(Location timestamp\)": "2020-02-12T19:36:17.934425"
        }
    ]
}
```

a. Se déconnecter de la console LDR. Entrez : `exit`

2. À partir d'un nœud d'administration, recherchez dans les journaux d'audit le message d'audit ORLM correspondant à cet objet pour vous assurer que la gestion du cycle de vie des informations (ILM) a placé des copies, si nécessaire.

   a. Connectez-vous au nœud grid :

      i. Saisissez la commande suivante : `ssh admin@grid_node_IP`

      ii. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

      iii. Entrez la commande suivante pour passer à la racine : `su -`

      iv. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier. Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

   b. Accédez au répertoire dans lequel se trouvent les journaux d'audit : `cd /var/local/audit/export/`

   c. Utilisez grep pour extraire les messages d'audit associés à l'objet dans un fichier de sortie. Entrez : `grep uuid-valueaudit_file_name > output_file_name`

      Par exemple :

      ```
      Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
      messages_about_restored_object.txt
      ```

   d. Utilisez grep pour extraire les messages d'audit règles objet met (ORLM) de ce fichier de sortie. Entrez : `grep ORLM output_file_name`

      Par exemple :

      ```
      Admin: # grep ORLM messages_about_restored_object.txt
      ```

      Un message d'audit ORLM ressemble à cet exemple de message.

```
[AUDT:[CBID(UI64):0x38186FE53E3C49A5][RULE(CSTR):"Make 2 Copies"]
[STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"926026C4-00A4-449B-AC72-
BCCA72DD1311"]
[LOCS(CSTR):"**CLDI 12828634 2148730112**, CLDI 12745543 2147552014"]
[RSLT(FC32):SUCS][AVER(UI32):10][ATYP(FC32):ORLM][ATIM(UI64):15633982306
69]
[ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID(FC32):BCMS]]
```

a. Recherchez le champ EMPLACEMENTS dans le message d'audit.

   Le cas échéant, la valeur de CLDI dans LES EMPLACEMENTS est l'ID de nœud et l'ID de volume sur lequel une copie d'objet a été créée. Ce message indique que la ILM a été appliquée et que deux copies d'objet ont été créées à deux emplacements dans la grille.

b. Réinitialisez le nombre d'objets perdus dans le Grid Manager.

Informations associées

"Analyse des objets perdus"

"Confirmation de l'emplacement des données d'objet"

"Réinitialisation du nombre d'objets perdus et manquants"

"Examiner les journaux d'audit"

Réinitialisation du nombre d'objets perdus et manquants

Après avoir examiné le système StorageGRID et vérifié que tous les objets perdus enregistrés sont définitivement perdus ou qu'il s'agit d'une fausse alarme, vous pouvez réinitialiser la valeur de l'attribut objets perdus sur zéro.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

Vous pouvez réinitialiser le compteur objets perdus à partir de l'une des pages suivantes :

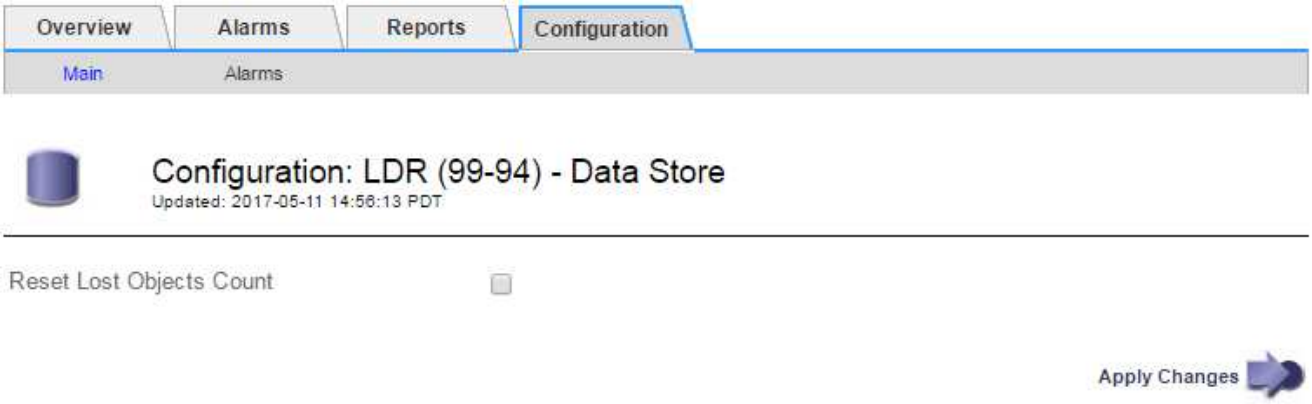
- **Support** > **Outils** > **topologie de grille** > ***site*** **>** ***nœud de stockage*** > **LDR** > **Data Store** > **Présentation** > **main**
- **Support** > **Outils** > **topologie de grille** > ***site*** **>** ***nœud de stockage*** > **DDS** > **Data Store** > **Présentation** > **main**

Ces instructions montrent la réinitialisation du compteur à partir de la page **LDR** > **Data Store**.

Étapes

1. Sélectionnez **support** > **Outils** > **topologie de grille**.
2. Sélectionnez ***site*** **>** ***nœud de stockage*** > **LDR** > **Data Store** > **Configuration** pour le nœud de stockage qui a l'alerte **objets perdus** ou L'alarme PERDUE.

3. Sélectionnez **Réinitialiser le nombre d'objets perdus**.



4. Cliquez sur **appliquer les modifications**.

   L'attribut objets perdus est réinitialisé à 0 et l'alerte **objets perdus** et l'effacement de l'alarme PERDUE, qui peut prendre quelques minutes.

5. Si vous le souhaitez, réinitialisez d'autres valeurs d'attribut associées qui auraient pu être incrémentées en cours d'identification de l'objet perdu.

   a. Sélectionnez ***site > nœud de stockage*** > **LDR** > **codage d'effacement** > **Configuration**.

   b. Sélectionnez **Réinitialiser les lectures nombre d'échecs** et **Réinitialiser les copies corrompues nombre d'échecs détectés**.

   c. Cliquez sur **appliquer les modifications**.

   d. Sélectionnez ***site > nœud de stockage*** > **LDR** > **Verification** > **Configuration**.

   e. Sélectionnez **Réinitialiser le nombre d'objets manquants** et **Réinitialiser le nombre d'objets corrompus**.

   f. Si vous êtes sûr que les objets en quarantaine ne sont pas nécessaires, vous pouvez sélectionner **Supprimer les objets en quarantaine**.

      Des objets mis en quarantaine sont créés lorsque la vérification en arrière-plan identifie une copie d'objet répliquée corrompue. Dans la plupart des cas, StorageGRID remplace automatiquement l'objet corrompu, et il est sûr de supprimer les objets mis en quarantaine. Cependant, si l'alerte **objets perdus** ou L'alarme PERDUE est déclenchée, le support technique peut vouloir accéder aux objets mis en quarantaine.

   g. Cliquez sur **appliquer les modifications**.

   La réinitialisation des attributs peut prendre quelques instants après avoir cliqué sur **appliquer les modifications**.

Informations associées

"Administrer StorageGRID"

Dépannage de l'alerte de stockage de données d'objet faible

L'alerte **mémoire de données d'objet faible** surveille la quantité d'espace disponible pour le stockage de données d'objet sur chaque nœud de stockage.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

Le **stockage de données d'objet faible** est déclenché lorsque la quantité totale de données d'objet répliquées et codées d'effacement sur un nœud de stockage correspond à l'une des conditions configurées dans la règle d'alerte.

Par défaut, une alerte majeure est déclenchée lorsque cette condition est évaluée comme vrai :

```
(storagegrid_storage_utilization_data_bytes/
(storagegrid_storage_utilization_data_bytes +
storagegrid_storage_utilization_usable_space_bytes)) >=0.90
```

Dans cette condition :

- `storagegrid_storage_utilization_data_bytes` Est une estimation de la taille totale des données d'objet répliquées et codées d'effacement pour un nœud de stockage.
- `storagegrid_storage_utilization_usable_space_bytes` Correspond à la quantité totale d'espace de stockage objet restant pour un nœud de stockage.

Si une alerte majeure ou mineure **stockage de données d'objet bas** est déclenchée, vous devez exécuter une procédure d'extension dès que possible.

Étapes

1. Sélectionnez **alertes** > **actuel**.

   La page alertes s'affiche.

2. Dans le tableau des alertes, développez le groupe d'alertes **stockage de données d'objet bas**, si nécessaire, et sélectionnez l'alerte que vous souhaitez afficher.

   Sélectionnez l'alerte, et non l'en-tête d'un groupe d'alertes.

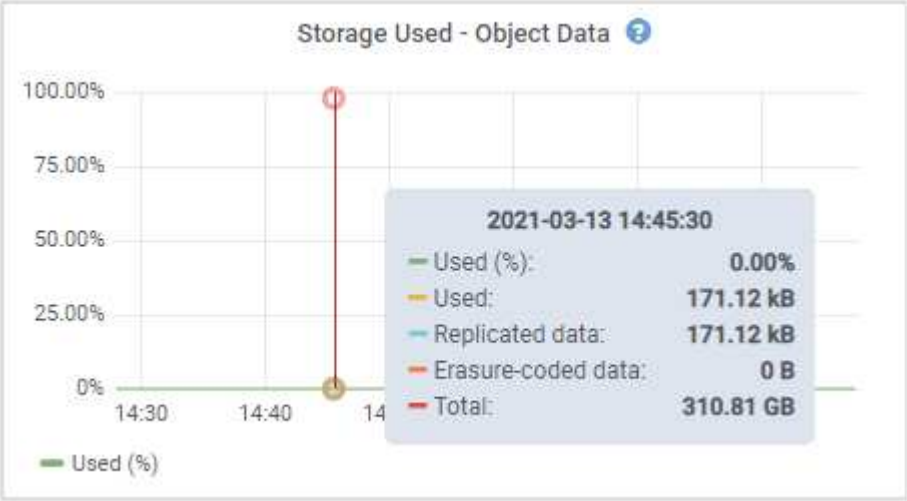
3. Vérifiez les détails dans la boîte de dialogue et notez ce qui suit :
   - Temps déclenché
   - Le nom du site et du noeud
   - Valeurs actuelles des mesures de cette alerte
4. Sélectionnez **Nodes** > ***Storage Node ou site*** > **Storage**.
5. Placez le curseur de la souris sur le graphique stockage utilisé - données d'objet.

   Les valeurs suivantes sont affichées :

   - **Utilisé (%)** : pourcentage de l'espace utilisable total qui a été utilisé pour les données d'objet.
   - **Used** : quantité de l'espace utilisable total qui a été utilisé pour les données d'objet.
   - **Données répliquées** : estimation de la quantité de données d'objet répliqué sur ce nœud, site ou

grille.

- **Données avec code d'effacement** : estimation de la quantité de données d'objet avec code d'effacement sur ce nœud, ce site ou ce grid.
- **Total** : la quantité totale d'espace utilisable sur ce nœud, site ou grille. La valeur utilisée est la `storagegrid_storage_utilization_data_bytes` métrique.



6. Sélectionnez les commandes de temps au-dessus du graphique pour afficher l'utilisation du stockage sur différentes périodes.

   Pour mieux comprendre la quantité de stockage utilisée auparavant et après le déclenchement de l'alerte, vous pouvez estimer le temps nécessaire pour que l'espace restant du nœud devienne complet.

7. Effectuez dès que possible une procédure d'extension pour ajouter de la capacité de stockage.

   Vous pouvez ajouter des volumes de stockage (LUN) à des nœuds de stockage existants ou ajouter de nouveaux nœuds de stockage.

   Pour gérer un nœud de stockage complet, reportez-vous aux instructions d'administration de StorageGRID.

Informations associées

"Dépannage de l'alarme Storage Status (SSTS)"

"Développez votre grille"

"Administrer StorageGRID"

Dépannage de l'alarme Storage Status (SSTS)

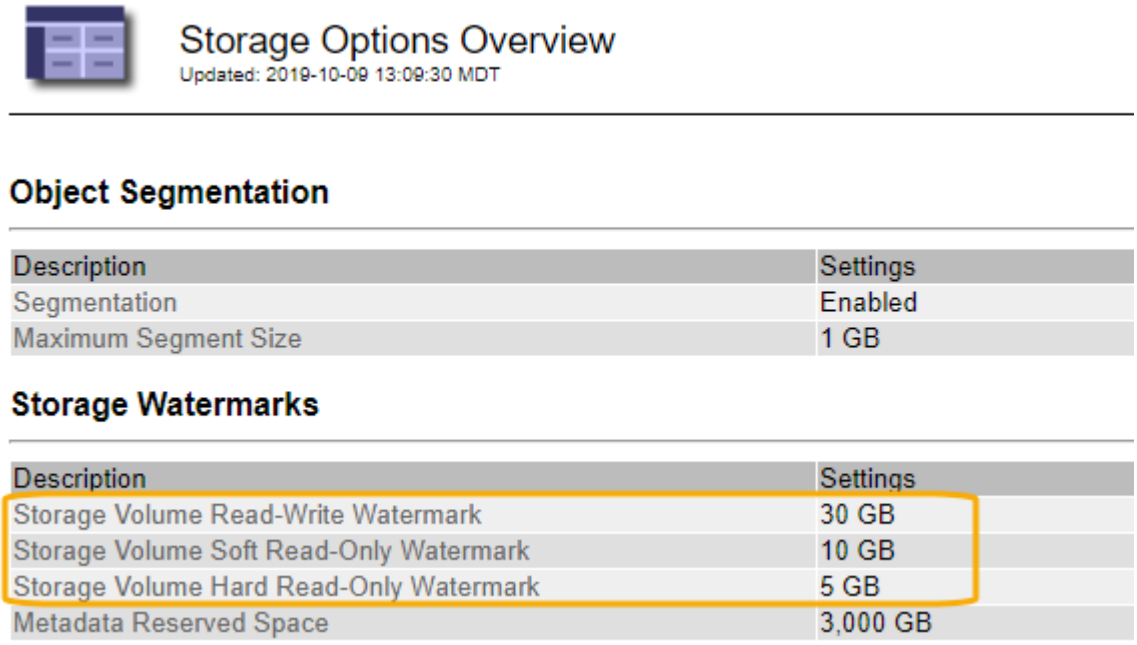
L'alarme Storage Status (SSTS) (État du stockage) est déclenchée si un nœud de stockage ne dispose pas d'espace disponible suffisant pour le stockage d'objets.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

L'alarme SSTS (État de stockage) est déclenchée au niveau des notifications lorsque la quantité d'espace libre sur chaque volume d'un nœud de stockage tombe en dessous de la valeur du filigrane du Storage Volume Soft Read Only (**Configuration Options de stockage Présentation**).



Storage Options Overview

Updated: 2019-10-09 13:09:30 MDT

Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark	30 GB
Storage Volume Soft Read-Only Watermark	10 GB
Storage Volume Hard Read-Only Watermark	5 GB
Metadata Reserved Space	3,000 GB

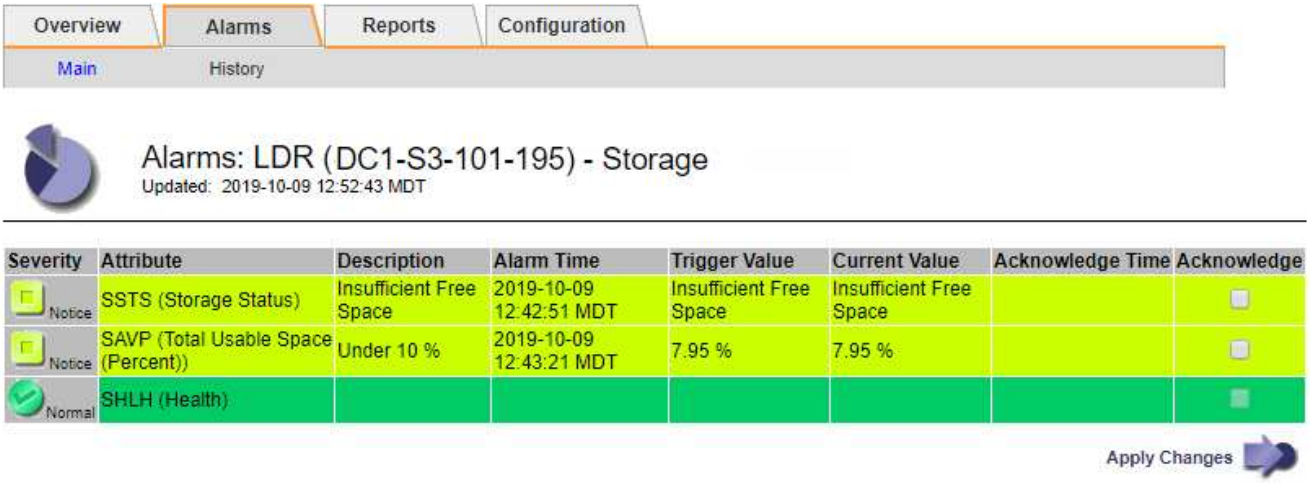
Par exemple, supposons que le filigrane de volume de stockage en lecture seule soit défini sur 10 Go, ce qui est sa valeur par défaut. L'alarme SSTS est déclenchée si moins de 10 Go d'espace utilisable reste sur chaque volume de stockage du nœud de stockage. Si l'un des volumes dispose d'au moins 10 Go d'espace disponible, l'alarme n'est pas déclenchée.

Si une alarme SSTS a été déclenchée, vous pouvez suivre ces étapes pour mieux comprendre le problème.

Étapes

1. Sélectionnez **support** > **alarmes (hérité)** > **alarmes actuelles**.
2. Dans la colonne Service, sélectionnez le centre de données, le nœud et le service associés à l'alarme SSTS.

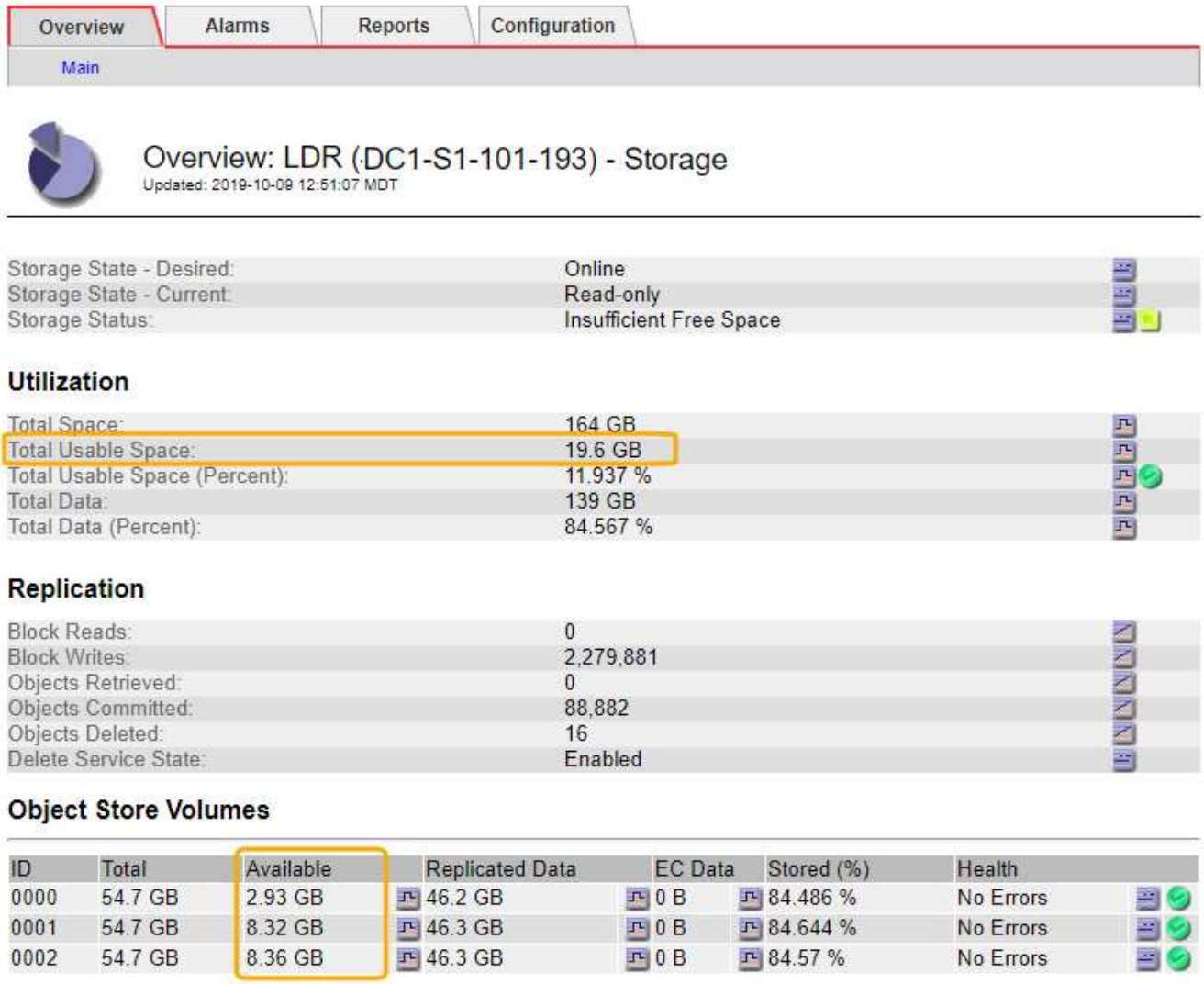
   La page topologie de la grille s'affiche. L'onglet alarmes affiche les alarmes actives pour le nœud et le service que vous avez sélectionnés.



Dans cet exemple, les alarmes SSTS (Storage Status) et SAVP (Total Usable Space (pourcentage)) ont été déclenchées au niveau Avis.

> En général, l'alarme SSTS et l'alarme SAVP sont déclenchées à peu près à la même heure ; cependant, si les deux alarmes sont déclenchées dépend du paramètre de filigrane en GB et du paramètre d'alarme SAVP en pourcentage.

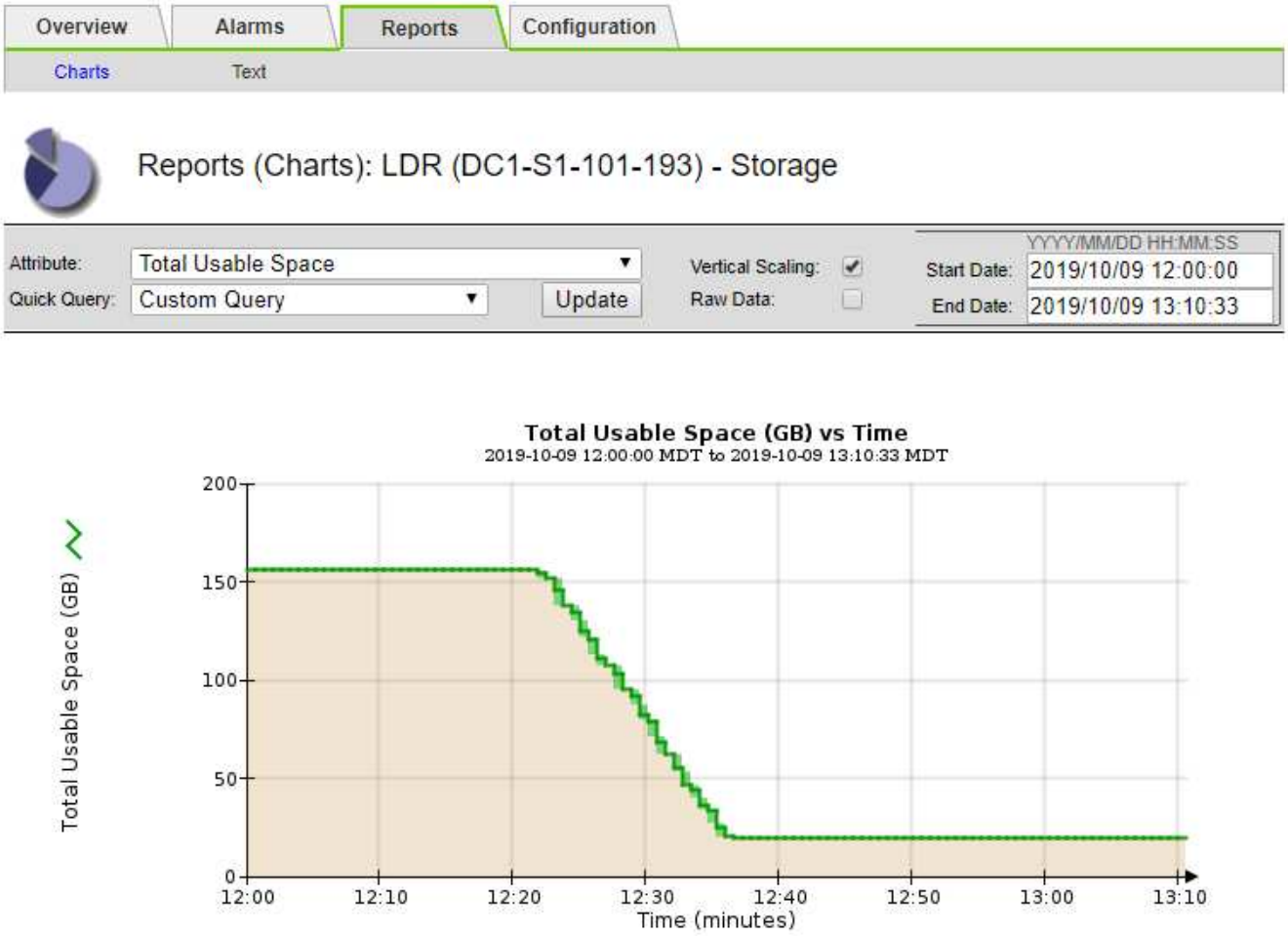
3. Pour déterminer la quantité d'espace utilisable réellement disponible, sélectionnez **LDR Storage Overview** et recherchez l'attribut Total Usable (STAS).



Dans cet exemple, seuls 19.6 Go d'espace de 164 Go sur ce nœud de stockage restent disponibles. Notez que la valeur totale est la somme des valeurs **disponibles** pour les trois volumes du magasin d'objets. L'alarme SSTS a été déclenchée car chacun des trois volumes de stockage avait moins de 10 Go d'espace disponible.

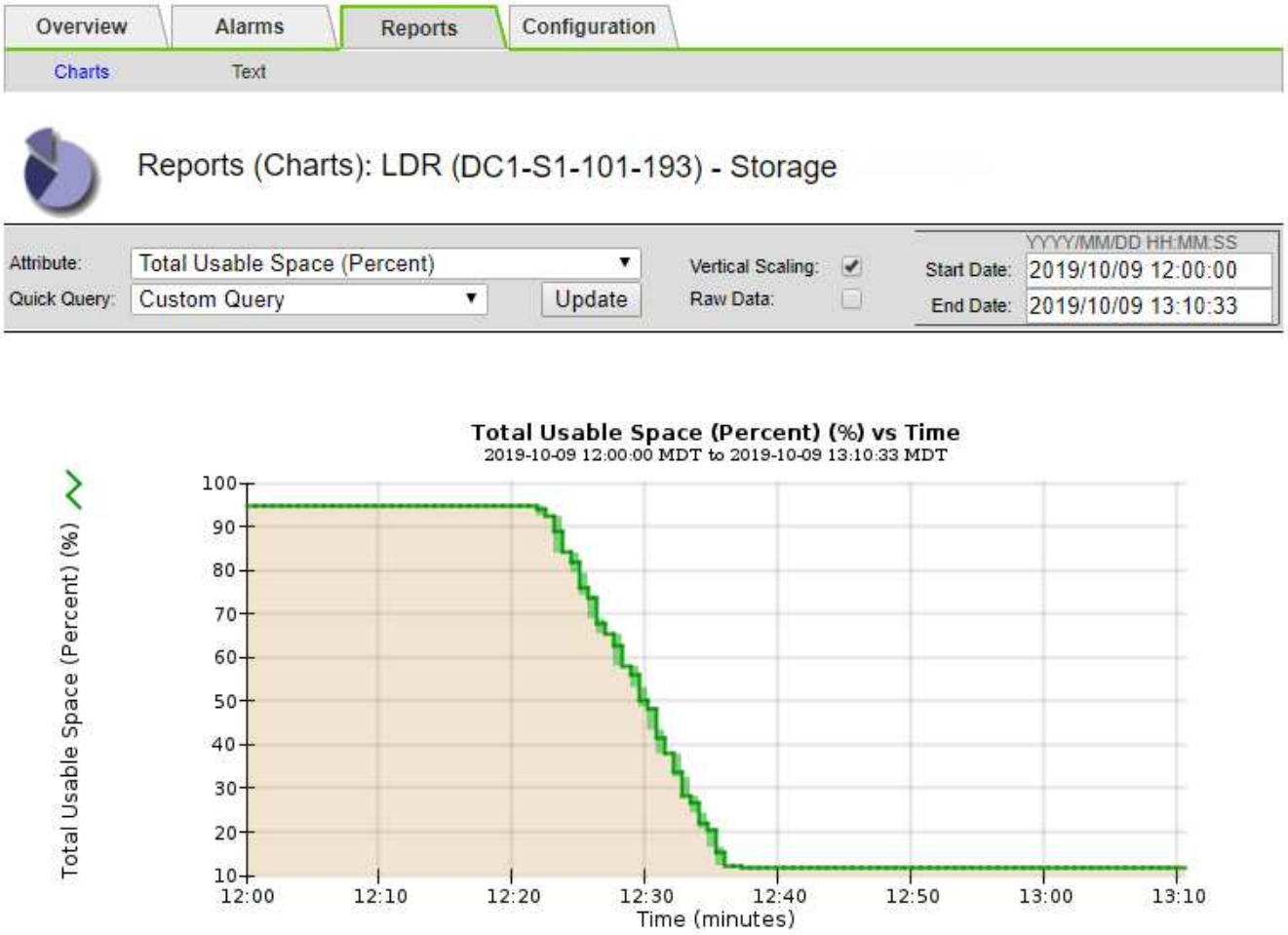
4. Pour comprendre comment le stockage a été utilisé au fil du temps, sélectionnez l'onglet **Rapports** et tracez l'espace utilisable total au cours des dernières heures.

   Dans cet exemple, l'espace utilisable total est passé d'environ 155 Go à 12:00 à 20 Go à 12:35, ce qui correspond à l'heure à laquelle l'alarme SSTS a été déclenchée.



5. Pour comprendre comment le stockage est utilisé en pourcentage du total, tracez l'espace utilisable total (pourcentage) au cours des dernières heures.

   Dans cet exemple, l'espace utilisable total a chuté de 95 % à un peu plus de 10 % environ au même moment.



6. Selon les besoins, ajoutez de la capacité de stockage en étendant le système StorageGRID.

   Pour connaître les procédures de gestion d'un nœud de stockage complet, reportez-vous aux instructions d'administration de StorageGRID.

Informations associées

"Développez votre grille"

"Administrer StorageGRID"

Résolution des problèmes de transmission des messages des services de plate-forme (alarme SMTT)

L'alarme Total Events (SMTT) est déclenchée dans Grid Manager si un message de service de plate-forme est envoyé à une destination qui ne peut pas accepter les données.

Description de la tâche

Par exemple, un téléchargement partitionné S3 peut réussir même si le message de réplication ou de notification associé ne peut pas être transmis au noeud final configuré. Ou bien, un message pour la réplication CloudMirror peut ne pas être livré si les métadonnées sont trop longues.

L'alarme SMTT contient un message du dernier événement qui indique : `Failed to publish notifications for` *`bucket-name object key`* pour le dernier objet dont la notification a échoué.

Pour plus d'informations sur le dépannage des services de plate-forme, reportez-vous aux instructions d'administration de StorageGRID. Vous devrez peut-être accéder au locataire à partir du gestionnaire des locataires pour déboguer une erreur du service de plateforme.

Étapes

1. Pour afficher l'alarme, sélectionnez **noeuds *site grid node* Events**.
2. Afficher le dernier événement en haut du tableau.

   Les messages d'événement sont également répertoriés dans le `/var/local/log/bycast-err.log`.

3. Suivez les instructions fournies dans le contenu de l'alarme SMTT pour corriger le problème.
4. Cliquez sur **Réinitialiser le nombre d'événements**.
5. Notifier le locataire des objets dont les messages de services de plate-forme n'ont pas été livrés.
6. Demandez au locataire de déclencher l'échec de la réplication ou de la notification en mettant à jour les métadonnées ou balises de l'objet.

Informations associées

"Administrer StorageGRID"

"Utilisez un compte de locataire"

"Référence des fichiers journaux"

"Réinitialisation du nombre d'événements"

Résolution des problèmes de métadonnées

Vous pouvez effectuer plusieurs tâches pour déterminer la source des problèmes de métadonnées.

Dépannage de l'alerte de stockage de métadonnées faible

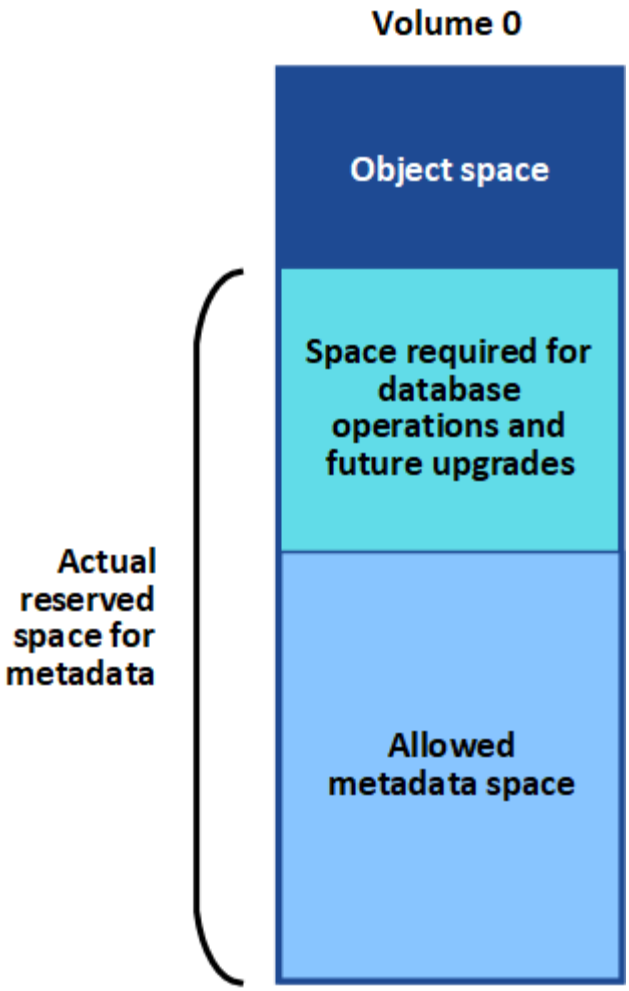
Si l'alerte **stockage de métadonnées faible** est déclenchée, vous devez ajouter de nouveaux nœuds de stockage.

Ce dont vous avez besoin

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

Description de la tâche

StorageGRID réserve un certain espace sur le volume 0 de chaque nœud de stockage pour les métadonnées de l'objet. Cet espace est appelé espace réservé réel, et il est divisé en l'espace autorisé pour les métadonnées d'objet (espace de métadonnées autorisé) et l'espace requis pour les opérations essentielles de base de données, telles que la compaction et la réparation. L'espace de métadonnées autorisé régit la capacité globale des objets.



Si la quantité d'espace autorisée pour les métadonnées est supérieure à 100 %, les opérations de la base de données ne peuvent pas fonctionner efficacement et des erreurs surviennent.

StorageGRID utilise la métrique Prometheus suivante pour mesurer la totalité 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 **stockage de métadonnées faible** est déclenchée.

- **Mineure** : les métadonnées d'objet utilisent au moins 70 % de l'espace autorisé pour les métadonnées. Vous devez ajouter des nœuds de stockage dès que possible.
- **Majeur** : les métadonnées d'objet utilisent au moins 90 % de l'espace autorisé pour les métadonnées. Vous devez immédiatement ajouter de nouveaux nœuds de stockage.

> Lorsque les métadonnées de l'objet utilisent au moins 90 % de l'espace de métadonnées autorisé, un avertissement s'affiche dans le Tableau de bord. Si cet avertissement s'affiche, vous devez immédiatement ajouter de nouveaux nœuds de stockage. Vous ne devez jamais autoriser les métadonnées objet à utiliser plus de 100 % de l'espace autorisé.

- **Critique** : les métadonnées d'objet utilisent au moins 100 % de l'espace de métadonnées autorisé et commencent à consommer l'espace requis pour les opérations essentielles de la base de données. Vous devez arrêter l'ingestion des nouveaux objets et vous devez immédiatement ajouter de nouveaux nœuds de stockage.

Dans l'exemple suivant, les métadonnées d'objet utilisent plus de 100 % de l'espace autorisé pour les métadonnées. Cette situation est critique, ce qui entraîne un fonctionnement inefficace de la base de données et des erreurs.

The following Storage Nodes are using more than 90% of the space allowed for object metadata:

Node	% Used	Used	Allowed
DC1-S2-227	104.51%	6.73 GB	6.44 GB
DC1-S3-228	104.36%	6.72 GB	6.44 GB
DC2-S2-233	104.20%	6.71 GB	6.44 GB
DC1-S1-226	104.20%	6.71 GB	6.44 GB
DC2-S3-234	103.43%	6.66 GB	6.44 GB

Undesirable results can occur if object metadata uses more than 100% of the allowed space. You must add new Storage Nodes immediately or contact support.

Si la taille du volume 0 est inférieure à celle de l'option de stockage de l'espace réservé aux métadonnées (par exemple, dans un environnement non productif), le calcul de l'alerte **stockage de métadonnées faible** peut être inexact.

Étapes

1. Sélectionnez **alertes** > **actuel**.
2. Dans le tableau des alertes, développez le groupe d'alertes **stockage de métadonnées faible**, si nécessaire, et sélectionnez l'alerte spécifique que vous souhaitez afficher.
3. Vérifiez les détails dans la boîte de dialogue d'alerte.
4. Si une alerte majeure ou critique **stockage de métadonnées faible** a été déclenchée, effectuez immédiatement une extension pour ajouter des nœuds de stockage.

Dans la mesure où StorageGRID conserve des copies complètes de toutes les métadonnées d'objet sur chaque site, la capacité de métadonnées de l'ensemble de la grille est limitée par la capacité des métadonnées du site le plus petit. Si vous devez ajouter de la capacité des métadonnées à un site, vous devez également étendre tous les autres sites jusqu'au même nombre de nœuds de stockage.

Une fois l'extension effectuée, StorageGRID redistribue les métadonnées de l'objet existantes vers les nouveaux nœuds, qui augmentent la capacité globale des métadonnées de la grille. Aucune action de l'utilisateur n'est requise. L'alerte **stockage de métadonnées faible** est effacée.

Informations associées

"Surveillance de la capacité des métadonnées d'objet pour chaque nœud de stockage"

"Développez votre grille"

Dépannage de l'alarme Services : état - Cassandra (SVST)

L'alarme Services : Status - Cassandra (SVST) indique que vous devrez peut-être reconstruire la base de données Cassandra pour un nœud de stockage. Cassandra est utilisée comme magasin de métadonnées pour StorageGRID.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.
- Vous devez avoir le `Passwords.txt` fichier.

Description de la tâche

Si Cassandra est arrêtée pendant plus de 15 jours (par exemple, le nœud de stockage est mis hors tension), Cassandra ne démarre pas lorsque le nœud est remis en ligne. Vous devez reconstruire la base de données Cassandra pour le service DDS affecté.

Vous pouvez utiliser la page Diagnostics pour obtenir des informations supplémentaires sur l'état actuel de votre grille.

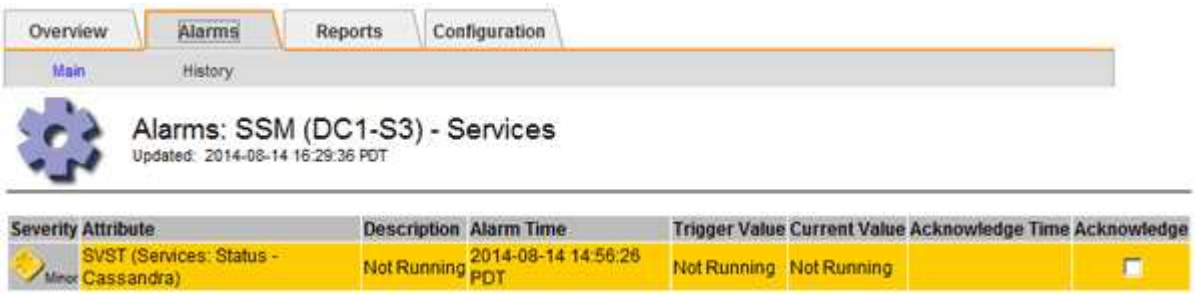
"Exécution des diagnostics"

> Si au moins deux des services de base de données Cassandra sont en panne pendant plus de 15 jours, contactez le support technique et ne suivez pas les étapes ci-dessous.

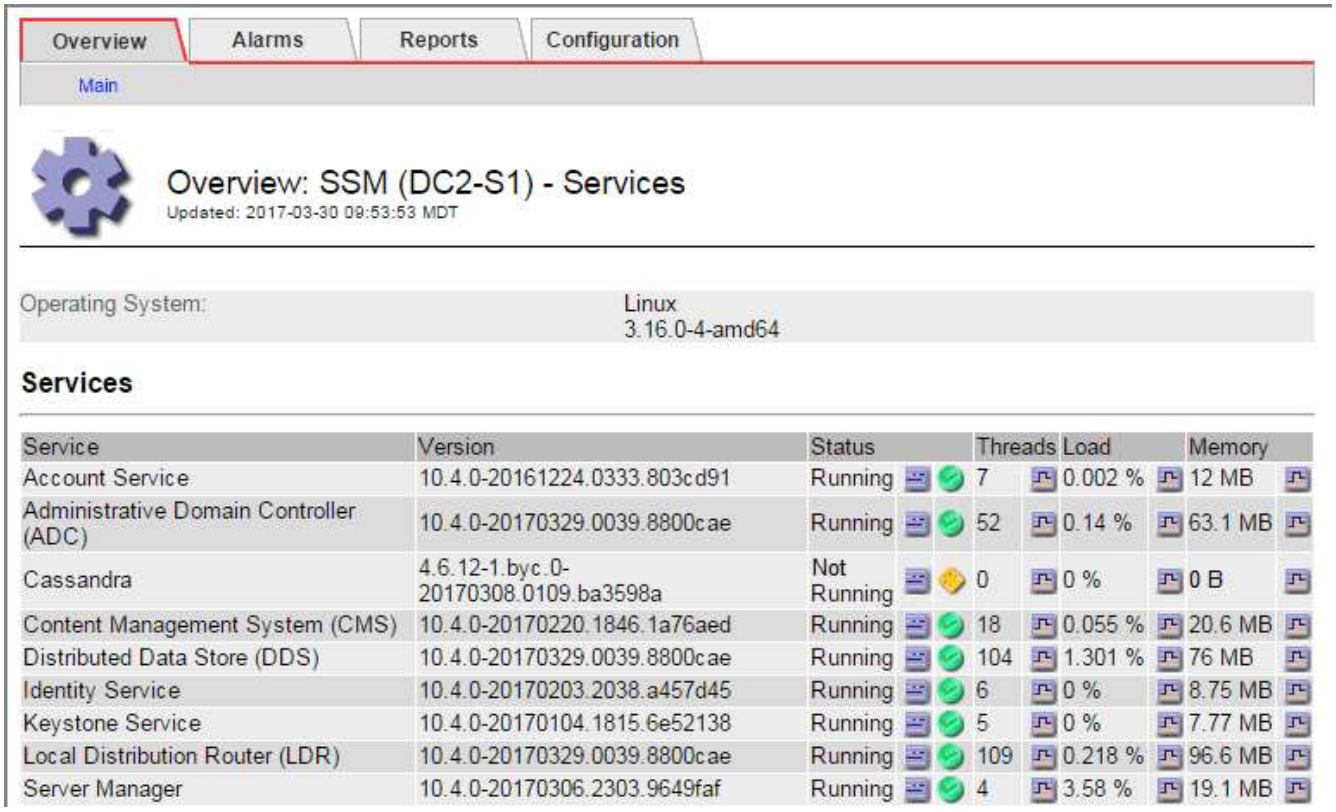
Étapes

1. Sélectionnez **support** > **Outils** > **topologie de grille**.
2. Sélectionnez ***site* > *nœud de stockage*** > **SSM** > **Services** > **alarmes** > **main** pour afficher les alarmes.

   Cet exemple montre que l'alarme SVST a été déclenchée.



   La page principale des services SSM indique également que Cassandra n'est pas en cours d'exécution.



1. Essayez de redémarrer Cassandra depuis le nœud de stockage :
   a. Connectez-vous au nœud grid :
      i. Saisissez la commande suivante : `ssh admin@grid_node_IP`
      ii. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
      iii. Entrez la commande suivante pour passer à la racine : `su -`
      iv. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier. Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.
   b. Entrez : `/etc/init.d/cassandra status`
   c. Si Cassandra n'est pas en cours d'exécution, redémarrez-le : `/etc/init.d/cassandra restart`
2. Si Cassandra ne redémarre pas, déterminez la durée de sa panne. Si Cassandra a été indisponible pendant plus de 15 jours, il vous faut reconstruire la base de données Cassandra.

   Si deux services de base de données Cassandra ou plus sont en panne, contactez le support technique et ne procédez pas aux étapes ci-dessous.

   Vous pouvez déterminer la durée d'interruption de Cassandra en la transcritant ou en consultant le fichier servermanager.log.

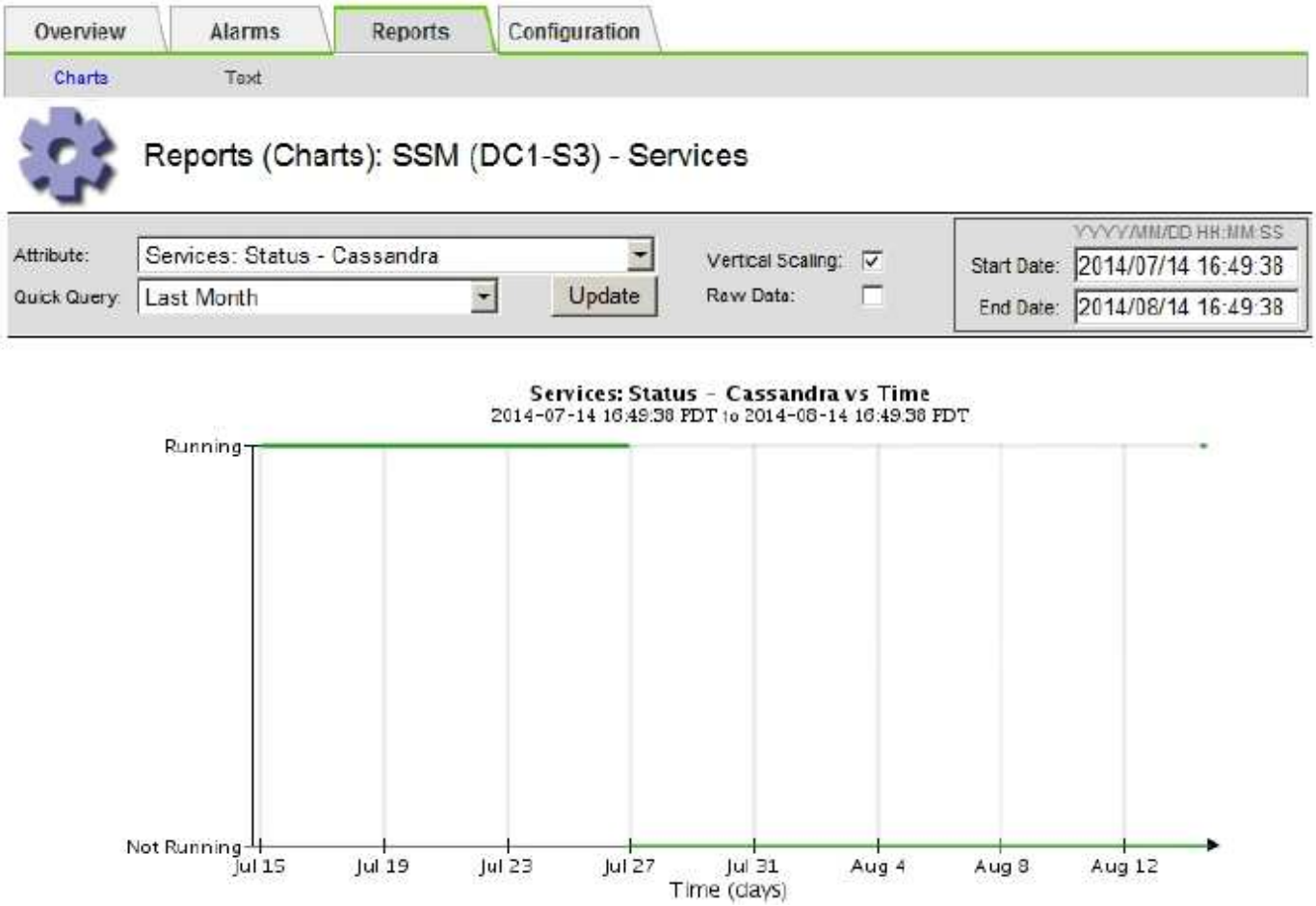
3. Pour le tableau Cassandra :
   a. Sélectionnez **support** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***site*** > ***Storage Node*** > **SSM** > **Services** > **Rapports** > **diagrammes**.
   b. Sélectionnez **attribut** > **Service : état - Cassandra**.
   c. Pour **Date de début**, entrez une date qui est au moins 16 jours avant la date du jour. Pour **Date de fin**,

saisissez la date actuelle.

d. Cliquez sur **mettre à jour**.

e. Si Cassandra est indisponible durant plus de 15 jours, reconstruisez la base de données Cassandra.

L'exemple de tableau suivant montre que Cassandra a été indisponible pendant au moins 17 jours.



1. Pour consulter le fichier servermanager.log sur le nœud de stockage :

   a. Connectez-vous au nœud grid :

      i. Saisissez la commande suivante : `ssh admin@grid_node_IP`

      ii. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

      iii. Entrez la commande suivante pour passer à la racine : `su -`

      iv. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier. Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

   b. Entrez : `cat /var/local/log/servermanager.log`

      Le contenu du fichier servermanager.log s'affiche.

      Si Cassandra a été indisponible pendant plus de 15 jours, le message suivant s'affiche dans le fichier servermanager.log :

```
"2014-08-14 21:01:35 +0000 | cassandra | cassandra not
started because it has been offline for longer than
its 15 day grace period - rebuild cassandra
```

a. Assurez-vous que l'horodatage de ce message correspond à l'heure à laquelle vous avez tenté de redémarrer Cassandra, comme indiqué à l'étape Redémarrez Cassandra à partir du nœud de stockage.

   Il peut y avoir plusieurs entrées pour Cassandra ; vous devez trouver l'entrée la plus récente.

b. Si Cassandra a été indisponible pendant plus de 15 jours, il vous faut reconstruire la base de données Cassandra.

   Pour obtenir des instructions, reportez-vous à la section « récupération à partir d'un seul nœud de stockage en panne pendant plus de 15 jours » dans les instructions de restauration et de maintenance.

c. Contactez le support technique si les alarmes ne sont pas claires après la reconstruction de Cassandra.

Informations associées

"Maintenance et récupération"

Dépannage des erreurs de mémoire Cassandra (alarme SMTT)

Une alarme Total Events (SMTT) est déclenchée lorsque la base de données Cassandra a une erreur de mémoire insuffisante. Si cette erreur se produit, contactez le support technique pour résoudre le problème.

Description de la tâche

Si une erreur de mémoire insuffisante se produit pour la base de données Cassandra, un vidage de mémoire est créé, une alarme Total Events (SMTT) est déclenchée et le nombre d'erreurs de mémoire de Cassandra est incrémenté d'un.

Étapes

1. Pour afficher l'événement, sélectionnez **noeuds** > ***grid node*** > **Events**.
2. Vérifiez que le nombre d'erreurs de mémoire du tas Cassandra est égal ou supérieur à 1.

   Vous pouvez utiliser la page Diagnostics pour obtenir des informations supplémentaires sur l'état actuel de votre grille.

   "Exécution des diagnostics"

3. Accédez à `/var/local/core/`, comprimer le `Cassandra.hprof` dossier et envoyez-le au support technique.
4. Faire une sauvegarde du `Cassandra.hprof` et supprimez-le de la `/var/local/core/ directory`.

   Ce fichier peut contenir jusqu'à 24 Go. Vous devez donc le supprimer pour libérer de l'espace.

5. Une fois le problème résolu, cliquez sur **Réinitialiser le nombre d'événements**.

Pour réinitialiser le nombre d'événements, vous devez disposer de l'autorisation Configuration de la page de topologie de la grille.

Informations associées

"Réinitialisation du nombre d'événements"

Dépannage des 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 Swift ou d'un outil de surveillance externe, vérifiez le certificat.

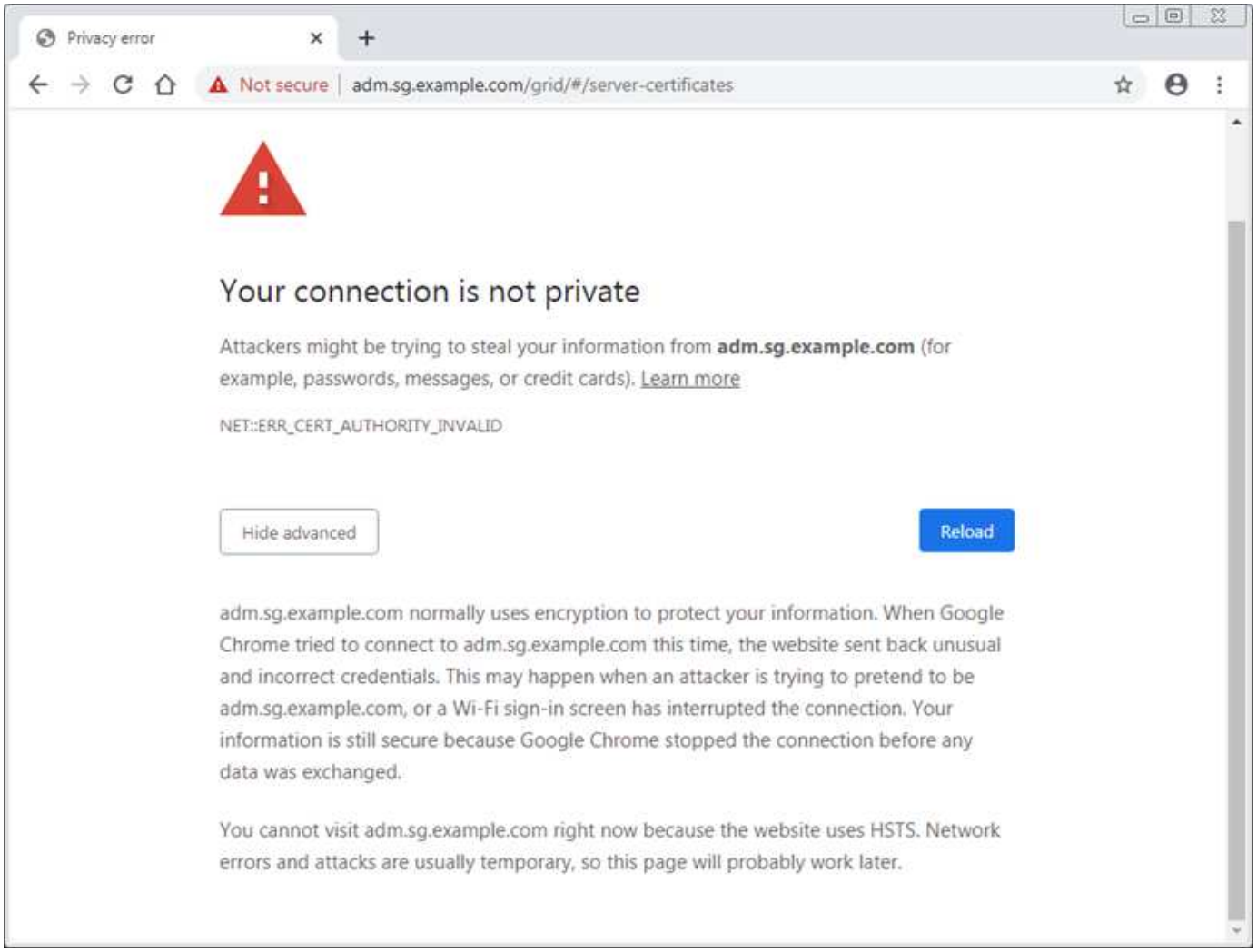
Description de la tâche

Les erreurs de certificat peuvent entraîner des problèmes lors de votre tentative de connexion à StorageGRID à l'aide de Grid Manager, de l'API de gestion du grid, du gestionnaire de locataires ou de l'API de gestion des locataires. Des erreurs liées au certificat peuvent également se produire lorsque vous tentez de vous connecter à un client S3 ou Swift ou à un outil de surveillance externe.

Si vous accédez à Grid Manager ou au Gestionnaire de locataires à l'aide d'un nom de domaine au lieu d'une adresse IP, le navigateur affiche une erreur de certificat sans option de contournement si l'un des cas suivants se produit :

- Votre certificat de serveur de l'interface de gestion personnalisée expire.
- Vous restaurez un certificat de serveur d'interface de gestion personnalisée vers le certificat de serveur par défaut.

L'exemple suivant montre une erreur de certificat lorsque le certificat du serveur de l'interface de gestion personnalisée a expiré :



Pour garantir que les opérations ne sont pas interrompues par un certificat de serveur ayant échoué, l'alerte **expiration du certificat de serveur pour l'interface de gestion** est déclenchée lorsque le certificat de serveur est sur le point d'expirer.

Lorsque vous utilisez des certificats client pour l'intégration avec Prometheus externe, les erreurs de certificat peuvent être dues au certificat du serveur de l'interface de gestion StorageGRID ou aux certificats client. L'alerte **expiration des certificats configurés sur la page des certificats client** est déclenchée lorsqu'un certificat client arrive à expiration.

Étapes

1. Si vous avez reçu une notification d'alerte concernant un certificat expiré, accédez aux détails du certificat :
   - Pour un certificat de serveur, sélectionnez **Configuration Paramètres réseau certificats de serveur**.
   - Pour un certificat client, sélectionnez **Configuration contrôle d'accès certificats client**.
2. Vérifiez la période de validité du certificat.

   Certains navigateurs Web et clients S3 ou Swift n'acceptent pas les certificats ayant une période de validité supérieure à 398 jours.

3. Si le certificat a expiré ou expire bientôt, téléchargez ou générez un nouveau certificat.
   - Pour un certificat de serveur, reportez-vous aux étapes de configuration d'un certificat de serveur personnalisé pour le gestionnaire de grille et le gestionnaire de locataires dans les instructions

d'administration de StorageGRID.

- Pour un certificat client, reportez-vous aux étapes de configuration d'un certificat client dans les instructions d'administration de StorageGRID.

4. Pour les erreurs de certificat de serveur, essayez l'une des options suivantes ou les deux :
   - Assurez-vous que le nom d'alternative de l'objet (SAN) du certificat est renseigné et que le SAN correspond à l'adresse IP ou au nom d'hôte du nœud auquel vous vous connectez.
   - Si vous tentez de vous connecter à StorageGRID à l'aide d'un nom de domaine :
     i. Entrez l'adresse IP du noeud d'administration au lieu du nom de domaine pour contourner l'erreur de connexion et accéder à Grid Manager.
     ii. Dans Grid Manager, sélectionnez **Configuration Paramètres réseau certificats de serveur** pour installer un nouveau certificat personnalisé ou poursuivre avec le certificat par défaut.
     iii. Dans les instructions d'administration de StorageGRID, reportez-vous aux étapes de configuration d'un certificat de serveur personnalisé pour le gestionnaire de grille et le gestionnaire de locataires.

Informations associées

"Administrer StorageGRID"

Résolution des problèmes liés au nœud d'administration et à l'interface utilisateur

Plusieurs tâches sont à effectuer pour déterminer la source des problèmes liés aux nœuds d'administration et à l'interface utilisateur de StorageGRID.

Dépannage des erreurs de connexion

Si une erreur s'est produite lors de la connexion à un nœud d'administration StorageGRID, la configuration de la fédération des identités, un problème de réseau ou de matériel, un problème avec les services du nœud d'administration ou un problème avec la base de données Cassandra sur les nœuds de stockage connectés.

Ce dont vous avez besoin

- Vous devez avoir le `Passwords.txt` fichier.
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

Suivez ces instructions de dépannage si vous voyez l'un des messages d'erreur suivants lorsque vous tentez de vous connecter à un noeud d'administration :

- `Your credentials for this account were invalid. Please try again.`
- `Waiting for services to start…`
- `Internal server error. The server encountered an error and could not complete your request. Please try again. If the problem persists, contact Technical Support.`
- `Unable to communicate with server. Reloading page…`

Étapes

1. Attendez 10 minutes et essayez à nouveau de vous connecter.

   Si l'erreur n'est pas résolue automatiquement, passez à l'étape suivante.

2. Si votre système StorageGRID comporte plusieurs nœuds d'administration, essayez de vous connecter à Grid Manager à partir d'un autre nœud d'administration.
   - Si vous pouvez vous connecter, vous pouvez utiliser les options **Dashboard**, **Nodes**, **Alerts** et **support** pour déterminer la cause de l'erreur.
   - Si vous ne disposez que d'un seul nœud d'administration ou que vous ne pouvez toujours pas vous connecter, passez à l'étape suivante.
3. Déterminez si le matériel du nœud est hors ligne.
4. Si l'authentification unique (SSO) est activée sur votre système StorageGRID, reportez-vous aux étapes de configuration de l'authentification unique dans les instructions d'administration de StorageGRID.

   Pour résoudre ces problèmes, il peut être nécessaire de désactiver et de réactiver temporairement l'authentification SSO pour un nœud d'administration unique.

   > Si SSO est activé, vous ne pouvez pas vous connecter à l'aide d'un port restreint. Vous devez utiliser le port 443.

5. Déterminez si le compte que vous utilisez appartient à un utilisateur fédéré.

   Si le compte d'utilisateur fédéré ne fonctionne pas, essayez de vous connecter à Grid Manager en tant qu'utilisateur local, tel que root.

   - Si l'utilisateur local peut se connecter :
     i. Examinez toutes les alarmes affichées.
     ii. Sélectionnez **Configuration** > **Fédération d'identités**.
     iii. Cliquez sur **Tester la connexion** pour valider vos paramètres de connexion pour le serveur LDAP.
     iv. Si le test échoue, corrigez toute erreur de configuration.
   - Si l'utilisateur local ne peut pas se connecter et que vous êtes sûr que les informations d'identification sont correctes, passez à l'étape suivante.
6. Utilisez SSH (Secure Shell) pour vous connecter au nœud d'administration :
   a. Saisissez la commande suivante : `ssh admin@Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

      Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

7. Afficher l'état de tous les services s'exécutant sur le nœud grid : `storagegrid-status`

   Assurez-vous que les services nms, mi, nginx et api de gestion sont tous en cours d'exécution.

   La sortie est immédiatement mise à jour si l'état d'un service change.

```
$ storagegrid-status
Host Name                      99-211
IP Address                     10.96.99.211
Operating System Kernel        4.19.0          Verified
Operating System Environment   Debian 10.1     Verified
StorageGRID Webscale Release   11.4.0          Verified
Networking                                     Verified
Storage Subsystem                              Verified
Database Engine                5.5.9999+default Running
Network Monitoring             11.4.0          Running
Time Synchronization           1:4.2.8p10+dfsg Running
ams                            11.4.0          Running
cmn                            11.4.0          Running
nms                            11.4.0          Running
ssm                            11.4.0          Running
mi                             11.4.0          Running
dynip                          11.4.0          Running
nginx                          1.10.3          Running
tomcat                         9.0.27          Running
grafana                        6.4.3           Running
mgmt api                       11.4.0          Running
prometheus                     11.4.0          Running
persistence                    11.4.0          Running
ade exporter                   11.4.0          Running
alertmanager                   11.4.0          Running
attrDownPurge                  11.4.0          Running
attrDownSamp1                  11.4.0          Running
attrDownSamp2                  11.4.0          Running
node exporter                  0.17.0+ds       Running
sg snmp agent                  11.4.0          Running
```

8. Vérifiez que le serveur Web Apache est en cours d'exécution : `# service apache2 status`

1. Utilisez Lumberjack pour récupérer les journaux : `# /usr/local/sbin/lumberjack.rb`

   Si l'authentification a échoué par le passé, vous pouvez utiliser les options de script --start et --end Lumberjack pour spécifier la plage horaire appropriée. Utilisez lumberjack -h pour plus de détails sur ces options.

   La sortie vers le terminal indique l'emplacement où l'archive de journal a été copiée.

1. Consultez les journaux suivants :
   - `/var/local/log/bycast.log`
   - `/var/local/log/bycast-err.log`
   - `/var/local/log/nms.log`

- `**/*commands.txt`

2. Si vous n'avez pas pu identifier de problèmes avec le nœud d'administration, exécutez l'une ou l'autre des commandes suivantes pour déterminer les adresses IP des trois nœuds de stockage exécutant le service ADC sur votre site. Il s'agit généralement des trois premiers nœuds de stockage installés sur le site.

```
# cat /etc/hosts
```

```
# vi /var/local/gpt-data/specs/grid.xml
```

Les nœuds Admin utilisent le service ADC pendant le processus d'authentification.

3. À partir du nœud d'administration, connectez-vous à chacun des nœuds de stockage ADC en utilisant les adresses IP que vous avez identifiées.
   a. Saisissez la commande suivante : `ssh admin@grid_node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

4. Afficher l'état de tous les services s'exécutant sur le nœud grid : `storagegrid-status`

   Assurez-vous que tous les services idnt, acct, nginx et cassandra fonctionnent.

5. Répéter les étapes Utilisez Lumberjack pour récupérer les journaux et Journaux de révision Pour consulter les journaux sur les nœuds de stockage.
6. Si vous ne parvenez pas à résoudre le problème, contactez le support technique.

   Fournissez les journaux que vous avez collectés au support technique.

Informations associées

"Administrer StorageGRID"

"Référence des fichiers journaux"

Résolution des problèmes liés à l'interface utilisateur

Après la mise à niveau vers une nouvelle version du logiciel StorageGRID, des problèmes peuvent s'afficher avec le gestionnaire Grid ou le gestionnaire de locataires.

L'interface Web ne répond pas comme prévu

Le gestionnaire de grid ou le gestionnaire de locataires peut ne pas répondre comme prévu après la mise à niveau du logiciel StorageGRID.

Si vous rencontrez des problèmes avec l'interface Web :

- Vérifiez que vous utilisez un navigateur pris en charge.

  > La prise en charge du navigateur a changé pour StorageGRID 11.5. Vérifiez que vous utilisez une version prise en charge.

- Effacez le cache de votre navigateur Web.

  L'effacement du cache supprime les ressources obsolètes utilisées par la version précédente du logiciel StorageGRID et permet à l'interface utilisateur de fonctionner de nouveau correctement. Pour obtenir des instructions, reportez-vous à la documentation de votre navigateur Web.

Informations associées

"Navigateurs Web pris en charge"

"Administrer StorageGRID"

Vérification de l'état d'un nœud d'administration non disponible

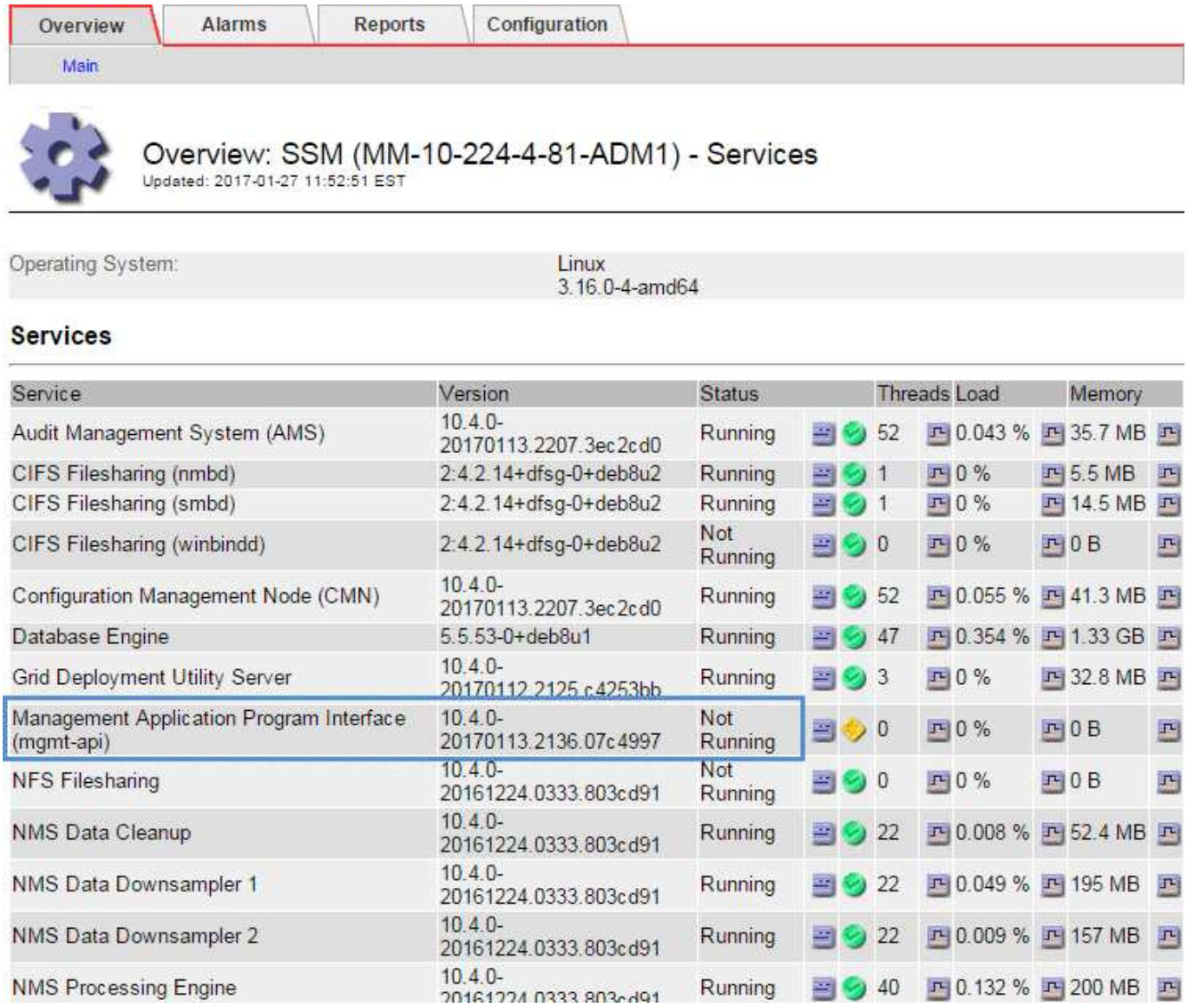
Si le système StorageGRID inclut plusieurs nœuds d'administration, vous pouvez utiliser un autre nœud d'administration pour vérifier l'état d'un nœud d'administration non disponible.

Ce dont vous avez besoin

Vous devez disposer d'autorisations d'accès spécifiques.

Étapes

1. Depuis un noeud d'administration disponible, connectez-vous à Grid Manager à l'aide d'un navigateur pris en charge.
2. Sélectionnez **support** > **Outils** > **topologie de grille**.
3. Sélectionnez ***site*** **> noeud d'administration non disponible** > **SSM** > **Services** > **Présentation** > **main**.
4. Recherchez les services dont l'état n'est pas en cours d'exécution et qui peuvent également s'afficher en bleu.



5. Déterminez si des alarmes ont été déclenchées.
6. Prenez les mesures appropriées pour résoudre le problème.

Informations associées

"Administrer StorageGRID"

Résolution des problèmes de réseau, de matériel et de plate-forme

Vous pouvez effectuer plusieurs tâches pour déterminer la source des problèmes liés au réseau, au matériel et à la plateforme StorageGRID.

Dépannage des erreurs « 422: Entité impossible à traiter »

L'erreur 422 : entité impossible à traiter peut se produire dans un certain nombre de circonstances. Consultez le message d'erreur pour déterminer la cause de votre problème.

Si l'un des messages d'erreur répertoriés s'affiche, effectuez l'action recommandée.

Message d'erreur	Cause première et action corrective

`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 se produire si vous sélectionnez l'option **ne pas utiliser TLS** pour transport Layer Security (TLS) lors de la configuration de la fédération d'identités à l'aide de Windows Active Directory (AD).
	
	L'utilisation de l'option **ne pas utiliser TLS** n'est pas prise en charge pour les serveurs AD qui appliquent la signature LDAP. Vous devez sélectionner l'option **Use STARTTLS** ou l'option **use LDAPS** pour TLS.

`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) entre StorageGRID et un système externe utilisé pour identifier la fédération ou les pools de stockage dans le 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.

Informations associées

"Administrer StorageGRID"

Dépannage de l'alerte de non-concordance de MTU du réseau Grid

L'alerte **Grid Network MTU mismatch** est déclenchée lorsque le paramètre MTU (maximum transmission Unit) de l'interface réseau Grid (eth0) diffère considérablement sur les nœuds de la grille.

Description de la tâche

Les différences dans les paramètres MTU peuvent indiquer que certains réseaux eth0, mais pas tous, sont

configurés pour les trames jumbo. Une différence de taille de MTU supérieure à 1000 peut entraîner des problèmes de performances du réseau.

Étapes

1. Répertorie les paramètres MTU pour eth0 sur tous les nœuds.
   - Utilisez la requête fournie dans Grid Manager.
   - Accédez à *primary Admin Node IP address*`/metrics/graph` et entrez la requête suivante : `node_network_mtu_bytes{interface='eth0'}`
2. Modifiez les paramètres MTU si nécessaire pour vous assurer qu'ils sont identiques pour l'interface réseau Grid (eth0) sur tous les nœuds.
   - Pour les nœuds d'appliance, reportez-vous aux instructions d'installation et de maintenance de votre appliance.
   - Pour les nœuds Linux et VMware, utilisez la commande suivante : `/usr/sbin/change-mtu.py [-h] [-n node] mtu network [network...]`

     Exemple : `change-mtu.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 qu'elle ait la valeur MTU souhaitée, puis utiliser `change-mtu.py` Script pour modifier la valeur MTU du réseau dans le conteneur.

     Utilisez les arguments suivants pour modifier la MTU sur les nœuds Linux ou VMware.

Arguments de position	Description
`mtu`	La MTU à définir. Doit être compris entre 1280 et 9216.
`network`	Réseaux auxquels appliquer la MTU. Incluez un ou plusieurs des types de réseau suivants : • grille • admin • client

+

Arguments facultatifs	Description
`-h, - help`	Afficher le message d'aide et quitter.
`-n node, --node node`	Le nœud. La valeur par défaut est le nœud local.

Informations associées

"SG100 etamp ; appareils de services SG1000"

"Dispositifs de stockage SG6000"

"Appliances de stockage SG5700"

"Appliances de stockage SG5600"

Dépannage de l'alarme d'erreur de réception réseau (NRER)

Les alarmes d'erreur de réception réseau (NRER) peuvent être causées par des problèmes de connectivité entre StorageGRID et votre matériel réseau. Dans certains cas, les erreurs NRER peuvent être résolues sans intervention manuelle. Si les erreurs ne sont pas claires, effectuez les actions recommandées.

Description de la tâche

Les alarmes NRER peuvent être causées par les problèmes suivants avec le matériel réseau connecté à StorageGRID :

- La correction d'erreur de marche avant (FEC) est requise et n'est pas utilisée
- Le port du commutateur et la MTU de la carte réseau ne correspondent pas
- Taux d'erreur de liaison élevés
- Dépassement de la mémoire tampon de la sonnerie NIC

Étapes

1. Suivez les étapes de dépannage pour toutes les causes potentielles de l'alarme NRER compte tenu de votre configuration réseau.

   - Si l'erreur est due à une discordance FEC, effectuez les opérations suivantes :

     Remarque: Ces étapes ne s'appliquent qu'aux erreurs de RER causées par le non-concordance FEC sur les appareils StorageGRID.

     i. Vérifiez l'état FEC du port du commutateur connecté à votre appliance StorageGRID.
     ii. Vérifiez l'intégrité physique des câbles entre l'appareil et le commutateur.
     iii. Si vous souhaitez modifier les paramètres FEC pour tenter de résoudre l'alarme NRER, assurez-vous d'abord que l'appliance est configurée pour le mode **Auto** sur la page Configuration des liens du programme d'installation de l'appareil StorageGRID (voir les instructions d'installation et de maintenance de votre appareil). Modifiez ensuite les paramètres FEC sur les ports du commutateur. Si possible, les ports de l'appliance StorageGRID ajustent leurs paramètres FEC.

     (Vous ne pouvez pas configurer les paramètres FEC sur les appliances StorageGRID. Au lieu de cela, les appareils tentent de détecter et de mettre en miroir les paramètres FEC sur les ports de commutateur auxquels ils sont connectés. Si les liaisons sont forcées à des vitesses de réseau 25 GbE ou 100 GbE, le commutateur et la carte réseau peuvent ne pas négocier un paramètre FEC commun. Sans paramètre FEC commun, le réseau revient en mode « no-FEC ». Lorsque le mode FEC n'est pas activé, les connexions sont plus susceptibles d'erreurs dues au bruit électrique.)

     Note: Les appareils StorageGRID prennent en charge Firecode (FC) et Solomon Reed (RS) FEC, ainsi que pas de FEC.

   - Si l'erreur est causée par une discordance de port de commutateur et de MTU de carte réseau, vérifiez que la taille de MTU configurée sur le nœud est identique au paramètre MTU du port de commutateur.

     La taille de MTU configurée sur le nœud peut être inférieure à celle définie sur le port de commutateur auquel le nœud est connecté. Si un nœud StorageGRID reçoit une trame Ethernet supérieure à sa

MTU, ce qui est possible avec cette configuration, l'alarme NRER peut être signalée. Si vous pensez que c'est ce qui se passe, modifiez la MTU du port du switch pour qu'il corresponde à la MTU de l'interface réseau StorageGRID, ou modifiez la MTU de l'interface réseau StorageGRID pour qu'elle corresponde au port du switch, en fonction de vos objectifs ou de vos exigences MTU de bout en bout.

> Pour des performances réseau optimales, tous les nœuds doivent être configurés avec des valeurs MTU similaires sur leurs interfaces réseau Grid. L'alerte **Grid Network MTU mismatch** est déclenchée en cas de différence importante dans les paramètres MTU pour le réseau Grid sur les nœuds individuels. Les valeurs MTU ne doivent pas être identiques pour tous les types de réseau.

> Pour modifier les paramètres MTU, consultez le guide d'installation et de maintenance de votre appareil.

- Si l'erreur est causée par des taux d'erreur élevés de liaison, effectuez les opérations suivantes :
  i. Activez FEC, si ce n'est déjà fait.
  ii. Vérifiez que le câblage réseau est de bonne qualité et qu'il n'est pas endommagé ou mal connecté.
  iii. Si les câbles ne semblent pas être à l'origine du problème, contactez le support technique.

  > Vous remarquerez peut-être des taux d'erreur élevés dans un environnement présentant un bruit électrique élevé.

- Si l'erreur est un dépassement de la mémoire tampon de la sonnerie de la carte réseau, contactez le support technique.

  La mémoire tampon annulaire peut être surchargée lorsque le système StorageGRID est surchargé et ne peut pas traiter les événements réseau en temps opportun.

2. Une fois que vous avez résolu le problème sous-jacent, réinitialisez le compteur d'erreurs.
   a. Sélectionnez **support** > **Outils** > **topologie de grille**.
   b. Sélectionnez ***site*** > ***grid node*** > **SSM** > **Resources** > **Configuration** > **main**.
   c. Sélectionnez **Réinitialiser le nombre d'erreurs de réception** et cliquez sur **appliquer les modifications**.

Informations associées

"Dépannage de l'alerte de non-concordance de MTU du réseau Grid"

"Référence des alarmes (système hérité)"

"Dispositifs de stockage SG6000"

"Appliances de stockage SG5700"

"Appliances de stockage SG5600"

"SG100 etamp ; appareils de services SG1000"

Dépannage des erreurs de synchronisation de l'heure

Des problèmes de synchronisation de l'heure peuvent s'afficher dans votre grille.

Si vous rencontrez des problèmes de synchronisation du temps, vérifiez que vous avez spécifié au moins quatre sources NTP externes, chacune fournissant une référence Stratum 3 ou supérieure, et que toutes les sources NTP externes fonctionnent normalement et sont accessibles par vos nœuds StorageGRID.

> Lorsque vous spécifiez la source NTP externe pour une installation StorageGRID au niveau de la production, n'utilisez pas le service Windows Time (W32Time) sur une version de Windows antérieure à Windows Server 2016. Le service de temps des versions antérieures de Windows n'est pas suffisamment précis et n'est pas pris en charge par Microsoft pour une utilisation dans des environnements à haute précision, tels que StorageGRID.

Informations associées

"Maintenance et récupération"

Linux : problèmes de connectivité réseau

Il se peut que des problèmes de connectivité réseau existent pour les nœuds grid StorageGRID hébergés sur des hôtes Linux.

Clonage d'adresses MAC

Dans certains cas, les problèmes de réseau peuvent être résolus en utilisant le clonage d'adresses MAC. Si vous utilisez des hôtes virtuels, définissez la valeur de la clé de clonage d'adresse MAC de chacun de vos réseaux sur « true » dans le fichier de configuration de nœud. Ce paramètre entraîne l'utilisation de l'adresse MAC du conteneur StorageGRID de l'hôte. Pour créer des fichiers de configuration de nœud, reportez-vous aux instructions du guide d'installation de votre plate-forme.

> Créez des interfaces réseau virtuelles distinctes pour le système d'exploitation hôte Linux. L'utilisation des mêmes interfaces réseau pour le système d'exploitation hôte Linux et le conteneur StorageGRID peut rendre le système d'exploitation hôte inaccessible si le mode promiscuous n'a pas été activé sur l'hyperviseur.

Pour plus d'informations sur l'activation du clonage MAC, reportez-vous aux instructions du guide d'installation de votre plate-forme.

Mode promiscueux

Si vous ne souhaitez pas utiliser le clonage d'adresses MAC et que toutes les interfaces puissent recevoir et transmettre des données pour des adresses MAC autres que celles attribuées par l'hyperviseur, Assurez-vous que les propriétés de sécurité aux niveaux de commutateur virtuel et de groupe de ports sont définies sur **Accept** pour le mode promiscuous, les changements d'adresse MAC et les transmissions forgées. Les valeurs définies sur le commutateur virtuel peuvent être remplacées par les valeurs au niveau du groupe de ports, de sorte que les paramètres soient les mêmes aux deux endroits.

Informations associées

"Installez Red Hat Enterprise Linux ou CentOS"

"Installez Ubuntu ou Debian"

Linux : l'état du nœud est « orphelin »

Un nœud Linux à l'état orphelin indique généralement que le service StorageGRID ou le démon du nœud StorageGRID contrôlant le conteneur du nœud est décédé de façon inattendue.

Description de la tâche

Si un nœud Linux signale qu'il est dans un état orphelin, vous devez :

- Vérifiez les journaux à la recherche d'erreurs et de messages.
- Tentative de démarrage du nœud.
- Si nécessaire, utilisez des commandes Docker pour arrêter le conteneur de nœud existant.
- Redémarrez le nœud.

Étapes

1. Vérifiez les journaux du démon du service et du nœud orphelin pour voir si des erreurs évidentes et des messages relatifs à la fermeture inopinée.
2. Connectez-vous à l'hôte en tant que root ou en utilisant un compte avec l'autorisation sudo.
3. Tentative de démarrage du nœud à nouveau 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 conteneur Docker et tous les processus de nœud StorageGRID qui contrôlent :`sudo docker stop --time secondscontainer-name`

   Pour `seconds`, saisissez le nombre de secondes que vous souhaitez attendre l'arrêt du conteneur (généralement 15 minutes ou moins).

   ```
   sudo docker stop --time 900 storagegrid-DC1-S1-172-16-1-172
   ```

5. Redémarrez le nœud : `storagegrid node start node-name`

   ```
   storagegrid node start DC1-S1-172-16-1-172
   ```

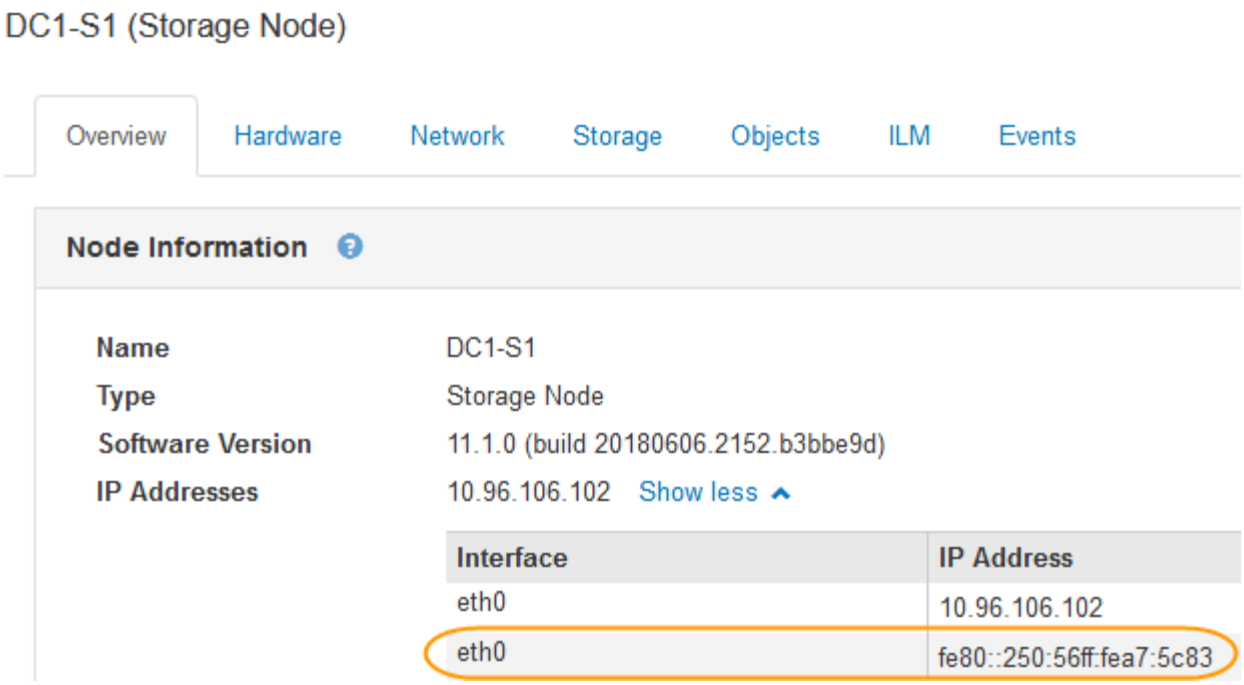
Linux : dépannage de la prise en charge IPv6

Vous devrez peut-être activer la prise en charge IPv6 dans le noyau si vous avez installé des nœuds StorageGRID sur des hôtes Linux et que vous remarquez que les adresses IPv6 n'ont pas été attribuées aux conteneurs de nœuds comme prévu.

Description de la tâche

L'adresse IPv6 attribuée à un nœud de grille s'affiche aux emplacements suivants dans Grid Manager :

- Sélectionnez **Nodes** et sélectionnez le nœud. Cliquez ensuite sur **Afficher plus** en regard de **adresses IP** dans l'onglet vue d'ensemble.



- Sélectionnez **support** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***node*** > **SSM** > **Ressources**. Si une adresse IPv6 a été attribuée, elle est répertoriée sous l'adresse IPv4 dans la section **adresses réseau**.

Si l'adresse IPv6 n'est pas affichée et que le nœud est installé sur un hôte Linux, procédez comme suit pour activer la prise en charge IPv6 dans le noyau.

Étapes

1. Connectez-vous à l'hôte en tant que root ou en utilisant un compte avec l'autorisation sudo.
2. Exécutez la commande suivante : `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@SG:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

Le résultat doit être 0.

```
net.ipv6.conf.all.disable_ipv6 = 0
```

> Si le résultat n'est pas 0, reportez-vous à la documentation de votre système d'exploitation pour la modification `sysctl` paramètres. Ensuite, définissez la valeur sur 0 avant de continuer.

3. Saisissez le conteneur de nœuds StorageGRID : `storagegrid node enter node-name`
4. Exécutez la commande suivante : `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@DC1-S1:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

Le résultat doit être 1.

```
net.ipv6.conf.all.disable_ipv6 = 1
```

> Si le résultat n'est pas 1, cette procédure ne s'applique pas. Contactez l'assistance technique.

5. Quitter le conteneur : `exit`

```
root@DC1-S1:~ # exit
```

6. En tant que racine, modifiez 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
```

Examiner les journaux d'audit

Apprenez les journaux d'audit du système StorageGRID et affichez la liste de tous les messages d'audit.

- "Présentation du message d'audit"
- "Formats du fichier journal d'audit et des messages"
- "Messages d'audit et cycle de vie de l'objet"
- "Messages d'audit"

Présentation du message d'audit

Ces instructions contiennent des informations sur la structure et le contenu des messages d'audit StorageGRID et des journaux d'audit. Vous pouvez utiliser ces informations pour lire et analyser la piste d'audit de l'activité du système.

Ces instructions s'adresse aux administrateurs responsables de la production de rapports d'activité et d'utilisation du système qui nécessitent une analyse des messages d'audit du système StorageGRID.

Vous êtes supposé avoir une bonne compréhension de la nature des activités vérifiées dans le système StorageGRID. Pour utiliser le fichier journal texte, vous devez avoir accès au partage d'audit configuré sur le nœud d'administration.

Informations associées

"Administrer StorageGRID"

Flux et conservation des messages d'audit

Tous les services StorageGRID génèrent des messages d'audit pendant le fonctionnement normal du système. Vous devez comprendre comment ces messages d'audit passent du système StorageGRID au système `audit.log` fichier.

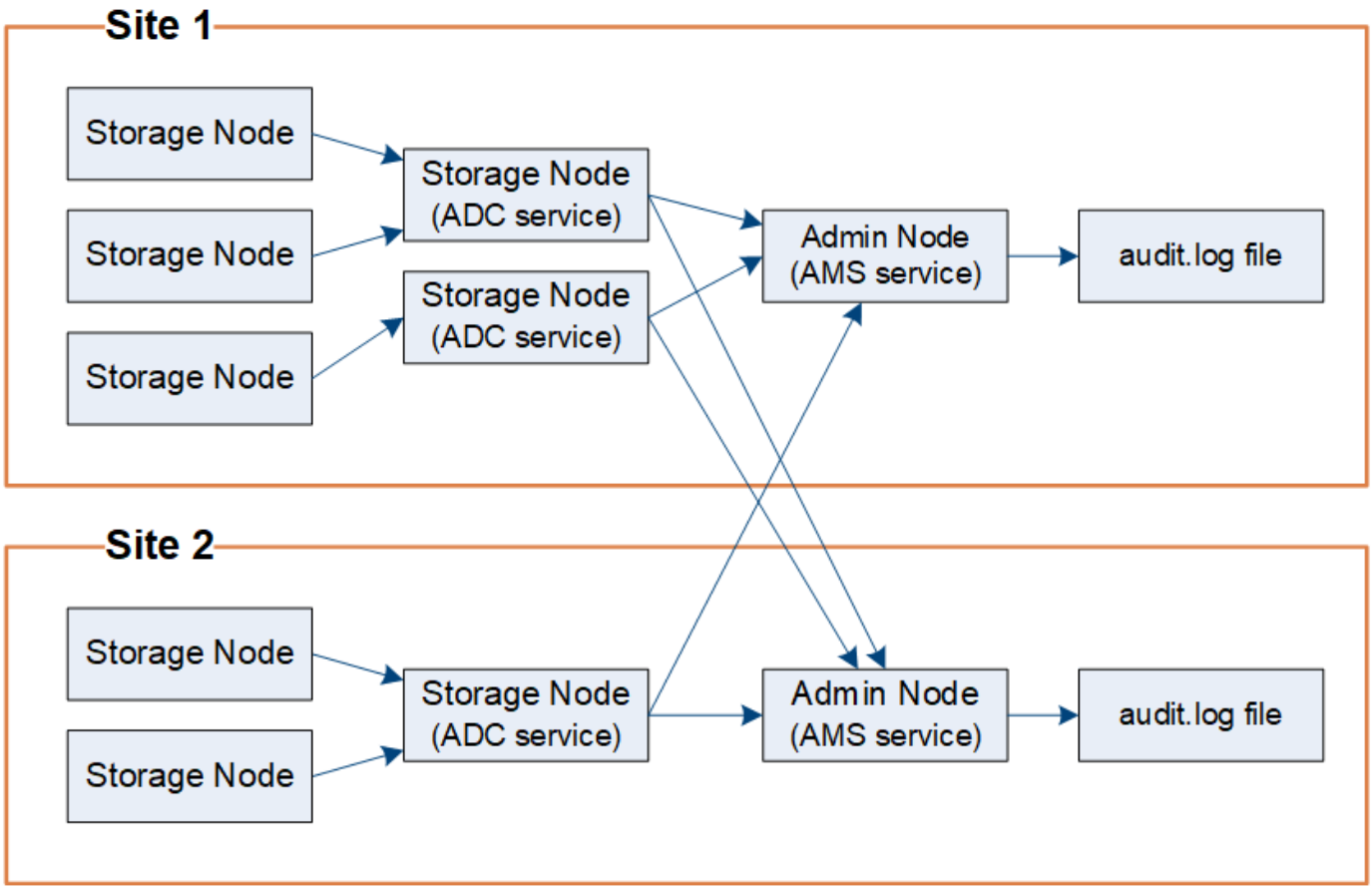
Flux de message d'audit

Les messages d'audit sont traités par des nœuds d'administration et par les nœuds de stockage disposant d'un service ADC (administrative Domain Controller).

Comme indiqué dans le schéma de flux des messages d'audit, chaque nœud StorageGRID envoie ses messages d'audit à l'un des services ADC du site du centre de données. Le service ADC est automatiquement activé pour les trois premiers nœuds de stockage installés sur chaque site.

De son tour, chaque service ADC agit comme un relais et envoie sa collection de messages d'audit à chaque nœud d'administration du système StorageGRID, ce qui donne à chaque nœud d'administration un enregistrement complet de l'activité du système.

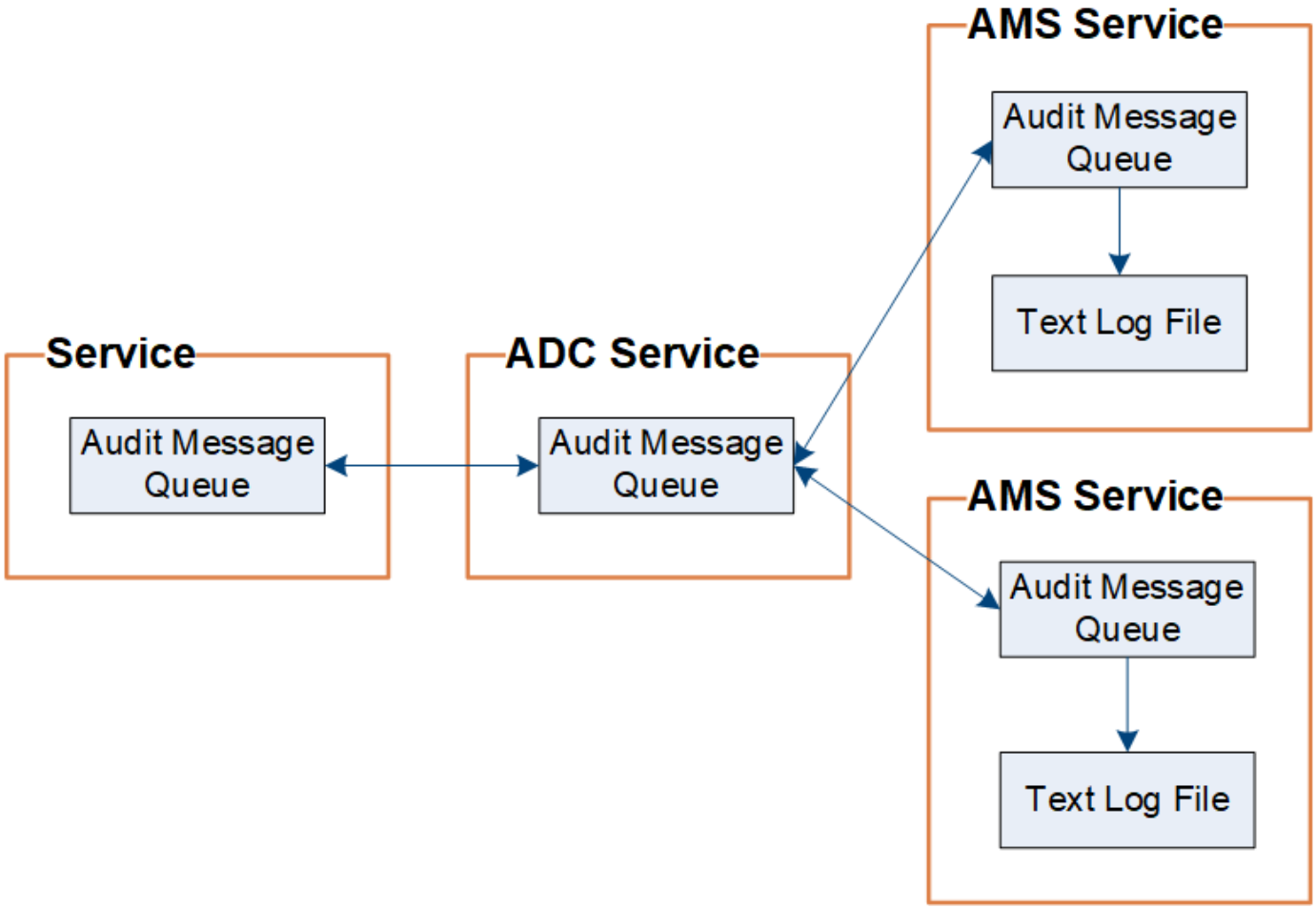
Chaque nœud d'administration stocke les messages d'audit dans des fichiers journaux texte ; le fichier journal actif est nommé `audit.log`.



Conservation des messages d'audit

StorageGRID utilise un processus de copie et de suppression pour garantir qu'aucun message d'audit ne soit perdu avant d'être écrit dans le journal d'audit.

Lorsqu'un nœud génère ou transmet un message d'audit, celui-ci est stocké dans une file d'attente de messages d'audit sur le disque système du nœud de la grille. Une copie du message est toujours conservée dans une file d'attente de messages d'audit jusqu'à ce que le message soit écrit dans le fichier journal d'audit du nœud d'administration `/var/local/audit/export` répertoire. Cela permet d'éviter la perte d'un message d'audit pendant le transport.



La file d'attente des messages d'audit peut augmenter temporairement en raison de problèmes de connectivité réseau ou d'une capacité d'audit insuffisante. Au fur et à mesure que les files d'attente augmentent, elles consomment davantage d'espace disponible dans chaque nœud `/var/local/` répertoire. Si le problème persiste et que le répertoire des messages d'audit d'un nœud devient trop plein, les nœuds individuels priorisent le traitement de leur carnet de commandes et deviennent temporairement indisponibles pour les nouveaux messages.

Plus précisément, vous pouvez voir les comportements suivants :

- Si le `/var/local/audit/export` Le répertoire utilisé par un nœud d'administration devient plein, le nœud d'administration sera signalé comme indisponible pour les nouveaux messages d'audit jusqu'à ce que le répertoire ne soit plus plein. Les demandes des clients S3 et Swift ne sont pas affectées. L'alarme XAMS (Unreable Audit Revers) 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 signalé comme indisponible pour les messages d'audit jusqu'à ce que le répertoire soit plein à seulement 87 %. Les demandes des clients S3 et Swift vers d'autres nœuds ne sont pas affectées. L'alarme NRLY (relais d'audit disponibles) est déclenchée lorsque les relais d'audit sont inaccessibles.

  > Si aucun nœud de stockage n'est disponible avec le service ADC, les nœuds de stockage stockent les messages d'audit localement.

- Si le `/var/local/` Le répertoire utilisé par un nœud de stockage devient plein à 85 %. Le nœud refuse les demandes des clients S3 et Swift avec `503 Service Unavailable`.

Les types de problèmes suivants peuvent entraîner une augmentation très importante des files d'attente de messages d'audit :

- Panne d'un nœud d'administration ou d'un nœud de stockage avec le service ADC. Si l'un des nœuds du système est en panne, les nœuds restants peuvent devenir connectés à un nœud défaillant.
- Un taux d'activité soutenu qui dépasse la capacité d'audit du système.
- Le `/var/local/` L'espace sur un nœud de stockage ADC est saturé pour des raisons sans rapport avec les messages d'audit. Dans ce cas, le nœud n'accepte plus de nouveaux messages d'audit et hiérarchise son carnet de commandes actuel, ce qui peut entraîner des arriérés sur les autres nœuds.

Alerte de file d'attente d'audit et alarme de messages d'audit en file d'attente (AMQS)

Pour vous aider à surveiller la taille des files d'attente de messages d'audit dans le temps, l'alerte **grande file d'attente d'audit** et l'alarme AMQS héritée sont déclenchées lorsque le nombre de messages dans une file d'attente de nœud de stockage ou une file d'attente de nœud d'administration atteint certains seuils.

Si l'alerte **grande file d'attente d'audit** ou l'alarme AMQS héritée est déclenchée, commencez par vérifier la charge sur le système—s'il y a eu un nombre important de transactions récentes, l'alerte et l'alarme doivent être résolus au fil du temps et peuvent être ignorées.

Si l'alerte ou l'alarme persiste et augmente la gravité, affichez un graphique de la taille de la file d'attente. Si ce chiffre augmente régulièrement au fil des heures ou des jours, la charge d'audit a probablement dépassé la capacité d'audit du système. Réduisez le taux de fonctionnement du client ou diminuez le nombre de messages d'audit consignés en modifiant le niveau d'audit pour les écritures du client et les lectures du client sur erreur ou Désactivé. Voir «"Modification des niveaux de messages d'audit"."

Dupliquer les messages

Le système StorageGRID adopte une approche prudente en cas de panne sur un réseau ou un nœud. Pour cette raison, des messages en double peuvent exister dans le journal d'audit.

Modification des niveaux de messages d'audit

Vous pouvez ajuster les niveaux d'audit pour augmenter ou diminuer le nombre de messages d'audit enregistrés dans le journal d'audit pour chaque catégorie de messages d'audit.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

Les messages d'audit enregistrés dans le journal d'audit sont filtrés en fonction des paramètres de la page **Configuration** > **surveillance** > **Audit**.

Vous pouvez définir un niveau d'audit différent pour chacune des catégories de messages suivantes :

- **Système** : par défaut, ce niveau est défini sur Normal.
- **Stockage** : par défaut, ce niveau est défini sur erreur.
- **Gestion** : par défaut, ce niveau est défini sur Normal.
- **Lecture client** : par défaut, ce niveau est défini sur Normal.

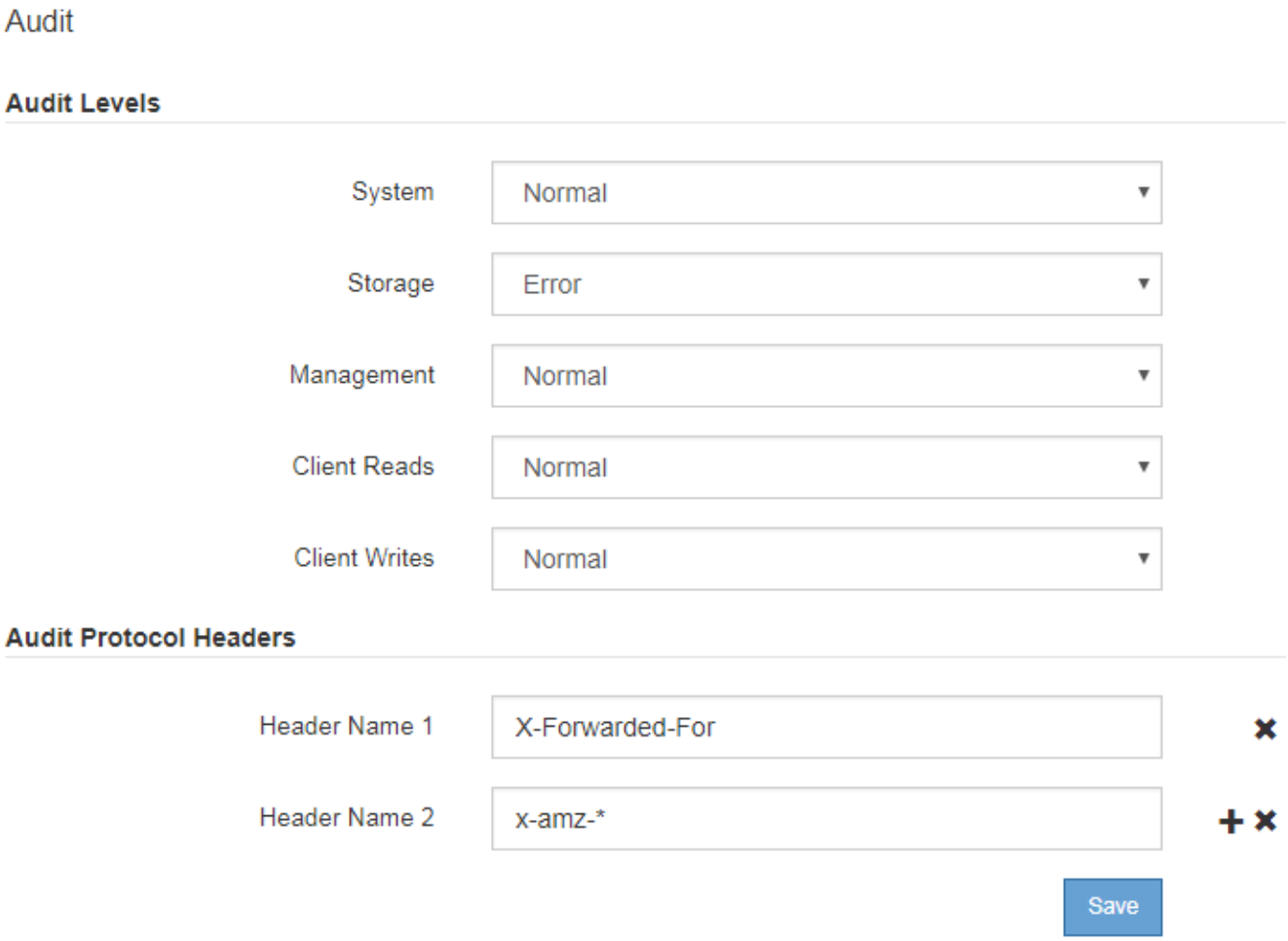
- **Écrit client** : par défaut, ce niveau est défini sur Normal.

Ces valeurs par défaut s'appliquent si vous avez installé StorageGRID à l'origine à l'aide de la version 10.3 ou ultérieure. Si vous avez mis à niveau à partir d'une version antérieure de StorageGRID, la valeur par défaut pour toutes les catégories est Normal.

Durant les mises à niveau, les configurations des niveaux d'audit ne seront pas effectives immédiatement.

Étapes

1. Sélectionnez **Configuration** > **surveillance** > **Audit**.



2. Pour chaque catégorie de message d'audit, sélectionnez un niveau d'audit dans la liste déroulante :

Niveau d'audit	Description
Éteint	Aucun message d'audit de la catégorie n'est enregistré.
Erreur	Seuls les messages d'erreur sont consignés—les messages d'audit pour lesquels le code de résultat n'a pas été « réussi » (CMC).

Niveau d'audit	Description
Normale	Les messages transactionnels standard sont consignés—les messages répertoriés dans ces instructions pour la catégorie.
Débogage	Obsolète. Ce niveau se comporte de la même manière que le niveau d'audit normal.

Les messages inclus pour tout niveau particulier incluent ceux qui seraient consignés aux niveaux supérieurs. Par exemple, le niveau Normal inclut tous les messages d'erreur.

3. Sous **en-têtes de protocole d'audit**, entrez le nom des en-têtes de requête HTTP à inclure dans les messages d'audit lecture client et écriture client. Utilisez un astérisque (*) comme caractère générique ou utilisez la séquence d'échappement (*) comme astérisque littéral. Cliquez sur le signe plus pour créer une liste de champs de nom d'en-tête.

   Les en-têtes de protocole d'audit ne s'appliquent qu'aux demandes S3 et Swift.

   Lorsque de tels en-têtes HTTP sont trouvés dans une requête, ils sont inclus dans le message d'audit sous le champ HTRH.

   Les en-têtes de requête de protocole d'audit ne sont consignés que si le niveau d'audit pour **lecture client** ou **écriture client** n'est pas **off**.

4. Cliquez sur **Enregistrer**.

Informations associées

"Messages d'audit système"

"Messages d'audit du stockage objet"

"Message d'audit de gestion"

"Messages d'audit de lecture du client"

"Administrer StorageGRID"

Accès au fichier journal d'audit

Le partage d'audit contient le partage actif `audit.log` fichier et tous les fichiers journaux d'audit compressés. Pour accéder facilement aux journaux d'audit, vous pouvez configurer l'accès des clients aux partages d'audit pour NFS et CIFS (obsolètes). Vous pouvez également accéder aux fichiers journaux d'audit directement à partir de la ligne de commande du nœud d'administration.

Ce dont vous avez besoin

- Vous devez disposer d'autorisations d'accès spécifiques.
- Vous devez avoir le `Passwords.txt` fichier.
- Vous devez connaître l'adresse IP d'un nœud d'administration.

Étapes

1. Connectez-vous à un nœud d'administration :
   a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
2. Accédez au répertoire contenant les fichiers journaux d'audit :

   ```
   cd /var/local/audit/export
   ```

3. Afficher le fichier journal d'audit actuel ou enregistré, selon les besoins.

Informations associées

"Administrer StorageGRID"

Rotation du fichier journal d'audit

Les fichiers journaux d'audit sont enregistrés sur un nœud d'administration `/var/local/audit/export` répertoire. Les fichiers journaux d'audit actifs sont nommés `audit.log`.

Une fois par jour, le 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 dans un seul jour, les noms de fichiers utilisent la date d'enregistrement du fichier, ajoutée par un nombre, dans le format *`yyyy-mm-dd.txt.n`*. Par exemple : `2018-04-15.txt` et `2018-04-15.txt.1` Sont les premier et deuxième fichiers journaux créés et enregistrés le 15 avril 2018.

Après un jour, le fichier enregistré est compressé et renommé, au format *`yyyy-mm-dd.txt.gz`*, qui conserve la date originale. Avec le temps, cela entraîne la consommation du stockage alloué aux journaux d'audit sur le nœud d'administration. Un script surveille la consommation d'espace du journal d'audit et supprime les fichiers journaux si nécessaire pour libérer de l'espace dans le `/var/local/audit/export` répertoire. Les journaux d'audit sont supprimés en fonction de la date de création, le plus ancien étant supprimé en premier. Vous pouvez contrôler les actions du script dans le fichier suivant : `/var/local/log/manage-audit.log`.

Cet exemple montre l'actif `audit.log` fichier du jour précédent (`2018-04-15.txt`), et le fichier compressé pour la veille (`2018-04-14.txt.gz`).

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

Formats du fichier journal d'audit et des messages

Les journaux d'audit permettent de collecter les informations sur votre système et de résoudre les problèmes. Vous devez comprendre le format du fichier journal d'audit et le format général utilisé pour les messages d'audit.

Format du fichier journal d'audit

Les fichiers journaux d'audit se trouvent sur chaque nœud d'administration et contiennent

un ensemble de messages d’audit individuels.

Chaque message d’audit contient les éléments suivants :

- Temps universel coordonné (UTC) de l’événement qui a déclenché le message d’audit (ATIM) au format ISO 8601, suivi d’un espace :

  YYYY-MM-DDTHH:MM:SS.UUUUUU, où *UUUUUU* sont des microsecondes.

- Le message d’audit lui-même, entre crochets et commençant par `AUDT`.

L’exemple suivant montre trois messages d’audit dans un fichier journal d’audit (sauts de ligne ajoutés pour la lisibilité). Ces messages ont été générés lorsqu’un locataire a créé un compartiment S3 et a ajouté deux objets dans ce compartiment.

```
2019-08-07T18:43:30.247711
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][SAI
P(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][AVER(UI32):10][ATIM(UI64):1565203410247711]
[ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):7074142
142472611085]]

2019-08-07T18:43:30.783597
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991696][TIME(UI64):120713][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-0"]
[CBID(UI64):0x779557A069B2C037][UUID(CSTR):"94BA6949-38E1-4B0C-BC80-
EB44FB4FCC7F"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410783597][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):8439606722108456022]]

2019-08-07T18:43:30.784558
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991693][TIME(UI64):121666][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-2000"]
[CBID(UI64):0x180CBD8E678EED17][UUID(CSTR):"19CE06D0-D2CF-4B03-9C38-
E578D66F7ADD"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410784558][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):13489590586043706682]]
```

Dans leur format par défaut, les messages d'audit dans les fichiers journaux d'audit ne sont pas faciles à lire ou à interpréter. Vous pouvez utiliser le `audit-explain` outil pour obtenir des résumés simplifiés des messages d'audit dans le journal d'audit. Vous pouvez utiliser le `audit-sum` outil pour résumer le nombre d'opérations d'écriture, de lecture et de suppression enregistrées, ainsi que la durée nécessaire à ces opérations.

Informations associées

"Utilisation de l'outil d'explication d'audit"

"À l'aide de l'outil audit-sum"

Utilisation de l'outil d'explication d'audit

Vous pouvez utiliser le `audit-explain` outil permettant de traduire les messages d'audit du journal d'audit dans un format facile à lire.

Ce dont vous avez besoin

- Vous devez disposer d'autorisations d'accès spécifiques.
- Vous devez avoir le `Passwords.txt` fichier.
- Vous devez connaître l'adresse IP du nœud d'administration principal.

Description de la tâche

Le `audit-explain` Disponible sur le nœud d'administration principal, cet outil fournit des résumés simplifiés des messages d'audit dans un journal d'audit.

> Le `audit-explain` l'outil est principalement destiné au support technique lors des opérations de dépannage. En cours de traitement `audit-explain` Les requêtes peuvent consommer une très grande quantité d'énergie dans le processeur, ce qui peut affecter les opérations de StorageGRID.

Cet exemple montre une sortie type de l' `audit-explain` outil. Ces quatre messages d'audit SPUT ont été générés lorsque le locataire S3 avec l'ID de compte 92484777680322627870 a UTILISÉ les demandes S3 POUR créer un compartiment nommé « bucket1 » et ajouter trois objets dans ce compartiment.

```
SPUT S3 PUT bucket bucket1 account:92484777680322627870 usec:124673
SPUT S3 PUT object bucket1/part1.txt tenant:92484777680322627870
cbid:9DCB157394F99FE5 usec:101485
SPUT S3 PUT object bucket1/part2.txt tenant:92484777680322627870
cbid:3CFBB07AB3D32CA9 usec:102804
SPUT S3 PUT object bucket1/part3.txt tenant:92484777680322627870
cbid:5373D73831ECC743 usec:93874
```

Le `audit-explain` l'outil peut traiter des journaux d'audit simples ou compressés. Par exemple :

```
audit-explain audit.log
```

```
audit-explain 2019-08-12.txt.gz
```

Le `audit-explain` l'outil peut également traiter plusieurs fichiers en même temps. Par exemple :

```
audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-explain /var/local/audit/export/*
```

Enfin, le `audit-explain` l'outil peut accepter les entrées d'un tuyau, ce qui vous permet de filtrer et de prétraiter l'entrée à l'aide de l' `grep` commande ou autre moyen. Par exemple :

```
grep SPUT audit.log | audit-explain
```

```
grep bucket-name audit.log | audit-explain
```

Puisque les journaux d'audit peuvent être très volumineux et lents à analyser, vous pouvez gagner du temps en filtrant les pièces que vous voulez regarder et exécuter `audit-explain` sur les pièces, au lieu du fichier entier.

> Le `audit-explain` l'outil n'accepte pas les fichiers compressés comme entrée de canalisation. Pour traiter des fichiers compressés, indiquez leurs noms de fichier comme arguments de ligne de commande ou utilisez le `zcat` outil de décompression des fichiers en premier. Par exemple :

```
zcat audit.log.gz | audit-explain
```

Utilisez le `help (-h)` pour voir les options disponibles. Par exemple :

```
$ audit-explain -h
```

Étapes

1. Connectez-vous au nœud d'administration principal :
   a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
2. Entrez la commande suivante, où `/var/local/audit/export/audit.log` représente le nom et l'emplacement du ou des fichiers à analyser :

   ```
   $ audit-explain /var/local/audit/export/audit.log
   ```

   Le `audit-explain` l'outil imprime les interprétations lisibles par l'homme de tous les messages du ou des fichiers spécifiés.

   > Pour réduire la longueur des lignes et faciliter leur lisibilité, les horodatages ne sont pas affichés par défaut. Si vous voulez voir les horodatages, utilisez l'horodatage (`-t`) option.

Informations associées

"SPUT : PUT S3"

À l'aide de l'outil audit-sum

Vous pouvez utiliser le `audit-sum` outil permettant de compter les messages d'audit d'écriture, de lecture, d'en-tête et de suppression, ainsi que les temps minimum, maximum et moyen (ou taille) pour chaque type d'opération.

Ce dont vous avez besoin

- Vous devez disposer d'autorisations d'accès spécifiques.
- Vous devez avoir le `Passwords.txt` fichier.
- Vous devez connaître l'adresse IP du nœud d'administration principal.

Description de la tâche

Le `audit-sum` Disponible sur le nœud d'administration principal, cet outil récapitule 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 au support technique lors des opérations de dépannage. En cours de traitement `audit-sum` Les requêtes peuvent consommer une très grande quantité d'énergie dans le processeur, ce qui peut affecter les opérations de StorageGRID.

Cet exemple montre une sortie type de l' `audit-sum` outil. Cet exemple montre la durée des opérations de protocoles.

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  IDEL                      274
  SDEL                   213371        0.004          20.934
0.352
  SGET                   201906        0.010        1740.290
1.132
  SHEA                    22716        0.005           2.349
0.272
  SPUT                 1771398        0.011        1770.563
0.487
```

Le `audit-sum` Dans un journal d'audit, l'outil indique le nombre et la durée des messages d'audit S3, Swift et ILM suivants :

Code	Description	Reportez-vous à la section
ARCT	Archivage depuis le Tier cloud	"ARCT : récupération d'archives depuis Cloud-Tier"
ASCT	Tier cloud du magasin d'archivage	"ASCT : magasin d'archives, niveau du cloud"

Code	Description	Reportez-vous à la section
IDEL	ILM initialisée – journaux lorsque l'ILM démarre le processus de suppression d'un objet.	"IDEL : suppression initiée ILM"
SDEL	SUPPRESSION S3 : journal une transaction réussie pour supprimer un objet ou un compartiment.	"SDEL : SUPPRESSION S3"
SGET	S3 GET : log une transaction réussie pour récupérer un objet ou répertorier les objets dans un compartiment.	"SGET : OBTENEZ S3"
SHEA	TÊTE S3 : consigne une transaction réussie pour vérifier l'existence d'un objet ou d'un compartiment.	"SHEA : TÊTE S3"
SPUT	S3 PUT : enregistre la réussite d'une transaction pour créer un nouvel objet ou un compartiment.	"SPUT : PUT S3"
WDEL	SUPPRESSION Swift : enregistre une transaction réussie pour supprimer un objet ou un conteneur.	"WDEL : SUPPRESSION rapide"
C'EST PARTI	SWIFT GET : log une transaction réussie pour récupérer un objet ou répertorier les objets dans un conteneur.	"WGET: SWIFT GET"
WHEA	SWIFT HEAD : consigne une transaction réussie afin de vérifier l'existence d'un objet ou d'un conteneur.	"WHEA: TÊTE SWIFT"
WPUT	SWIFT PUT : consigne une transaction réussie pour créer un nouvel objet ou conteneur.	"WPUT : PUT SWIFT"

Le `audit-sum` l'outil peut traiter des journaux d'audit simples ou compressés. Par exemple :

```
audit-sum audit.log
```

```
audit-sum 2019-08-12.txt.gz
```

Le `audit-sum` l'outil peut également traiter plusieurs fichiers en même temps. Par exemple :

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-sum /var/local/audit/export/*
```

Enfin, le `audit-sum` l'outil peut également accepter l'entrée d'un tuyau, ce qui vous permet de filtrer et de prétraiter l'entrée à l'aide de l' `grep` commande ou autre moyen. Par exemple :

```
grep WGET audit.log | audit-sum
```

```
grep bucket1 audit.log | audit-sum
```

```
grep SPUT audit.log | grep bucket1 | audit-sum
```

> Cet outil n'accepte pas les fichiers compressés comme entrée de pipettes. Pour traiter des fichiers compressés, indiquez leurs noms de fichier comme arguments de ligne de commande ou utilisez le `zcat` outil de décompression des fichiers en premier. Par exemple :

```
audit-sum audit.log.gz
```

```
zcat audit.log.gz | audit-sum
```

Vous pouvez utiliser les options de ligne de commande pour résumer les opérations sur des compartiments séparément des opérations sur des objets ou pour regrouper les résumés de messages par nom de compartiment, par période ou par type de cible. Par défaut, les résumés indiquent le temps de fonctionnement minimum, maximum et moyen, mais vous pouvez utiliser le `size (-s)` option pour regarder la taille de l'objet.

Utilisez le `help (-h)` pour voir les options disponibles. Par exemple :

```
$ audit-sum -h
```

Étapes

1. Connectez-vous au nœud d'administration principal :
   a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
2. Pour analyser tous les messages liés aux opérations d'écriture, de lecture, de tête et de suppression, procédez comme suit :

a. Entrez la commande suivante, où `/var/local/audit/export/audit.log` représente le nom et l'emplacement du ou des fichiers à analyser :

```
$ audit-sum /var/local/audit/export/audit.log
```

Cet exemple montre une sortie type de l' `audit-sum` outil. Cet exemple montre la durée des opérations de protocoles.

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  IDEL                      274
  SDEL                   213371        0.004          20.934
0.352
  SGET                   201906        0.010        1740.290
1.132
  SHEA                    22716        0.005           2.349
0.272
  SPUT                 1771398        0.011        1770.563
0.487
```

Dans cet exemple, les opérations SGET (S3 GET) sont les opérations les plus lentes en moyenne à 1.13 secondes, mais les opérations SGET et SPUT (S3 PUT) affichent toutes les deux de longues périodes de pire des cas d'environ 1,770 secondes.

b. Pour afficher les opérations de récupération 10 les plus lentes, utilisez la commande grep pour sélectionner uniquement les messages SGET et ajouter l'option de sortie longue (`-l`) pour inclure les chemins d'accès aux objets : `grep SGET audit.log | audit-sum -l`

Les résultats incluent le type (objet ou compartiment) et le chemin, ce qui vous permet d'afficher le journal d'audit pour les autres messages relatifs à ces objets particuliers.

```
Total:          201906 operations
    Slowest:      1740.290 sec
    Average:         1.132 sec
    Fastest:         0.010 sec
    Slowest operations:
        time(usec)       source ip         type      size(B) path
        ========== ============== ============ ============ ====
        1740289662   10.96.101.125       object   5663711385
backup/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
```

+ Dans cet exemple de sortie, vous pouvez constater que les trois demandes GET S3 les plus lentes étaient celles des objets d'une taille d'environ 5 Go (ce qui est beaucoup plus important que les autres objets). La grande taille tient compte des délais de récupération lents les moins importants.

3. Pour déterminer la taille des objets en cours d'ingestion et d'extraction à partir de votre grille, utilisez l'option size (`-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 des objets pour SPUT est inférieure à 2.5 Mo, mais la taille moyenne pour SGET est beaucoup plus grande. Le nombre de messages SPUT est beaucoup plus élevé que le nombre de messages SGET, ce qui indique que la plupart des objets ne sont jamais récupérés.

4. Si vous voulez déterminer si les récupérations étaient lentes hier :
   a. Exécutez la commande sur le journal d'audit approprié et utilisez l'option group-by-time (`-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 S3 GÉNÈRE un trafic entre 06:00 et 07:00. Les temps maximum et moyen sont à la fois considérablement plus élevés à ces moments aussi, et ils n'ont pas augmenté progressivement à mesure que le comptage a augmenté. Cela suggère que la capacité a été dépassée quelque part, peut-être dans le réseau ou que la grille peut traiter les demandes.

b. Pour déterminer la taille des objets récupérés chaque heure hier, ajoutez l'option size (`-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 des récupérations très importantes se sont produites lorsque le trafic global de récupération était à son maximum.

c. Pour plus de détails, utilisez le `audit-explain` Outil pour passer en revue toutes les opérations du SGET au cours de cette heure :

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

Si la sortie de la commande grep est censée être de nombreuses 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 godets sont plus lentes que les opérations SPUT pour les objets :

a. Commencez par utiliser le `-go` option, qui regroupe les messages pour les opérations liées aux objets et aux compartiments séparément :

```
grep SPUT sample.log | audit-sum -go
```

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  SPUT.bucket                 1        0.125           0.125
0.125
  SPUT.object                12        0.025           1.019
0.236
```

Les résultats montrent que les opérations SPUT pour les compartiments ont des caractéristiques de performances différentes de celles des opérations SPUT pour les objets.

b. Pour déterminer les godets dont les opérations SPUT sont les plus lentes, utiliser le `-gb` option, qui regroupe les messages par compartiment :

```
grep SPUT audit.log | audit-sum -gb
```

```
  message group                  count     min(sec)        max(sec)
average(sec)
  =============                  =====     ========        ========
============
  SPUT.cho-non-versioning        71943        0.046        1770.563
1.571
  SPUT.cho-versioning            54277        0.047        1736.633
1.415
  SPUT.cho-west-region           80615        0.040          55.557
1.329
  SPUT.ldt002                  1564563        0.011          51.569
0.361
```

c. Pour déterminer quels compartiments ont la plus grande taille d'objet SPUT, utilisez les deux `-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
```

Informations associées

"Utilisation de l'outil d'explication d'audit"

Format du message d'audit

Les messages d'audit échangés dans le système StorageGRID incluent des informations standard communes à tous les messages et du contenu spécifique décrivant l'événement ou l'activité signalé.

Si le résumé fourni par le `audit-explain` et `audit-sum` les outils sont insuffisants, reportez-vous à cette section pour comprendre le format général de tous les messages de vérification.

Voici un exemple de message d'audit tel qu'il peut apparaître dans le fichier journal d'audit :

```
2014-07-17T03:50:47.484627
[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP(F
C32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265006
03516]]
```

Chaque message d'audit contient une chaîne d'éléments d'attribut. L'ensemble de la chaîne est entre crochets (`[ ]`), et chaque élément d'attribut de la chaîne possède les caractéristiques suivantes :

- Entre crochets `[ ]`
- 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 flux de ligne `\n`

Chaque élément inclut un code d'attribut, un type de données et une valeur qui sont rapportées dans ce format :

```
[ATTR(type):value][ATTR(type):value]...
[ATTR(type):value]\n
```

Le nombre d'éléments d'attribut dans le message dépend du type d'événement du message. Les éléments d'attribut ne sont pas répertoriés dans un ordre particulier.

La liste suivante décrit les éléments d'attribut :

- `ATTR` est un code à quatre caractères pour l'attribut en cours de signalement. Certains attributs sont communs à tous les messages d'audit et à d'autres, qui sont spécifiques à un événement.
- `type` Est un identificateur à quatre caractères du type de données de programmation de la valeur, comme UI64, FC32, etc. Le type est entre parenthèses `( )`.
- `value` est le contenu de l'attribut, généralement une valeur numérique ou de texte. Les valeurs suivent toujours deux-points (`:`). Les valeurs du type de données CSTR sont entourées de guillemets doubles `" "`.

Informations associées

"Utilisation de l'outil d'explication d'audit"

"À l'aide de l'outil audit-sum"

"Messages d'audit"

"Éléments communs dans les messages d'audit"

"Types de données"

"Exemples de messages d'audit"

Types de données

Différents types de données sont utilisés pour stocker les informations dans les messages d'audit.

Type	Description
UI32	Entier long non signé (32 bits) ; il peut stocker les nombres 0 à 4,294,967,295.
UI64	Entier double non signé (64 bits) ; il peut stocker les nombres 0 à 18,446,744,073,709,551,615.
FC32	Constante de quatre caractères ; valeur entière non signée de 32 bits représentée sous la forme de quatre caractères ASCII tels que « ABCD ».
IPAD	Utilisé pour les adresses IP.

Type	Description
REST	Un tableau de caractères UTF-8 à longueur variable. Les caractères peuvent être échappé avec les conventions suivantes : • La barre oblique inverse est \\. • Le retour chariot est \r. • Les guillemets sont \". • La ligne d'alimentation (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 un événement

Chaque message d'audit du journal d'audit enregistre les 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):"account"]
[S3AK(CSTR):"SGKH4_Nc8SO1H6w3w0nCOFCGgk__E6dYzKlumRsKJA=="]
[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` elément (souligné dans l'exemple) identifie l'événement qui a généré le message. Cet exemple de message inclut le code de message SHEA ([ATYP(FC32):SHEA]), indiquant qu'il a été généré par une demande DE TÊTE S3 réussie.

Informations associées

"Éléments communs dans les messages d'audit"

"Messages d'audit"

Éléments communs dans les messages d'audit

Tous les messages d'audit contiennent les éléments communs.

Code	Type	Description
AU MILIEU	FC32	ID du module : identifiant à quatre caractères de l'ID du module qui a généré le message. Ceci indique le segment de code dans lequel le message d'audit a été généré.
ANID	UI32	ID de nœud : ID de nœud de la grille attribué au service qui a généré le message. Un identifiant unique est attribué à chaque service au moment de la configuration et de l'installation du système StorageGRID. Cet ID ne peut pas être modifié.
ASE	UI64	Identifiant de session d'audit : dans les versions précédentes, cet élément indique l'heure à laquelle le système d'audit a été initialisé après le démarrage du service. Cette valeur temporelle a été mesurée en microsecondes depuis l'époque du système d'exploitation (00:00:00 UTC le 1er janvier 1970). **Remarque :** cet élément est obsolète et n'apparaît plus dans les messages d'audit.
ASQN	UI64	Nombre de séquences : dans les versions précédentes, ce compteur a été incrémenté pour chaque message d'audit généré sur le nœud de la grille (ANID) et remis à zéro au redémarrage du service. **Remarque :** cet élément est obsolète et n'apparaît plus dans les messages d'audit.
ATID	UI64	Trace ID : identifiant partagé par l'ensemble de messages déclenchés par un seul événement.
ATIM	UI64	Timestamp: Heure à laquelle l'événement a été généré le message d'audit, mesuré en microsecondes depuis l'époque du système d'exploitation (00:00:00 UTC le 1er janvier 1970). Notez que la plupart des outils disponibles pour convertir l'horodatage en date et heure locales sont basés sur des millisecondes. Il peut être nécessaire d'arrondir ou de tronquer l'horodatage enregistré. Temps lisible par l'homme qui apparaît au début du message d'audit dans le `audit.log` Fichier est l'attribut ATIM au format ISO 8601. La date et l'heure sont représentées sous la forme *`YYYY-MMDDTHH:MM:SS.UUUUUU`*, où `T` est un caractère de chaîne littérale indiquant le début du segment de temps de la date. *`UUUUUU`* sont des microsecondes.
ATYP	FC32	Type d'événement : identificateur à quatre caractères de l'événement en cours d'enregistrement. Cela régit le contenu « charge utile » du message : les attributs inclus.
FINISSEUR	UI32	Version : version du message d'audit. À mesure que le logiciel StorageGRID évolue, les nouvelles versions de services peuvent intégrer de nouvelles fonctionnalités dans les rapports d'audit. Ce champ permet une rétrocompatibilité dans le service AMS pour traiter les messages provenant de versions antérieures de services.

Code	Type	Description
RSLT	FC32	Résultat : résultat de l'événement, du processus ou de la transaction. Si n'est pas pertinent pour un message, AUCUN n'est utilisé plutôt que LES CMC pour que le message ne soit pas filtré accidentellement.

Exemples de messages d'audit

Vous trouverez des informations détaillées dans chaque message d'audit. Tous les messages d'audit utilisent le même format.

Voici un exemple de message d'audit tel qu'il peut apparaître dans le `audit.log` fichier :

```
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 en cours d'enregistrement, ainsi que des informations sur le message d'audit lui-même.

Pour identifier l'événement enregistré par le message d'audit, recherchez l'attribut ATYP (mis en évidence ci-dessous) :

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"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. SPUT représente une transaction PUT S3, dans laquelle il consigne l'entrée d'un objet dans un compartiment.

Le message d'audit suivant indique également le compartiment à partir duquel l'objet est associé :

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"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 universel coordonné (UTC) au début du message d'audit. Cette valeur est une version lisible par l'utilisateur de l'attribut ATIM du message d'audit lui-même :

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"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` Traduit au jeudi 17 juillet 2014 21:17:59 UTC.

Informations associées

"SPUT : PUT S3"

"Éléments communs dans les messages d'audit"

Messages d'audit et cycle de vie de l'objet

Des messages d'audit sont générés à chaque ingestion, récupération ou suppression d'un objet. Vous pouvez identifier ces transactions dans le journal des audits en localisant les messages d'audit spécifiques à l'API (S3 ou Swift).

Les messages d'audit sont liés par des identificateurs spécifiques à chaque protocole.

Protocole	Code
Liaison des opérations S3	S3BK (compartiment S3) et/ou S3KY (clé S3)
Liaison d'opérations Swift	WCON (conteneur Swift) et/ou WOBJ (objet Swift)
Liaison des opérations internes	CBID (identifiant interne de l'objet)

Calendrier des messages d'audit

En raison de facteurs tels que les différences de synchronisation entre les nœuds de la grille, la taille de l'objet et les retards réseau, l'ordre des messages d'audit générés par les différents services peut varier de celui présenté dans les exemples de cette section.

Configuration des règles de gestion du cycle de vie des informations

La règle ILM (2 copie de base) par défaut permet de copier une seule fois les données d'objet, pour un total de deux copies. Si la politique ILM nécessite plus de deux copies, il y aura un jeu supplémentaire de messages CBRE, CBSE et SCMT pour chaque copie supplémentaire. Pour plus d'informations sur les règles ILM, reportez-vous aux informations à propos de la gestion des objets avec la gestion du cycle de vie des informations.

Nœuds d'archivage

La série de messages d'audit générés lorsqu'un nœud d'archivage envoie des données d'objet à un système de stockage d'archives externe est similaire à celle des nœuds de stockage, à l'exception du message SCMT (Store Object commit), Et les messages ATCE (Archive Object Store Begin) et ASCE (Archive Object Store End) sont générés pour chaque copie archivée de données d'objet.

La série de messages d'audit générés lorsqu'un nœud d'archivage récupère des données d'objet à partir d'un système de stockage d'archives externe est similaire à celle des nœuds de stockage, sauf que les messages ARCB (début de la récupération de l'objet d'archivage) et ARCE (fin de la récupération de l'objet d'archivage) sont générés pour chaque copie récupérée des données d'objet.

La série de messages d'audit générés lorsqu'un nœud d'archivage supprime des données d'objet d'un système de stockage d'archives externe est similaire à celle des nœuds de stockage, sauf qu'il n'y a pas de message SREM (Object Store Remove) et qu'il y a un message AREM (Archive Object Remove) pour chaque demande de suppression.

Informations associées

"Gestion des objets avec ILM"

Transactions d'ingestion d'objets

Vous pouvez identifier les transactions d'entrée de clients dans le journal d'audit en localisant les messages d'audit spécifiques aux API (S3 ou Swift).

Tous les messages d'audit générés lors d'une transaction d'entrée ne sont pas répertoriés dans les tableaux suivants. Seuls les messages nécessaires au suivi de la transaction d'acquisition sont inclus.

Ingestion des messages d'audit S3

Code	Nom	Description	Tracé	Voir
SPUT	Transaction PUT S3	Une transaction d'entrée DE PUT S3 a été effectuée avec succès.	CBID, S3BK, S3KY	"SPUT : PUT S3"

Code	Nom	Description	Tracé	Voir
ORLM	Règles d'objet respectées	La politique ILM a été satisfaite pour cet objet.	CBID	"ORLM : règles d'objet respectées"

Ingestion des messages d'audit Swift

Code	Nom	Description	Tracé	Voir
WPUT	EFFECTUER la transaction Swift	Une transaction d'entrée DE PUT Swift a été effectuée avec succès.	CBID, WCON, WOBJ	"WPUT : PUT SWIFT"
ORLM	Règles d'objet respectées	La politique ILM a été satisfaite pour cet objet.	CBID	"ORLM : règles d'objet respectées"

Exemple : ingestion d'objet S3

La série de messages d'audit ci-dessous est un exemple des messages d'audit générés et enregistrés dans le journal d'audit lorsqu'un client S3 ingère un objet à un nœud de stockage (LDR).

Dans cet exemple, la politique ILM active inclut la règle ILM stock, à effectuer 2 copies.

> Tous les messages d'audit générés pendant une transaction ne sont pas répertoriés dans l'exemple ci-dessous. Seules les personnes liées à la transaction de transfert S3 (SPUT) sont répertoriées.

Dans cet exemple, un compartiment S3 a déjà été créé.

SPUT : PUT S3

Le message SPUT est généré pour indiquer qu'une transaction PUT S3 a été émise pour créer un objet dans un compartiment spécifique.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):25771][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"][S3BK(CSTR):"example"]<strong
class="S3KY(CSTR):"testobject-0-
3"">[CBID(UI64):0x8EF52DF8025E63A8]</strong>[CSIZ(UI64):30720][AVER(UI32):
10]<strong
class="ATIM(UI64):150032627859669">[ATYP(FC32):SPUT]</strong>[ANID(UI32):1
2086324][AMID(FC32):S3RQ][ATID(UI64):14399932238768197038]]
```

ORLM : règles d'objet respectées

Le message ORLM indique que la politique ILM a été satisfaite pour cet objet. Le message inclut le CBID de l'objet et le nom de la règle ILM appliquée.

Pour les objets répliqués, le champ EMPLACEMENTS inclut l'ID de nœud LDR et l'ID de volume des emplacements d'objets.

```
2019-07-17T21:18:31.230669[AUDT:
<strong>[CBID(UI64):0x50C4F7AC2BC8EDF7]</strong> [RULE(CSTR):"Make 2
Copies"][STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"0B344E18-98ED-4F22-
A6C8-A93ED68F8D3F"]<strong class="LOCS(CSTR): *"CLDI 12828634
2148730112">[RSLT(FC32):SUCS][AVER(UI32):10] [ATYP(FC32):ORLM]</strong>
[ATIM(UI64):1563398230669][ATID(UI64):15494889725796157557][ANID(UI32):131
00453][AMID(FC32):BCMS]]
```

Pour les objets avec code d'effacement, le champ LOCS inclut l'ID de profil d'effacement et l'ID de groupe de code 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][ATYP(FC32):ORLM][ANID(UI32):12355278][AMI
D(FC32):ILMX][ATID(UI64):41685590464737255 60]]
```

Le champ CHEMIN d'ACCÈS inclut des informations clés et un compartiment S3 ou des informations sur le conteneur Swift et l'objet, selon l'API utilisée.

```
2019-09-15.txt:2018-01-24T13:52:54.131559
[AUDT:[CBID(UI64):0x82704DFA4C9674F4][RULE(CSTR):"Make 2
Copies"][STAT(FC32):DONE][CSIZ(UI64):3145729][UUID(CSTR):"8C1C9CAC-22BB-
4880-9115-
CE604F8CE687"][PATH(CSTR):"frisbee_Bucket1/GridDataTests151683676324774_1_
1vf9d"][LOCS(CSTR):"CLDI 12525468, CLDI
12222978"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1568555574559][ATYP(
FC32):ORLM][ANID(UI32):12525468][AMID(FC32):OBDI][ATID(UI64):3448338865383
69336]]
```

Transactions de suppression d'objet

Vous pouvez identifier les transactions de suppression d'objets dans le journal d'audit en localisant les messages d'audit spécifiques aux API (S3 et Swift).

Tous les messages d'audit générés lors d'une opération de suppression ne sont pas répertoriés dans les tableaux suivants. Seuls les messages requis pour suivre la transaction de suppression sont inclus.

S3 supprime les messages d'audit

Code	Nom	Description	Tracé	Voir
SDEL	Suppression S3	Demande de suppression de l'objet d'un compartiment.	CBID, S3KY	"SDEL : SUPPRESSION S3"

Supprimez les messages d'audit Swift

Code	Nom	Description	Tracé	Voir
WDEL	Suppression Swift	Demande de suppression de l'objet d'un conteneur ou du conteneur.	CBID, WOBJ	"WDEL : SUPPRESSION rapide"

Exemple : suppression d'objet S3

Lorsqu'un client S3 supprime un objet d'un nœud de stockage (service LDR), un message d'audit est généré et enregistré dans le journal des audits.

> Tous les messages d'audit générés lors d'une opération de suppression ne sont pas répertoriés dans l'exemple ci-dessous. Seules les personnes liées à la transaction de suppression S3 (SDEL) sont répertoriées.

SDEL : suppression S3

La suppression d'objet commence lorsque le client envoie une requête DE SUPPRESSION d'objet à un service LDR. Le message contient le compartiment à partir duquel vous souhaitez supprimer l'objet ainsi que la clé S3 de l'objet, qui permet d'identifier l'objet.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):14316][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"] <strong>[S3BK(CSTR):"example"][S3KY(CSTR):"testobject-0-
7"][CBID(UI64):0x339F21C5A6964D89]</strong>
[CSIZ(UI64):30720][AVER(UI32):10][ATIM(UI64):150032627859669]
<strong>[ATYP(FC32):SDEL]</strong>[ANID(UI32):12086324][AMID(FC32):S3RQ][A
TID(UI64):4727861330952970593]]
```

Transactions de récupération d'objet

Vous pouvez identifier les transactions de récupération d'objets dans le journal d'audit en localisant les messages d'audit spécifiques à l'API (S3 et Swift).

Tous les messages d'audit générés lors d'une transaction de récupération ne sont pas répertoriés dans les tableaux suivants. Seuls les messages requis pour suivre la transaction de récupération sont inclus.

Messages d'audit de récupération S3

Code	Nom	Description	Tracé	Voir
SGET	OBTENTION S3	Demande de récupération d'un objet à partir d'un compartiment.	CBID, S3BK, S3KY	"SGET : OBTENEZ S3"

Messages d'audit de récupération Swift

Code	Nom	Description	Tracé	Voir
C'EST PARTI	PROFITEZ-en rapidement	Demande de récupération d'un objet à partir d'un conteneur.	CBID, WCON, WOBJ	"WGET: SWIFT GET"

Exemple : récupération d'objets S3

Lorsqu'un client S3 récupère un objet à partir d'un nœud de stockage (service LDR), un message d'audit est généré et enregistré dans le journal d'audit.

Notez que tous les messages d'audit générés pendant une transaction ne sont pas répertoriés dans l'exemple

ci-dessous. Seules les transactions liées à la transaction de récupération S3 (SGET) sont répertoriées.

SGET : OBTENEZ S3

L'extraction d'objet commence lorsque le client envoie une requête GET Object à un service LDR. Le message contient le compartiment à partir duquel vous pouvez récupérer l'objet ainsi que la clé S3 de l'objet, qui permet d'identifier l'objet.

```
2017-09-20T22:53:08.782605
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):47807][SAIP(IPAD):"10.96.112.26"][S3AI(
CSTR):"43979298178977966408"][SACC(CSTR):"s3-account-
a"][S3AK(CSTR):"SGKHt7GzEcu0yXhFhT_rL5mep4nJt1w75GBh-
O_FEw=="][SUSR(CSTR):"urn:sgws:identity::43979298178977966408:root"][SBAI(
CSTR):"43979298178977966408"][SBAC(CSTR):"s3-account-a"]
[S3BK(CSTR):"bucket-
anonymous"][S3KY(CSTR):"Hello.txt"][CBID(UI64):0x83D70C6F1F662B02][CSIZ(UI
64):12][AVER(UI32):10][ATIM(UI64):1505947988782605][ATYP(FC32):SGET][ANID(
UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):17742374343649889669]]
```

Si la règle de compartiment le permet, un client peut récupérer des objets de façon anonyme ou récupérer des objets à partir d'un compartiment qui est détenu par un autre compte de locataire. Le message d'audit contient des informations sur le compte du propriétaire du compartiment afin que vous puissiez suivre ces demandes anonymes et inter-comptes.

Dans l'exemple suivant, le client envoie une requête GET Object pour un objet stocké dans un compartiment qu'il ne possède pas. Les valeurs de SBAI et SBAC enregistrent l'ID et le nom de compte du propriétaire du compartiment, qui diffèrent de l'ID et du nom du compte du locataire enregistré dans S3AI et SACC.

```
2017-09-20T22:53:15.876415
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):53244][SAIP(IPAD):"10.96.112.26"]
<strong>[S3AI(CSTR):"17915054115450519830"][SACC(CSTR):"s3-account-
b"]</strong>[S3AK(CSTR):"SGKHpoblWlP_kBkqSCbTi754Ls8lBUog67I2LlSiUg=="]<st
rong
class="SUSR(CSTR):"urn:sgws:identity::17915054115450519830:root"">[SBAI(CS
TR):"43979298178977966408"][SBAC(CSTR):"s3-account-
a"]</strong>[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]]
```

Messages de mise à jour des métadonnées

Des messages d'audit sont générés lorsqu'un client S3 met à jour les métadonnées d'un objet.

Messages d'audit de la mise à jour des métadonnées S3

Code	Nom	Description	Tracé	Voir
SUPD	Métadonnées S3 mises à jour	Générées lorsqu'un client S3 met à jour les métadonnées d'un objet ingéré.	CBID, S3KY, HTRH	"SUPD : métadonnées S3 mises à jour"

Exemple : mise à jour des métadonnées S3

L'exemple illustre la réussite d'une transaction permettant de mettre à jour les métadonnées d'un objet S3 existant.

SUPD : mise à jour des métadonnées S3

Le client S3 demande (SUPD) de mettre à jour les métadonnées spécifiées (`x-amz-meta-*`) Pour l'objet S3 (S3KY). Dans cet exemple, les en-têtes de requête sont inclus dans le champ HTRH car ils ont été configurés comme en-tête de protocole d'audit (**Configuration** > **surveillance** > **Audit**).

```
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]]
```

Informations associées

"Modification des niveaux de messages d'audit"

Messages d'audit

Les descriptions détaillées des messages d'audit renvoyés par le système sont

répertoriées dans les sections suivantes. Chaque message d'audit est d'abord répertorié dans un tableau qui regroupe les messages associés en fonction de la classe d'activité que le message représente. Ces regroupements sont utiles à la fois pour comprendre les types d'activités auditées et pour sélectionner le type souhaité de filtrage des messages d'audit.

Les messages d'audit sont également répertoriés par ordre alphabétique par leur code à quatre caractères. Cette liste alphabétique vous permet de trouver des informations sur des messages spécifiques.

Les codes à quatre caractères utilisés dans 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][<stro
ng>ATYP\(FC32\):SYSU</strong>][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(
UI64):9445736326500603516]]
```

Informations associées

"Messages d'audit"

"Modification des niveaux de messages d'audit"

Catégories de messages d'audit

Vous devez connaître les différentes catégories dans lesquelles les messages d'audit sont regroupés. Ces groupes sont organisés en fonction de la classe d'activité que le message représente.

Messages d'audit système

Vous devez connaître les messages d'audit appartenant à la catégorie d'audit système. Il s'agit d'événements liés au système d'audit lui-même, à l'état des nœuds grid, à l'activité des tâches à l'échelle du système (tâches grid) et aux opérations de sauvegarde de service, pour que vous puissiez résoudre les problèmes potentiels.

Code	Titre et description du message	Voir
ECOC	Fragment de données codé d'effacement corrompu : indique qu'un fragment de données codé d'effacement corrompu a été détecté.	"ECOC : fragment de données codé d'effacement corrompu"
EN	Échec de l'authentification de sécurité : une tentative de connexion à l'aide du protocole TLS (transport Layer Security) a échoué.	"ETAF : échec de l'authentification de sécurité"

Code	Titre et description du message	Voir
GNRG	Enregistrement GNDS : service mis à jour ou enregistré des informations sur lui-même dans le système StorageGRID.	"GNRG : enregistrement GNDS"
GNUR	Annulation de l'enregistrement du GNDS : un service s'est désinscrit du système StorageGRID.	"GNUR : non-inscription du GNDS"
GTED	Tâche de grille terminée : le service CMN a terminé le traitement de la tâche de grille.	"GTED : tâche de grille terminée"
GTST	Tâche de grille démarrée : le service CMN a commencé à traiter la tâche de grille.	"GTST : tâche de grille démarrée"
GTSU	Tâche de grille soumise : une tâche de grille a été envoyée au service CMN.	"GTSU : tâche de grille soumise"
IDEL	Suppression initiée de l'ILM : ce message d'audit est généré lorsque l'ILM démarre le processus de suppression d'un objet.	"IDEL : suppression initiée ILM"
LKCU	Nettoyage d'objet écrasé. Ce message d'audit est généré lorsqu'un objet écrasé est automatiquement supprimé pour libérer de l'espace de stockage.	"LKCU : nettoyage d'objet écrasé"
LLST	Emplacement perdu : ce message d'audit est généré en cas de perte d'un emplacement.	"LLST : emplacement perdu"
OLST	Objet perdu : un objet demandé ne peut pas se trouver dans le système StorageGRID.	"OLST : le système a détecté un objet perdu"
ORLM	Règles d'objet respectées : les données d'objet sont stockées comme spécifié par les règles ILM.	"ORLM : règles d'objet respectées"
AJOUTER	Désactivation de l'audit de sécurité : l'enregistrement des messages d'audit a été désactivé.	"SADD : désactivation de l'audit de sécurité"

Code	Titre et description du message	Voir
SADE	Activation de l'audit de sécurité : la journalisation des messages d'audit a été restaurée.	"SADE : activation de l'audit de sécurité"
SVRF	Échec de la vérification du magasin d'objets : échec de la vérification d'un bloc de contenu.	"SVRF : échec de la vérification du magasin d'objets"
SVRU	Vérification du magasin d'objets Inconnu : données d'objet inattendues détectées dans le magasin d'objets.	"SVRU : Vérification du magasin d'objets inconnue"
SYSD	Arrêt du nœud : un arrêt a été demandé.	"SYSD : arrêt du nœud"
SYST	Arrêt du nœud : un service a démarré un arrêt normal.	"SYST : arrêt du nœud"
SYSU	Node Start : service démarré, la nature de l'arrêt précédent est indiquée dans le message.	"SYSU : démarrage du nœud"
VLST	Volume lancé par l'utilisateur perdu : le `/proc/CMSI/Volume_Lost` la commande a été exécutée.	"VLST : perte du volume généré par l'utilisateur"

Informations associées

"LKCU : nettoyage d'objet écrasé"

Messages d'audit du stockage objet

Vous devez connaître les messages d'audit appartenant à la catégorie d'audit du stockage objet. Ce sont des événements liés au stockage et à la gestion des objets dans le système StorageGRID. Il s'agit notamment du stockage objet et des récupérations, des transferts entre nœuds grid et nœuds.

Code	Description	Voir
APCT	Suppression d'archivage à partir du Tier cloud : les données d'objet archivé sont supprimées d'un système de stockage d'archivage externe qui se connecte au StorageGRID via l'API S3.	"APCT : archive Purge à partir du Tier cloud"

Code	Description	Voir
ARCB	Début de la récupération de l'objet d'archive : le service ARC lance la récupération des données d'objet à partir du système de stockage d'archives externe.	"ARCB : début de la récupération de l'objet d'archive"
ARCE	Fin de la récupération de l'objet d'archive : les données de l'objet ont été extraites d'un système de stockage d'archives externe et le service ARC signale l'état de l'opération de récupération.	"ARCE : fin de la récupération de l'objet d'archive"
ARCT	Archivage à partir du Tier cloud : les données d'objet archivé sont récupérées depuis un système de stockage d'archivage externe qui se connecte à StorageGRID via l'API S3.	"ARCT : récupération d'archives depuis Cloud-Tier"
AREM	Suppression de l'objet d'archive : un bloc de contenu a été supprimé avec succès ou sans succès du système de stockage d'archives externe.	"AREM : suppression de l'objet d'archive"
ASCE	Fin du magasin d'objets d'archivage : un bloc de contenu a été écrit dans le système de stockage d'archives externe et le service ARC signale l'état de l'opération d'écriture.	"ASCE : fin du magasin d'objets d'archivage"
ASCT	Tier dans le stockage d'archives : les données d'objet sont stockées dans un système de stockage d'archives externe qui se connecte à StorageGRID via l'API S3.	"ASCT : magasin d'archives, niveau du cloud"
ATCE	Début de l'archive du magasin d'objets : l'écriture d'un bloc de contenu sur un stockage d'archivage externe a commencé.	"ATCE : début du magasin d'objets d'archivage"
AVCC	Archive Valider la configuration du Tier cloud : les paramètres du compte et des compartiments fournis ont été validés avec succès ou non.	"AVCC : validation de la configuration du Tier cloud"

Code	Description	Voir
CBSE	Objet Envoyer fin : l'entité source a terminé une opération de transfert des données nœud-grille vers nœud-grille.	"CBSE : fin de l'envoi de l'objet"
CBRE	Fin de réception de l'objet : l'entité de destination a terminé une opération de transfert des données nœud-grille vers nœud-grille.	"CBRE : fin de la réception de l'objet"
BALAYAGE	Validation d'un magasin d'objets : un bloc de contenu a été entièrement stocké et vérifié, et peut désormais être demandé.	"SCMT : validation du magasin d'objets"
SREM	Suppression du magasin d'objets : un bloc de contenu a été supprimé d'un nœud de grille et ne peut plus être demandé directement.	"SREM : Suppression du magasin d'objets"

Messages d'audit de lecture du client

Les messages d'audit de lecture des clients sont consignés lorsqu'une application client S3 ou Swift demande de récupérer un objet.

Code	Description	Utilisé par	Voir
SGET	S3 GET : log une transaction réussie pour récupérer un objet ou répertorier les objets dans un compartiment. **Remarque :** si la transaction fonctionne sur une sous-ressource, le message d'audit inclura le champ S3SR.	Client S3	"SGET : OBTENEZ S3"
SHEA	TÊTE S3 : consigne une transaction réussie pour vérifier l'existence d'un objet ou d'un compartiment.	Client S3	"SHEA : TÊTE S3"

Code	Description	Utilisé par	Voir
C'EST PARTI	SWIFT GET : log une transaction réussie pour récupérer un objet ou répertorier les objets dans un conteneur.	Client Swift	"WGET: SWIFT GET"
WHEA	SWIFT HEAD : consigne une transaction réussie afin de vérifier l'existence d'un objet ou d'un conteneur.	Client Swift	"WHEA: TÊTE SWIFT"

Écrire des messages d'audit client

Les messages d'audit d'écriture client sont consignés lorsqu'une application client S3 ou Swift demande de créer ou de modifier un objet.

Code	Description	Utilisé par	Voir
OVWR	Remplacement d'objet : consigne une transaction afin de remplacer un objet par un autre.	Clients S3 Clients Swift	"OVWR : remplacement d'objet"
SDEL	SUPPRESSION S3 : journal une transaction réussie pour supprimer un objet ou un compartiment. **Remarque :** si la transaction fonctionne sur une sous-ressource, le message d'audit inclura le champ S3SR.	Client S3	"SDEL : SUPPRESSION S3"
SPR	POST S3 : consigne une transaction réussie pour restaurer un objet à partir du stockage AWS Glacier vers un pool de stockage cloud.	Client S3	"SPO : BORNE S3"

Code	Description	Utilisé par	Voir
SPUT	S3 PUT : enregistre la réussite d'une transaction pour créer un nouvel objet ou un compartiment. **Remarque :** si la transaction fonctionne sur une sous-ressource, le message d'audit inclura le champ S3SR.	Client S3	"SPUT : PUT S3"
SUPD	Métadonnées S3 mises à jour : enregistre une transaction réussie pour mettre à jour les métadonnées d'un objet ou d'un compartiment.	Client S3	"SUPD : métadonnées S3 mises à jour"
WDEL	SUPPRESSION Swift : enregistre une transaction réussie pour supprimer un objet ou un conteneur.	Client Swift	"WDEL : SUPPRESSION rapide"
WPUT	SWIFT PUT : consigne une transaction réussie pour créer un nouvel objet ou conteneur.	Client Swift	"WPUT : PUT SWIFT"

Message d'audit de gestion

La catégorie gestion consigne les requêtes utilisateur dans l'API de gestion.

Code	Titre et description du message	Voir
MGAU	Message d'audit de l'API de gestion : journal des demandes utilisateur.	"MGAU : message d'audit de gestion"

Messages d'audit

Lorsque des événements système se produisent, le système StorageGRID génère des messages d'audit et les enregistre dans le journal d'audit.

APCT : archive Purge à partir du Tier cloud

Ce message est généré lorsque les données d'objet archivé sont supprimées d'un système de stockage d'archives externe qui se connecte à StorageGRID via l'API S3.

Code	Champ	Description
CBID	ID du bloc de contenu	Identifiant unique du bloc de contenu supprimé.
CSIZ	Taille du contenu	Taille de l'objet en octets. Renvoie toujours 0.
RSLT	Code de résultat	Renvoie réussi (CS) ou l'erreur signalée par le back-end.
SUID	Identifiant unique du stockage	Identifiant unique (UUID) du Tier cloud à partir duquel l'objet a été supprimé.

ARCB : début de la récupération de l'objet d'archive

Ce message est généré lorsqu'une demande est faite pour récupérer les données d'objet archivées et que le processus de récupération commence. Les demandes de récupération sont traitées immédiatement, mais peuvent être réorganisées pour améliorer l'efficacité de la récupération à partir de supports linéaires tels que des bandes.

Code	Champ	Description
CBID	ID du bloc de contenu	Identifiant unique du bloc de contenu à extraire du système de stockage d'archives externe.
RSLT	Résultat	Indique le résultat du démarrage du processus de récupération des archives. La valeur actuellement définie est :SUCS : la demande de contenu a été reçue et mise en file d'attente pour récupération.

Ce message d'audit indique l'heure de récupération d'une archive. Il vous permet de faire correspondre le message avec un message de fin D'ARCE correspondant pour déterminer la durée de récupération de l'archive et si l'opération a réussi.

ARCE : fin de la récupération de l'objet d'archive

Ce message est généré lorsqu'une tentative du nœud d'archivage de récupérer des données d'objet à partir d'un système de stockage d'archives externe est terminée. En cas de réussite, le message indique que les données de l'objet demandé ont été entièrement lues à partir de l'emplacement d'archivage et qu'elles ont été vérifiées avec succès. Une fois que les données de l'objet ont été récupérées et vérifiées, elles sont envoyées au service requérant.

Code	Champ	Description
CBID	ID du bloc de contenu	Identifiant unique du bloc de contenu à extraire du système de stockage d'archives externe.
VLID	Identifiant du volume	Identifiant du volume sur lequel les données ont été archivées.si aucun emplacement d'archive n'est trouvé, un ID de volume 0 est renvoyé.
RSLT	Résultat de la récupération	L'état d'achèvement du processus de récupération des archives : • CMC : réussi • VRFL : échec (échec de la vérification de l'objet) • ARUN : échec (système de stockage d'archivage externe indisponible) • ANNUL : échec (opération de récupération annulée) • GERR : échec (erreur générale)

Le fait de faire correspondre ce message au message ARCB correspondant peut indiquer le temps nécessaire à la récupération de l'archive. Ce message indique si la récupération a réussi et, en cas d'échec, la cause de l'échec de récupération du bloc de contenu.

ARCT : récupération d'archives depuis Cloud-Tier

Ce message est généré lorsque les données d'objet archivé sont récupérées depuis un système de stockage d'archives externe qui se connecte à StorageGRID via l'API S3.

Code	Champ	Description
CBID	ID du bloc de contenu	Identifiant unique du bloc de contenu qui a été récupéré.
CSIZ	Taille du contenu	Taille de l'objet en octets. La valeur est précise uniquement pour les résultats des récupération.
RSLT	Code de résultat	Renvoie réussi (CS) ou l'erreur signalée par le back-end.

Code	Champ	Description
SUID	Identifiant unique du stockage	Identificateur unique (UUID) du système de stockage d'archives externe.
TEMPS	Temps	Temps de traitement total de la demande en microsecondes.

AREM : suppression de l'objet d'archive

Le message d'audit de suppression d'objet d'archive indique qu'un bloc de contenu a été supprimé avec succès ou sans succès d'un nœud d'archive. Si le résultat est réussi, le nœud d'archivage a bien informé le système de stockage d'archives externe qu'StorageGRID a libéré un emplacement d'objet. La suppression de l'objet du système de stockage d'archives externe dépend du type de système et de sa configuration.

Code	Champ	Description
CBID	ID du bloc de contenu	Identifiant unique du bloc de contenu à extraire du système de supports d'archivage externe.
VLID	Identifiant du volume	Identificateur du volume sur lequel les données de l'objet ont été archivées.
RSLT	Résultat	L'état d'achèvement du processus de suppression d'archive : • CMC : réussi • ARUN : échec (système de stockage d'archivage externe indisponible) • GERR : échec (erreur générale)

ASCE : fin du magasin d'objets d'archivage

Ce message indique que l'écriture d'un bloc de contenu sur un système de stockage d'archives externe est terminée.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant du bloc de contenu stocké sur le système de stockage d'archives externe.

Code	Champ	Description
VLID	Identifiant du volume	Identifiant unique du volume d'archivage sur lequel les données de l'objet sont écrites.
VREN	Vérification activée	Indique si la vérification est effectuée pour les blocs de contenu. Les valeurs actuellement définies sont : • VENA : la vérification est activée • VDSA : la vérification est désactivée
CLM	Classe de gestion	Chaîne identifiant la classe de gestion TSM à laquelle le bloc de contenu est affecté, le cas échéant.
RSLT	Résultat	Indique le résultat du processus d'archivage. Les valeurs actuellement définies sont : • SUCS : succès (processus d'archivage réussi) • OFFL : échec (archivage hors ligne) • VRFL : échec (échec de la vérification de l'objet) • ARUN : échec (système de stockage d'archivage externe indisponible) • GERR : échec (erreur générale)

Ce message d'audit signifie que le bloc de contenu spécifié a été écrit sur le système de stockage d'archivage externe. Si l'écriture échoue, le résultat fournit des informations de dépannage de base sur l'emplacement de la défaillance. Pour obtenir des informations plus détaillées sur les échecs d'archivage, consultez les attributs du nœud d'archivage dans le système StorageGRID.

ASCT : magasin d'archives, niveau du cloud

Ce message est généré lorsque les données d'objet archivé sont stockées sur un système de stockage d'archives externe qui se connecte à StorageGRID via l'API S3.

Code	Champ	Description
CBID	ID du bloc de contenu	Identifiant unique du bloc de contenu qui a été récupéré.
CSIZ	Taille du contenu	Taille de l'objet en octets.
RSLT	Code de résultat	Renvoie réussi (CS) ou l'erreur signalée par le back-end.
SUID	Identifiant unique du stockage	Identifiant unique (UUID) du Tier cloud sur lequel le contenu a été stocké.
TEMPS	Temps	Temps de traitement total de la demande en microsecondes.

ATCE : début du magasin d'objets d'archivage

Ce message indique que l'écriture d'un bloc de contenu sur un système de stockage d'archivage externe a démarré.

Code	Champ	Description
CBID	ID du bloc de contenu	Identifiant unique du bloc de contenu à archiver.
VLID	Identifiant du volume	L'identifiant unique du volume sur lequel le bloc de contenu est écrit. Si l'opération échoue, un ID de volume 0 est renvoyé.

Code	Champ	Description
RSLT	Résultat	Indique le résultat du transfert du bloc de contenu. Les valeurs actuellement définies sont : • SUC : succès (le bloc de contenu a été enregistré avec succès) • EXIS : ignoré (le bloc de contenu était déjà stocké) • ISFD : échec (espace disque insuffisant) • STER : échec (erreur lors du stockage du CBID) • OFFL : échec (archivage hors ligne) • GERR : échec (erreur générale)

AVCC : validation de la configuration du Tier cloud

Ce message est généré lorsque les paramètres de configuration sont validés pour un type de cible Cloud Tiering - simple Storage Service (S3).

Code	Champ	Description
RSLT	Code de résultat	Renvoie réussi (CS) ou l'erreur signalée par le back-end.
SUID	Identifiant unique du stockage	UUID associé au système de stockage d'archivage externe validé.

CBRB : début de la réception de l'objet

Dans le cadre d'opérations normales, les blocs de contenu sont transférés en continu entre différents nœuds lorsque des données sont accessibles, répliquées et conservées. Lorsque le transfert d'un bloc de contenu d'un nœud à un autre est lancé, ce message est émis par l'entité de destination.

Code	Champ	Description
CNID	Identificateur de connexion	Identifiant unique de la session/connexion nœud à nœud.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu en cours de transfert.
CTDR	Direction de transfert	Indique si le transfert CBID a été initié par Push ou par Pull : PUSH : l'opération de transfert a été demandée par l'entité émettrice. EXTRACTION : l'opération de transfert a été demandée par l'entité destinataire.
CTSR	Entité source	ID de nœud de la source (expéditeur) du transfert CBID.
CTD	Entité de destination	ID de nœud de la destination (récepteur) du transfert CBID.
CTSS	Nombre de séquences de début	Indique le premier nombre de séquences demandé. En cas de réussite, le transfert commence à partir de ce nombre de séquences.
CTE	Nombre de séquences de fin prévu	Indique le dernier nombre de séquences demandé. En cas de réussite, le transfert est considéré comme terminé lorsque ce nombre de séquences a été reçu.
RSLT	Statut de début du transfert	État au moment du démarrage du transfert : CMC : le transfert a démarré avec succès.

Ce message d'audit signifie qu'une opération de transfert de données nœud à nœud a été lancée sur un seul élément de contenu, tel qu'identifié par son identificateur de bloc de contenu. L'opération demande des données de « nombre de séquences de début » à « nombre de séquences de fin attendu ». Les nœuds d'envoi et de réception sont identifiés par leurs ID de nœud. Ces informations peuvent être utilisées pour suivre le flux de données du système et lorsqu'elles sont associées à des messages d'audit de stockage, pour vérifier le nombre de répliques.

CBRE : fin de la réception de l'objet

Lorsque le transfert d'un bloc de contenu d'un nœud à un autre est terminé, ce message est émis par l'entité de destination.

Code	Champ	Description
CNID	Identificateur de connexion	Identifiant unique de la session/connexion nœud à nœud.
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu en cours de transfert.
CTDR	Direction de transfert	Indique si le transfert CBID a été initié par Push ou par Pull : PUSH : l'opération de transfert a été demandée par l'entité émettrice. EXTRACTION : l'opération de transfert a été demandée par l'entité destinataire.
CTSR	Entité source	ID de nœud de la source (expéditeur) du transfert CBID.
CTD	Entité de destination	ID de nœud de la destination (récepteur) du transfert CBID.
CTSS	Nombre de séquences de début	Indique le nombre de séquences sur lesquelles le transfert a démarré.
CTAS	Nombre de séquences de fin réelles	Indique que le dernier nombre de séquences a été transféré avec succès. Si le nombre de séquences de fin réelles est le même que le nombre de séquences de début et que le résultat du transfert n'a pas réussi, aucune donnée n'a été échangée.

Code	Champ	Description
RSLT	Résultat du transfert	Résultat de l'opération de transfert (du point de vue de l'entité émettrice) : SUC : transfert terminé avec succès ; tous les comptes de séquence demandés ont été envoyés. CONL : connexion perdue pendant le transfert CTMO : expiration de la connexion pendant l'établissement ou le transfert UNRE : ID de nœud de destination inaccessible CRPT : transfert terminé en raison de la réception de données corrompues ou non valides (peut indiquer une altération)

Ce message d'audit signifie qu'une opération de transfert des données nœud à nœud est terminée. Si le résultat du transfert a réussi, l'opération a transféré les données de « nombre de séquences de début » à « nombre de séquences de fin réelles ». Les nœuds d'envoi et de réception sont identifiés par leurs ID de nœud. Ces informations peuvent être utilisées pour suivre le flux de données système et pour localiser, tabuler et analyser les erreurs. Lorsqu'il est associé à des messages d'audit du stockage, il peut également être utilisé pour vérifier le nombre de répliques.

CBSB : début de l'envoi de l'objet

Dans le cadre d'opérations normales, les blocs de contenu sont transférés en continu entre différents nœuds lorsque des données sont accessibles, répliquées et conservées. Lorsque le transfert d'un bloc de contenu d'un nœud à un autre est lancé, ce message est émis par l'entité source.

Code	Champ	Description
CNID	Identificateur de connexion	Identifiant unique de la session/connexion nœud à nœud.
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu en cours de transfert.

Code	Champ	Description
CTDR	Direction de transfert	Indique si le transfert CBID a été initié par Push ou par Pull : PUSH : l'opération de transfert a été demandée par l'entité émettrice. EXTRACTION : l'opération de transfert a été demandée par l'entité destinataire.
CTSR	Entité source	ID de nœud de la source (expéditeur) du transfert CBID.
CTD	Entité de destination	ID de nœud de la destination (récepteur) du transfert CBID.
CTSS	Nombre de séquences de début	Indique le premier nombre de séquences demandé. En cas de réussite, le transfert commence à partir de ce nombre de séquences.
CTE	Nombre de séquences de fin prévu	Indique le dernier nombre de séquences demandé. En cas de réussite, le transfert est considéré comme terminé lorsque ce nombre de séquences a été reçu.
RSLT	Statut de début du transfert	État au moment du démarrage du transfert : CMC : le transfert a démarré avec succès.

Ce message d'audit signifie qu'une opération de transfert de données nœud à nœud a été lancée sur un seul élément de contenu, tel qu'identifié par son identificateur de bloc de contenu. L'opération demande des données de « nombre de séquences de début » à « nombre de séquences de fin attendu ». Les nœuds d'envoi et de réception sont identifiés par leurs ID de nœud. Ces informations peuvent être utilisées pour suivre le flux de données du système et lorsqu'elles sont associées à des messages d'audit de stockage, pour vérifier le nombre de répliques.

CBSE : fin de l'envoi de l'objet

Lorsque le transfert d'un bloc de contenu d'un nœud à un autre est terminé, ce message est émis par l'entité source.

Code	Champ	Description
CNID	Identificateur de connexion	Identifiant unique de la session/connexion nœud à nœud.
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu en cours de transfert.
CTDR	Direction de transfert	Indique si le transfert CBID a été initié par Push ou par Pull : PUSH : l'opération de transfert a été demandée par l'entité émettrice. EXTRACTION : l'opération de transfert a été demandée par l'entité destinataire.
CTSR	Entité source	ID de nœud de la source (expéditeur) du transfert CBID.
CTD	Entité de destination	ID de nœud de la destination (récepteur) du transfert CBID.
CTSS	Nombre de séquences de début	Indique le nombre de séquences sur lesquelles le transfert a démarré.
CTAS	Nombre de séquences de fin réelles	Indique que le dernier nombre de séquences a été transféré avec succès. Si le nombre de séquences de fin réelles est le même que le nombre de séquences de début et que le résultat du transfert n'a pas réussi, aucune donnée n'a été échangée.

Code	Champ	Description
RSLT	Résultat du transfert	Résultat de l'opération de transfert (du point de vue de l'entité émettrice) : SUC : transfert terminé avec succès ; tous les comptes de séquence demandés ont été envoyés. CONL : connexion perdue pendant le transfert CTMO : expiration de la connexion pendant l'établissement ou le transfert UNRE : ID de nœud de destination inaccessible CRPT : transfert terminé en raison de la réception de données corrompues ou non valides (peut indiquer une altération)

Ce message d'audit signifie qu'une opération de transfert des données nœud à nœud est terminée. Si le résultat du transfert a réussi, l'opération a transféré les données de « nombre de séquences de début » à « nombre de séquences de fin réelles ». Les nœuds d'envoi et de réception sont identifiés par leurs ID de nœud. Ces informations peuvent être utilisées pour suivre le flux de données système et pour localiser, tabuler et analyser les erreurs. Lorsqu'il est associé à des messages d'audit du stockage, il peut également être utilisé pour vérifier le nombre de répliques.

ECOC : fragment de données codé d'effacement corrompu

Ce message d'audit indique que le système a détecté un fragment de données codé par effacement corrompu.

Code	Champ	Description
VCCO	ID VCS	Nom du VCS contenant le bloc corrompu.
VLID	ID du volume	Volume RangeDB contenant le fragment codé d'effacement corrompu.
CCID	ID de bloc	Identificateur du fragment codé d'effacement corrompu.

Code	Champ	Description
RSLT	Résultat	Ce champ a la valeur 'NONE'. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message particulier. 'AUCUN' est utilisé plutôt que 'UCS' pour que ce message ne soit pas filtré.

ETAF : échec de l'authentification de sécurité

Ce message est généré lorsqu'une tentative de connexion avec TLS (transport Layer Security) a échoué.

Code	Champ	Description
CNID	Identificateur de connexion	Identifiant système unique pour la connexion TCP/IP sur laquelle l'authentification a échoué.
RUID	Identité de l'utilisateur	Identifiant dépendant du service représentant l'identité de l'utilisateur distant.

Code	Champ	Description
RSLT	Code de motif	La raison de l'échec : SCNI : échec de l'établissement de connexion sécurisée. CERM : certificat 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'est pas valide. CSGU : le signataire de certificat était inconnu. UCRM : les informations d'identification de l'utilisateur étaient manquantes. UCRI : les informations d'identification de l'utilisateur étaient incorrectes. UCRU : les informations d'identification de l'utilisateur ont été interdites. TOUT : expiration du délai d'authentification.

Lorsqu'une connexion est établie à un service sécurisé qui utilise TLS, les informations d'identification de l'entité distante sont vérifiées à l'aide du profil TLS et de la logique supplémentaire intégrée au service. Si cette authentification échoue en raison de certificats ou d'informations d'identification non valides, inattendus ou interdits, un message d'audit est consigné. Cela permet de rechercher des tentatives d'accès non autorisées et d'autres problèmes de connexion liés à la sécurité.

Le message peut être dû à une entité distante ayant une configuration incorrecte ou à des tentatives de présentation d'informations d'identification non valides ou interdites au système. Ce message d'audit doit être surveillé pour détecter les tentatives d'accès non autorisé au système.

GNRG : enregistrement GNDS

Le service CMN génère ce message d'audit lorsqu'un service a mis à jour ou enregistré des informations sur lui-même dans le système StorageGRID.

Code	Champ	Description
RSLT	Résultat	Résultat de la demande de mise à jour : • CMC : réussi • SUNV : service non disponible • GERR : autre panne
GNID	ID de nœud	ID de nœud du service qui a lancé la demande de mise à jour.
GNTP	Type de périphérique	Type de périphérique du nœud de grid (par exemple BLDR pour un service LDR).
GNDV	Version du modèle de périphérique	Chaîne identifiant la version du modèle de terminal du nœud de grille dans le bundle DMDL.
GNP	Groupe	Groupe auquel appartient le nœud de la grille (dans le contexte des coûts de lien et du classement des requêtes de service).
GNIA	Adresse IP	Adresse IP du nœud de la grille.

Ce message est généré chaque fois qu'un nœud de la grille met à jour son entrée dans le pack Grid Nodes.

GNUR : non-inscription du GNDS

Le service CMN génère ce message d'audit lorsqu'un service a des informations non enregistrées sur lui-même à partir du système StorageGRID.

Code	Champ	Description
RSLT	Résultat	Résultat de la demande de mise à jour : • CMC : réussi • SUNV : service non disponible • GERR : autre panne
GNID	ID de nœud	ID de nœud du service qui a lancé la demande de mise à jour.

GTED : tâche de grille terminée

Ce message d'audit indique que le service CMN a terminé le traitement de la tâche de grille spécifiée et a déplacé la tâche vers la table Historique. Si le résultat est SUC, ABRT ou ROLF, un message d'audit correspondant à la tâche de grille démarrée sera affiché. Les autres résultats indiquent que le traitement de cette tâche de grille n'a jamais démarré.

Code	Champ	Description
2	ID de tâche	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. Une tâche de grille donnée peut être soumise plusieurs fois. Dans ce cas, le champ ID tâche n'est pas suffisant pour lier de manière unique les messages d'audit soumis, lancés et terminés.
RSLT	Résultat	Résultat de l'état final de la tâche de grille : • SUC : la tâche de grille s'est terminée avec succès. • ABRT : la tâche de grille a été abandonnée sans erreur de retour arrière. • ROLF : la tâche de grille a été abandonnée et n'a pas pu terminer le processus de restauration. • ANNUL : la tâche de grille a été annulée par l'utilisateur avant son démarrage. • EXPR : la tâche de grille a expiré avant son démarrage. • 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 en double.

GTST : tâche de grille démarrée

Ce message d'audit indique que le service CMN a commencé à traiter la tâche de grille spécifiée. Le message d'audit suit immédiatement le message de la tâche de grille soumise pour les tâches de grille initiées par le service interne Grid Task Submission et sélectionnées pour l'activation automatique. Pour les tâches de grille soumises dans la table en attente, ce message est généré lorsque l'utilisateur démarre la tâche de grille.

Code	Champ	Description
2	ID de tâche	Ce champ identifie de manière unique une tâche de grille générée et permet de gérer la tâche tout au long de son cycle de vie. **Remarque :** l'ID de tâche est attribué au moment où une tâche de grille est générée, et non au moment où elle est soumise. Une tâche de grille donnée peut être soumise plusieurs fois. Dans ce cas, le champ ID tâche n'est pas suffisant pour lier de manière unique les messages d'audit soumis, lancés et terminés.
RSLT	Résultat	Résultat. Ce champ n'a qu'une seule valeur : • SUC : la tâche de grille a été démarrée avec succès.

GTSU : tâche de grille soumise

Ce message d'audit indique qu'une tâche de grille a été envoyée au service CMN.

Code	Champ	Description
2	ID de tâche	Identifie de manière unique une tâche de grille générée et permet de gérer la tâche tout au long de son cycle de vie. **Remarque :** l'ID de tâche est attribué au moment où une tâche de grille est générée, et non au moment où elle est soumise. Une tâche de grille donnée peut être soumise plusieurs fois. Dans ce cas, le champ ID tâche n'est pas suffisant pour lier de manière unique les messages d'audit soumis, lancés et terminés.
TTYP	Type de tâche	Type de tâche de grille.
VER	Version de la tâche	Numéro indiquant la version de la tâche de grille.
TDSC	Description de la tâche	Description lisible par l'homme de la tâche de grille.
CUVES	Valide après horodatage	La première fois (UINT64 microsecondes à partir du 1er janvier 1970 - heure UNIX) à laquelle la tâche de grille est valide.
VBTS	Valide avant horodatage	Dernière heure (UINT64 microsecondes à partir du 1er janvier 1970 - heure UNIX) à laquelle la tâche de grille est valide.
TSRC	Source	Source de la tâche : • TXTB : la tâche de grille a été soumise via le système StorageGRID sous forme de bloc de texte signé. • GRILLE : la tâche de grille a été soumise via le service de soumission de tâches Grid interne.

Code	Champ	Description
ACTV	Type d’activation	Type d’activation : • AUTO : la tâche de grille a été soumise pour l’activation automatique. • PEND : la tâche de grille a été envoyée dans la table en attente. C’est la seule possibilité pour la source TXTB.
RSLT	Résultat	Résultat de la soumission : • SUC : la tâche de grille a été envoyée avec succès. • ECHEC : la tâche a été déplacée directement vers la table historique.

IDEL : suppression initiée ILM

Ce message est généré lorsque ILM démarre le processus de suppression d’un objet.

Le message IDEL est généré dans l’une ou l’autre des situations suivantes :

- **Pour les objets dans des compartiments S3 conformes** : ce message est généré lorsque ILM démarre le processus de suppression automatique d’un objet parce que sa période de conservation a expiré (en supposant que le paramètre de suppression automatique est activé et que la conservation légale est désactivée).
- **Pour les objets dans des compartiments S3 non conformes ou des conteneurs Swift**. Ce message est généré lorsque ILM démarre le processus de suppression d’un objet, car aucune instruction de placement dans la politique ILM active ne s’applique actuellement à cet objet.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	CBID de l’objet.
CMPA	Conformité : suppression automatique	Pour les objets des compartiments S3 uniquement. 0 (false) ou 1 (true), indiquant si un objet conforme doit être supprimé automatiquement à la fin de sa période de conservation, à moins que le compartiment ne soit soumis à une conservation légale.

Code	Champ	Description
CMPL	Conformité : obligation légale	Pour les objets des compartiments S3 uniquement. 0 (faux) ou 1 (vrai), indiquant si le godet est actuellement en attente légale.
CMPR	Conformité : période de conservation	Pour les objets des compartiments S3 uniquement. Durée de conservation de l'objet en minutes.
CTME	Conformité : temps d'entrée	Pour les objets des compartiments S3 uniquement. Temps d'ingestion de l'objet. Vous pouvez ajouter la période de conservation en minutes à cette valeur pour déterminer quand l'objet peut être supprimé du compartiment.
DMRM	Supprimer l'ID de version de marqueur	ID de version du marqueur de suppression créé lors de la suppression d'un objet d'un compartiment multiversion. Les opérations sur les compartiments n'incluent pas ce champ.
CSIZ	Taille du contenu	Taille de l'objet en octets.
EMPLACEMENTS	Emplacements	L'emplacement de stockage des données d'objet dans le système StorageGRID. La valeur des EMPLACEMENTS est "" si l'objet n'a pas d'emplacement (par exemple, il a été supprimé). CLEC : pour les objets avec code d'effacement, l'ID du profil de code d'effacement et l'ID du groupe de code d'effacement appliqué aux données de l'objet. CLDI : pour les objets répliqués, l'ID de nœud LDR et l'ID de volume de l'emplacement de l'objet. CLNL : ID de nœud D'ARC de l'emplacement de l'objet si les données de l'objet sont archivées.

Code	Champ	Description
CHEMIN	Compartiment/clé S3 ou ID de conteneur/objet Swift	Le nom du compartiment S3 et la clé S3 ou le nom du conteneur Swift et l'identifiant de l'objet Swift.
RSLT	Résultat	Résultat de l'opération ILM. SUC : l'opération ILM a réussi.
RÈGLE	Libellé de règles	• Si un objet d'un compartiment S3 conforme est supprimé automatiquement car sa période de conservation a expiré, ce champ est vide. • Si l'objet est supprimé car il n'y a plus d'instructions de placement qui s'appliquent actuellement à l'objet, ce champ affiche l'étiquette lisible par l'homme de la dernière règle ILM appliquée à l'objet.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
VSID	ID de version	ID de version de la version spécifique d'un objet qui a été supprimé. Les opérations sur les compartiments et objets dans les compartiments sans version n'incluent pas ce champ.

LKCU : nettoyage d'objet écrasé

Ce message est généré lorsque StorageGRID supprime un objet écrasé qui auparavant requiert un nettoyage pour libérer de l'espace de stockage. Un objet est écrasé lorsqu'un client S3 ou Swift écrit un objet sur un chemin déjà contenant un objet. Le processus de suppression se produit automatiquement et en arrière-plan.

Code	Champ	Description
CSIZ	Taille du contenu	Taille de l'objet en octets.
LTYP	Type de nettoyage	*Usage interne uniquement.*
LUID	UUID d'objet supprimé	Identifiant de l'objet qui a été supprimé.

Code	Champ	Description
CHEMIN	Compartiment/clé S3 ou ID de conteneur/objet Swift	Le nom du compartiment S3 et la clé S3 ou le nom du conteneur Swift et l'identifiant de l'objet Swift.
SEGC	UUID de conteneur	UUID du conteneur pour l'objet segmenté. Cette valeur n'est disponible que si l'objet est segmenté.
UUID	Identifiant unique universel	Identifiant de l'objet qui existe toujours. Cette valeur est disponible uniquement si l'objet n'a pas été supprimé.

LLST : emplacement perdu

Ce message est généré chaque fois qu'un emplacement pour une copie objet (répliquée ou avec code d'effacement) est introuvable.

Code	Champ	Description
BIL	CBID	CBID affecté.
NON	ID de nœud source	ID de nœud sur lequel les emplacements ont été perdus.
UUID	ID universel unique	Identifiant de l'objet affecté dans le système StorageGRID.
ECPR	Profil de codage d'effacement	Pour les données d'objet avec code d'effacement. ID du profil de code d'effacement utilisé.
LTYP	Type d'emplacement	CLDI (Online) : pour les données d'objet répliquées CLEC (en ligne) : pour les données d'objet avec code d'effacement CLNL (Nearline) : pour les données d'objets répliqués archivés

Code	Champ	Description
PCLD	Chemin d'accès à l'objet répliqué	Chemin complet vers l'emplacement du disque des données de l'objet perdu. Renvoyé uniquement lorsque LTYP a une valeur CLDI (c'est-à-dire pour les objets répliqués). Prend la forme `/var/local/rangedb/2/p/13/13/00oJs6X%{h{U)SeUFxE@`
RSLT	Résultat	Toujours AUCUNE. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message. AUCUN n'est utilisé plutôt que LES CMC pour que ce message ne soit pas filtré.
TSRC	Déclenchement de la source	UTILISATEUR : utilisateur déclenché SYST : déclenchement du système

MGAU : message d'audit de gestion

La catégorie gestion consigne les requêtes utilisateur dans l'API de gestion. Chaque requête qui n'est pas une requête GET ou HEAD à l'API consigne une réponse avec le nom d'utilisateur, l'IP et le type de requête à l'API.

Code	Champ	Description
MDIP	Adresse IP de destination	Adresse IP du serveur (destination).
ADNM	Nom de domaine	Nom du domaine hôte.
MPAT	CHEMIN de la demande	Le chemin de la demande.
MPQP	Paramètres de requête	Paramètres de requête pour la demande.

Code	Champ	Description
MBD	Corps de la demande	Le contenu de l'organisme de demande. Lorsque le corps de réponse est enregistré par défaut, le corps de la demande est enregistré dans certains cas lorsque le corps de réponse est vide. Comme les informations suivantes ne sont pas disponibles dans le corps de réponse, elles sont extraites du corps de la demande pour les méthodes SUIVANTES : • Nom d'utilisateur et ID de compte dans **POST Authorise** • Nouvelle configuration de sous-réseaux dans **POST /grid/grid-Networks/update** • Nouveaux serveurs NTP dans **POST /grid/ntp-servers/update** • ID de serveur déclassés dans **POST /grid/serveurs/désaffecter** **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).
MMD	Méthode de demande	La méthode de requête HTTP : • POST • EN • SUPPRIMER • CORRECTIF
MRSC	Code de réponse	Le code de réponse.

Code	Champ	Description
MRSP	Corps de réponse	Le contenu de la réponse (le corps de réponse) est consigné 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	Adresse IP du client (source).
UUUN	URN de l'utilisateur	URN (nom de ressource uniforme) de l'utilisateur qui a envoyé la demande.
RSLT	Résultat	Renvoie réussi (CS) ou l'erreur signalée par le back-end.

OLST : le système a détecté un objet perdu

Ce message est généré lorsque le service DDS ne parvient pas à localiser une copie d'un objet dans le système StorageGRID.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	CBID de l'objet perdu.
NON	ID de nœud	Si disponible, dernier emplacement direct ou nearline connu de l'objet perdu. Il est possible d'avoir uniquement l'ID de nœud sans ID de volume si les informations sur le volume ne sont pas disponibles.
CHEMIN	Compartiment/clé S3 ou ID de conteneur/objet Swift	Si disponible, le nom du compartiment S3 et la clé S3 ou le nom du conteneur Swift et l'identifiant d'objet Swift.
RSLT	Résultat	Ce champ a la valeur AUCUNE. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message. AUCUN n'est utilisé plutôt que LES CMC pour que ce message ne soit pas filtré.

Code	Champ	Description
UUID	ID universel unique	Identificateur de l'objet perdu dans le système StorageGRID.
VOLI	ID du volume	Le cas échéant, l'ID de volume du nœud de stockage ou du nœud d'archivage pour le dernier emplacement connu de l'objet perdu.

ORLM : règles d'objet respectées

Ce message est généré lorsque l'objet est stocké et copié comme spécifié par les règles ILM.

> Le message ORLM n'est pas généré lorsqu'un objet est stocké avec succès par la règle de création de 2 copies par défaut si une autre règle de la stratégie utilise le filtre avancé taille d'objet.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	CBID de l'objet.
CSIZ	Taille du contenu	Taille de l'objet en octets.
EMPLACEMENTS	Emplacements	L'emplacement de stockage des données d'objet dans le système StorageGRID. La valeur des EMPLACEMENTS est "" si l'objet n'a pas d'emplacement (par exemple, il a été supprimé). CLEC : pour les objets avec code d'effacement, l'ID du profil de code d'effacement et l'ID du groupe de code d'effacement appliqué aux données de l'objet. CLDI : pour les objets répliqués, l'ID de nœud LDR et l'ID de volume de l'emplacement de l'objet. CLNL : ID de nœud D'ARC de l'emplacement de l'objet si les données de l'objet sont archivées.
CHEMIN	Compartiment/clé S3 ou ID de conteneur/objet Swift	Le nom du compartiment S3 et la clé S3 ou le nom du conteneur Swift et l'identifiant de l'objet Swift.

Code	Champ	Description
RSLT	Résultat	Résultat de l'opération ILM. SUC : l'opération ILM a réussi.
RÈGLE	Libellé de règles	Étiquette lisible par l'homme donnée à la règle ILM appliquée à cet objet.
SEGC	UUID de conteneur	UUID du conteneur pour l'objet segmenté. Cette valeur n'est disponible que si l'objet est segmenté.
SGCB	CBID conteneur	CBID du conteneur pour l'objet segmenté. Cette valeur n'est disponible que si l'objet est segmenté.
URGENCE	État	État de l'opération ILM. L'OPÉRATION ILM est terminée pour l'objet. DFER: L'objet a été marqué pour une future réévaluation ILM. PRGD : l'objet a été supprimé du système StorageGRID. NLOC : les données d'objet ne sont plus disponibles dans le système StorageGRID. Cet état peut indiquer que toutes les copies des données d'objet sont manquantes ou endommagées.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.

Le message d'audit ORLM peut être émis plusieurs fois pour un seul objet. Par exemple, il est émis chaque fois que l'un des événements suivants a lieu :

- Les règles ILM de l'objet sont satisfaites à jamais.
- Les règles ILM de l'objet sont satisfaites pour cette époque.
- Les règles ILM ont supprimé l'objet.
- Le processus de vérification en arrière-plan détecte qu'une copie des données d'objet répliqué est corrompue. Le système StorageGRID effectue une évaluation ILM pour remplacer l'objet corrompu.

Informations associées

"Transactions d'ingestion d'objets"

"Transactions de suppression d'objet"

OVWR : remplacement d'objet

Ce message est généré lorsqu'une opération externe (client-demandé) provoque le remplacement d'un objet par un autre objet.

Code	Champ	Description
CBID	Identifiant de bloc de contenu (nouveau)	CBID du nouvel objet.
CSIZ	Taille d'objet précédente	Taille, en octets, de l'objet à remplacer.
OCBD	Identifiant de bloc de contenu (précédent)	CBID de l'objet précédent.
UUID	ID universel unique (nouveau)	Identifiant du nouvel objet dans le système StorageGRID.
OUID	ID universel unique (précédent)	Identifiant de l'objet précédent dans le système StorageGRID.
CHEMIN	Chemin d'accès à l'objet S3 ou Swift	Chemin d'accès à l'objet S3 ou Swift utilisé pour le nouvel objet ou le précédent
RSLT	Code de résultat	Résultat de la transaction de remplacement d'objet. Le résultat est toujours : CMC : réussi

SADD : désactivation de l'audit de sécurité

Ce message indique que le service d'origine (ID de nœud) a désactivé la journalisation des messages d'audit ; les messages d'audit ne sont plus collectés ou livrés.

Code	Champ	Description
AETM	Activer la méthode	Méthode utilisée pour désactiver l'audit.
AEUN	Nom d'utilisateur	Nom d'utilisateur qui a exécuté la commande pour désactiver la journalisation d'audit.

Code	Champ	Description
RSLT	Résultat	Ce champ a la valeur AUCUNE. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message. AUCUN n'est utilisé plutôt que LES CMC pour que ce message ne soit pas filtré.

Ce message implique que la journalisation était déjà activée, mais qu'elle a été désactivée. Ces éléments sont généralement utilisés uniquement lors de l'ingestion en bloc afin d'améliorer les performances du système. Suite à l'activité groupée, l'audit est restauré (SADE) et la capacité de désactivation de l'audit est ensuite bloquée de manière permanente.

SADE : activation de l'audit de sécurité

Ce message indique que le service d'origine (ID de nœud) a restauré la journalisation des messages d'audit ; les messages d'audit sont de nouveau collectés et livrés.

Code	Champ	Description
AETM	Activer la méthode	Méthode utilisée pour activer l'audit.
AEUN	Nom d'utilisateur	Nom d'utilisateur qui a exécuté la commande pour activer la journalisation d'audit.
RSLT	Résultat	Ce champ a la valeur AUCUNE. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message. AUCUN n'est utilisé plutôt que LES CMC pour que ce message ne soit pas filtré.

Ce message implique que la consignation a été précédemment désactivée (SADD), mais qu'elle a maintenant été restaurée. Ces éléments sont généralement utilisés uniquement lors de l'ingestion en bloc afin d'améliorer les performances du système. Suite à l'activité groupée, l'audit est restauré et la fonctionnalité de désactivation de l'audit est bloquée définitivement.

SCMT : validation du magasin d'objets

Le contenu de la grille n'est pas disponible ou reconnu comme stocké tant qu'il n'a pas été engagé (c'est-à-dire qu'il a été stocké de manière persistante). Le contenu stocké de manière persistante a été entièrement écrit sur le disque et a transmis des contrôles d'intégrité liés. Ce message est émis lorsqu'un bloc de contenu est attribué au stockage.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu engagé dans le stockage permanent.
RSLT	Code de résultat	Statut au moment où l'objet était stocké sur le disque : SUCS : objet enregistré avec succès.

Ce message signifie qu'un bloc de contenu donné a été complètement stocké et vérifié, et qu'il peut maintenant être demandé. Il peut être utilisé pour suivre le flux de données dans le système.

SDEL : SUPPRESSION S3

Lorsqu'un client S3 émet une transaction DE SUPPRESSION, une requête est formulée pour supprimer l'objet ou le compartiment spécifié. Ce message est émis par le serveur si la transaction a réussi.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les compartiments n'incluent pas ce champ.
CNCH	En-tête de contrôle de cohérence	Valeur de l'en-tête de la requête HTTP de contrôle de cohérence, s'il est présent dans la demande.
CNID	Identificateur de connexion	Identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	Taille de l'objet supprimé en octets. Les opérations sur les compartiments n'incluent pas ce champ.
DMRM	Supprimer l'ID de version de marqueur	ID de version du marqueur de suppression créé lors de la suppression d'un objet d'un compartiment multiversion. Les opérations sur les compartiments n'incluent pas ce champ.

Code	Champ	Description
HTRH	En-tête de requête HTTP	Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration. **Remarque :** `X-Forwarded-For` est automatiquement inclus si elle est présente dans la demande et si `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	Horodatage Unix, en microsecondes, indiquant quand l'objet a été modifié pour la dernière fois.
RSLT	Code de résultat	Résultat de la transaction DE SUPPRESSION. Le résultat est toujours : CMC : réussi
S3AI	ID de compte de locataire S3 (expéditeur de la demande)	ID de compte de locataire de l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3AK	ID de clé d'accès S3 (expéditeur de la demande)	ID de clé d'accès S3 écrasé pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Compartiment S3	Nom du compartiment S3.
S3KY	Clé S3	Le nom de la clé S3 n'inclut pas le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.
S3SR	Sous-ressource S3	Le godet ou la sous-ressource d'objet utilisé, le cas échéant.
CCUA	Nom du compte de locataire S3 (expéditeur de la demande)	Nom du compte de tenant pour l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.

Code	Champ	Description
SAIP	Adresse IP (expéditeur de la demande)	Adresse IP de l'application client qui a fait la demande.
SBAC	Nom de compte de locataire S3 (propriétaire du compartiment)	Nom du compte du locataire pour le propriétaire du compartiment. Permet d'identifier les accès inter-comptes ou anonymes.
SBAI	ID de compte de locataire S3 (propriétaire du compartiment)	ID du compte du locataire du propriétaire du compartiment cible. Permet d'identifier les accès inter-comptes ou anonymes.
SUSR	URN de l'utilisateur S3 (expéditeur de la demande)	L'ID du compte de locataire et le nom d'utilisateur de l'utilisateur qui fait la demande. L'utilisateur peut être un utilisateur local ou LDAP. Par exemple : `urn:sgws:identity::03393893651506583485:root` Vide pour les demandes anonymes.
TEMPS	Temps	Temps de traitement total de la demande en microsecondes.
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
VSID	ID de version	ID de version de la version spécifique d'un objet qui a été supprimé. Les opérations sur les compartiments et objets dans les compartiments sans version n'incluent pas ce champ.

SGET : OBTENEZ S3

Lorsqu'un client S3 émet une transaction GET, une requête est effectuée pour récupérer un objet ou répertorier les objets dans un compartiment. Ce message est émis par le serveur si la transaction a réussi.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les compartiments n'incluent pas ce champ.
CNCH	En-tête de contrôle de cohérence	Valeur de l'en-tête de la requête HTTP de contrôle de cohérence, s'il est présent dans la demande.
CNID	Identificateur de connexion	Identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	Taille de l'objet récupéré en octets. Les opérations sur les compartiments n'incluent pas ce champ.
HTRH	En-tête de requête HTTP	Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration. **Remarque :** `X-Forwarded-For` est automatiquement inclus si elle est présente dans la demande et si `X-Forwarded-For` La valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP).
AU RANG	Plage lue	Pour les opérations de lecture de plage uniquement. Indique la plage d'octets lus par cette demande. La valeur après la barre oblique (/) indique la taille de l'objet entier.
RSLT	Code de résultat	Résultat de la transaction GET. Le résultat est toujours : CMC : réussi
S3AI	ID de compte de locataire S3 (expéditeur de la demande)	ID de compte de locataire de l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.

Code	Champ	Description
S3AK	ID de clé d'accès S3 (expéditeur de la demande)	ID de clé d'accès S3 écrasé pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Compartiment S3	Nom du compartiment S3.
S3KY	Clé S3	Le nom de la clé S3 n'inclut pas le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.
S3SR	Sous-ressource S3	Le godet ou la sous-ressource d'objet utilisé, le cas échéant.
CCUA	Nom du compte de locataire S3 (expéditeur de la demande)	Nom du compte de tenant pour l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SAIP	Adresse IP (expéditeur de la demande)	Adresse IP de l'application client qui a fait la demande.
SBAC	Nom de compte de locataire S3 (propriétaire du compartiment)	Nom du compte du locataire pour le propriétaire du compartiment. Permet d'identifier les accès inter-comptes ou anonymes.
SBAI	ID de compte de locataire S3 (propriétaire du compartiment)	ID du compte du locataire du propriétaire du compartiment cible. Permet d'identifier les accès inter-comptes ou anonymes.
SUSR	URN de l'utilisateur S3 (expéditeur de la demande)	L'ID du compte de locataire et le nom d'utilisateur de l'utilisateur qui fait la demande. L'utilisateur peut être un utilisateur local ou LDAP. Par exemple : `urn:sgws:identity::03393893651506583485:root` Vide pour les demandes anonymes.
TEMPS	Temps	Temps de traitement total de la demande en microsecondes.

Code	Champ	Description
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
VSID	ID de version	ID de version de la version spécifique d'un objet demandé. Les opérations sur les compartiments et objets dans les compartiments sans version n'incluent pas ce champ.

SHEA : TÊTE S3

Lorsqu'un client S3 émet une transaction DE TÊTE, une requête est effectuée afin de vérifier l'existence d'un objet ou d'un compartiment et de récupérer les métadonnées relatives à un objet. Ce message est émis par le serveur si la transaction a réussi.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les compartiments n'incluent pas ce champ.
CNID	Identificateur de connexion	Identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	Taille de l'objet vérifié en octets. Les opérations sur les compartiments n'incluent pas ce champ.

Code	Champ	Description
HTRH	En-tête de requête HTTP	Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration. **Remarque :** `X-Forwarded-For` est automatiquement inclus si elle est présente dans la demande et si `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 : CMC : réussi
S3AI	ID de compte de locataire S3 (expéditeur de la demande)	ID de compte de locataire de l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3AK	ID de clé d'accès S3 (expéditeur de la demande)	ID de clé d'accès S3 écrasé pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Compartiment S3	Nom du compartiment S3.
S3KY	Clé S3	Le nom de la clé S3 n'inclut pas le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.
CCUA	Nom du compte de locataire S3 (expéditeur de la demande)	Nom du compte de tenant pour l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SAIP	Adresse IP (expéditeur de la demande)	Adresse IP de l'application client qui a fait la demande.
SBAC	Nom de compte de locataire S3 (propriétaire du compartiment)	Nom du compte du locataire pour le propriétaire du compartiment. Permet d'identifier les accès inter-comptes ou anonymes.

Code	Champ	Description
SBAI	ID de compte de locataire S3 (propriétaire du compartiment)	ID du compte du locataire du propriétaire du compartiment cible. Permet d'identifier les accès inter-comptes ou anonymes.
SUSR	URN de l'utilisateur S3 (expéditeur de la demande)	L'ID du compte de locataire et le nom d'utilisateur de l'utilisateur qui fait la demande. L'utilisateur peut être un utilisateur local ou LDAP. Par exemple : `urn:sgws:identity::03393893651506583485:root` Vide pour les demandes anonymes.
TEMPS	Temps	Temps de traitement total de la demande en microsecondes.
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
VSID	ID de version	ID de version de la version spécifique d'un objet demandé. Les opérations sur les compartiments et objets dans les compartiments sans version n'incluent pas ce champ.

SPO : BORNE S3

Lorsqu'un client S3 émet une requête DE restauration POST-objet, une requête est envoyée afin de restaurer un objet à partir du stockage AWS Glacier vers un pool de stockage cloud. Ce message est émis par le serveur si la transaction a réussi.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0.

Code	Champ	Description
CNCH	En-tête de contrôle de cohérence	Valeur de l'en-tête de la requête HTTP de contrôle de cohérence, s'il est présent dans la demande.
CNID	Identificateur de connexion	Identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	Taille de l'objet récupéré en octets.
HTRH	En-tête de requête HTTP	Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration. **Remarque :** `X-Forwarded-For` est automatiquement inclus si elle est présente dans la demande et si `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 demande DE restauration POST Object. Le résultat est toujours : CMC : réussi
S3AI	ID de compte de locataire S3 (expéditeur de la demande)	ID de compte de locataire de l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3AK	ID de clé d'accès S3 (expéditeur de la demande)	ID de clé d'accès S3 écrasé pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Compartiment S3	Nom du compartiment S3.
S3KY	Clé S3	Le nom de la clé S3 n'inclut pas le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.
S3SR	Sous-ressource S3	Le godet ou la sous-ressource d'objet utilisé, le cas échéant.

Code	Champ	Description
CCUA	Nom du compte de locataire S3 (expéditeur de la demande)	Nom du compte de tenant pour l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SAIP	Adresse IP (expéditeur de la demande)	Adresse IP de l'application client qui a fait la demande.
SBAC	Nom de compte de locataire S3 (propriétaire du compartiment)	Nom du compte du locataire pour le propriétaire du compartiment. Permet d'identifier les accès inter-comptes ou anonymes.
SBAI	ID de compte de locataire S3 (propriétaire du compartiment)	ID du compte du locataire du propriétaire du compartiment cible. Permet d'identifier les accès inter-comptes ou anonymes.
SFCF	Configuration des sous-ressources	Informations sur la restauration.
SUSR	URN de l'utilisateur S3 (expéditeur de la demande)	L'ID du compte de locataire et le nom d'utilisateur de l'utilisateur qui fait la demande. L'utilisateur peut être un utilisateur local ou LDAP. Par exemple : `urn:sgws:identity::03393893651506583485:root` Vide pour les demandes anonymes.
TEMPS	Temps	Temps de traitement total de la demande en microsecondes.
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
VSID	ID de version	ID de version de la version spécifique d'un objet demandé. Les opérations sur les compartiments et objets dans les compartiments sans version n'incluent pas ce champ.

SPUT : PUT S3

Lorsqu'un client S3 émet une transaction PUT, une requête est formulée pour créer un nouvel objet ou un compartiment. Ce message est émis par le serveur si la transaction a réussi.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les compartiments n'incluent pas ce champ.
CMPS	Paramètres de conformité	Les paramètres de conformité utilisés lors de la création du compartiment, s'ils sont présents dans la demande PUT Bucket (tronquée aux 1024 premiers caractères)
CNCH	En-tête de contrôle de cohérence	Valeur de l'en-tête de la requête HTTP de contrôle de cohérence, s'il est présent dans la demande.
CNID	Identificateur de connexion	Identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	Taille de l'objet récupéré en octets. Les opérations sur les compartiments n'incluent pas ce champ.
HTRH	En-tête de requête HTTP	Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration. **Remarque :** `X-Forwarded-For` est automatiquement inclus si elle est présente dans la demande et si `X-Forwarded-For` La valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP).
LKEN	Verrouillage d'objet activé	Valeur de l'en-tête de demande `x-amz-bucket-object-lock-enabled`, Si présent dans la demande de godet PUT.

Code	Champ	Description
LKLH	Verrouillage de l'objet en attente légale	Valeur de l'en-tête de demande `x-amz-object-lock-legal-hold`, S'il est présent dans la demande D'objet PUT.
LKMD	Mode de conservation du verrouillage d'objet	Valeur de l'en-tête de demande `x-amz-object-lock-mode`, S'il est présent dans la demande D'objet PUT.
LKRU	Conservation de l'objet jusqu'à la date	Valeur de l'en-tête de demande `x-amz-object-lock-retain-until-date`, S'il est présent dans la demande D'objet PUT.
MTME	Heure de la dernière modification	Horodatage Unix, en microsecondes, indiquant quand l'objet a été modifié pour la dernière fois.
RSLT	Code de résultat	Résultat de la transaction PUT. Le résultat est toujours : CMC : réussi
S3AI	ID de compte de locataire S3 (expéditeur de la demande)	ID de compte de locataire de l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3AK	ID de clé d'accès S3 (expéditeur de la demande)	ID de clé d'accès S3 écrasé pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Compartiment S3	Nom du compartiment S3.
S3KY	S3KY	Le nom de la clé S3 n'inclut pas le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.
S3SR	Sous-ressource S3	Le godet ou la sous-ressource d'objet utilisé, le cas échéant.

Code	Champ	Description
CCUA	Nom du compte de locataire S3 (expéditeur de la demande)	Nom du compte de tenant pour l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SAIP	Adresse IP (expéditeur de la demande)	Adresse IP de l'application client qui a fait la demande.
SBAC	Nom de compte de locataire S3 (propriétaire du compartiment)	Nom du compte du locataire pour le propriétaire du compartiment. Permet d'identifier les accès inter-comptes ou anonymes.
SBAI	ID de compte de locataire S3 (propriétaire du compartiment)	ID du compte du locataire du propriétaire du compartiment cible. Permet d'identifier les accès inter-comptes ou anonymes.
SFCF	Configuration des sous-ressources	La nouvelle configuration de sous-ressource (tronquée aux 1024 premiers caractères).
SUSR	URN de l'utilisateur S3 (expéditeur de la demande)	L'ID du compte de locataire et le nom d'utilisateur de l'utilisateur qui fait la demande. L'utilisateur peut être un utilisateur local ou LDAP. Par exemple : `urn:sgws:identity::03393893651506583485:root` Vide pour les demandes anonymes.
TEMPS	Temps	Temps de traitement total de la demande en microsecondes.
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
ID ULID	ID de téléchargement	Inclus uniquement dans les messages SPUT pour les opérations de téléchargement multipièces complètes. Indique que toutes les pièces ont été téléchargées et assemblées.

Code	Champ	Description
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
VSID	ID de version	L'ID de version d'un nouvel objet créé dans un compartiment multiversion. Les opérations sur les compartiments et objets dans les compartiments sans version n'incluent pas ce champ.
VSST	Etat de gestion des versions	Nouvel état de gestion des versions d'un compartiment. Deux États sont utilisés : « activé » ou « suspendu ». Les opérations sur les objets n'incluent pas ce champ.

SREM : Suppression du magasin d'objets

Ce message est émis lorsque le contenu est supprimé du stockage persistant et n'est plus accessible via des API régulières.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu supprimé du stockage permanent.
RSLT	Code de résultat	Indique le résultat des opérations de suppression de contenu. La seule valeur définie est : SUCS : contenu supprimé du stockage persistant

Ce message d'audit signifie qu'un bloc de contenu donné a été supprimé d'un nœud et ne peut plus être demandé directement. Le message peut être utilisé pour suivre le flux de contenu supprimé dans le système.

SUPD : métadonnées S3 mises à jour

Ce message est généré par l'API S3 lorsqu'un client S3 met à jour les métadonnées pour un objet ingéré. Le message est émis par le serveur si la mise à jour des métadonnées a réussi.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les compartiments n'incluent pas ce champ.
CNCH	En-tête de contrôle de cohérence	Valeur de l'en-tête de requête HTTP de contrôle de cohérence, s'il est présent dans la demande, lors de la mise à jour des paramètres de conformité d'un compartiment.
CNID	Identificateur de connexion	Identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	Taille de l'objet récupéré en octets. Les opérations sur les compartiments n'incluent pas ce champ.
HTRH	En-tête de requête HTTP	Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration. **Remarque :** `X-Forwarded-For` est automatiquement inclus si elle est présente dans la demande et si `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 : CMC : réussi
S3AI	ID de compte de locataire S3 (expéditeur de la demande)	ID de compte de locataire de l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3AK	ID de clé d'accès S3 (expéditeur de la demande)	ID de clé d'accès S3 écrasé pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.

Code	Champ	Description
S3BK	Compartiment S3	Nom du compartiment S3.
S3KY	Clé S3	Le nom de la clé S3 n'inclut pas le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.
CCUA	Nom du compte de locataire S3 (expéditeur de la demande)	Nom du compte de tenant pour l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SAIP	Adresse IP (expéditeur de la demande)	Adresse IP de l'application client qui a fait la demande.
SBAC	Nom de compte de locataire S3 (propriétaire du compartiment)	Nom du compte du locataire pour le propriétaire du compartiment. Permet d'identifier les accès inter-comptes ou anonymes.
SBAI	ID de compte de locataire S3 (propriétaire du compartiment)	ID du compte du locataire du propriétaire du compartiment cible. Permet d'identifier les accès inter-comptes ou anonymes.
SUSR	URN de l'utilisateur S3 (expéditeur de la demande)	L'ID du compte de locataire et le nom d'utilisateur de l'utilisateur qui fait la demande. L'utilisateur peut être un utilisateur local ou LDAP. Par exemple : `urn:sgws:identity::03393893651506583485:root` Vide pour les demandes anonymes.
TEMPS	Temps	Temps de traitement total de la demande en microsecondes.
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.

Code	Champ	Description
VSID	ID de version	ID de version de la version spécifique d'un objet dont les métadonnées ont été mises à jour. Les opérations sur les compartiments et objets dans les compartiments sans version n'incluent pas ce champ.

SVRF : échec de la vérification du magasin d'objets

Ce message est émis chaque fois qu'un bloc de contenu échoue au processus de vérification. Chaque fois que les données d'objet répliqué sont lues ou écrites sur le disque, plusieurs vérifications et vérifications d'intégrité sont effectuées pour s'assurer que les données envoyées à l'utilisateur requérant sont identiques aux données initialement ingérées sur le système. Si l'une de ces vérifications échoue, le système met automatiquement en quarantaine les données d'objet répliqué corrompues pour les empêcher d'être récupérées à nouveau.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu qui a échoué à la vérification.
RSLT	Code de résultat	Type d'échec de vérification : CRCF : échec du contrôle de redondance cyclique (CRC). HMAC : échec de la vérification du code d'authentification du message basé sur le hachage (HMAC). EHSH : hachage de contenu crypté inattendu. PHSH : hachage de contenu original inattendu. SEQC : séquence de données incorrecte sur le disque. PERR : structure non valide du fichier de disque. DERR : erreur disque. FNAM : nom de fichier incorrect.

Remarque : ce message devrait être suivi de près. Les échecs de vérification du contenu peuvent indiquer des tentatives d'altération du contenu ou des pannes matérielles imminentes.

Pour déterminer quelle opération a déclenché le message, reportez-vous à la valeur du champ ID du module. Par exemple, une valeur SVFY indique que le message a été généré par le module Storage Verifier, c'est-à-dire la vérification en arrière-plan et STOR indique que le message a été déclenché par la récupération du contenu.

SVRU : Vérification du magasin d'objets inconnue

Le composant de stockage du service LDR analyse en continu toutes les copies des données objet répliquées dans le magasin d'objets. Ce message est émis lorsqu'une copie inconnue ou inattendue des données d'objet répliqué est détectée dans le magasin d'objets et déplacée vers le répertoire de quarantaine.

Code	Champ	Description
FPTH	Chemin du fichier	Chemin du fichier de la copie d'objet inattendue.
RSLT	Résultat	Ce champ a la valeur 'NONE'. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message. 'AUCUN' est utilisé plutôt que 'UCS' pour que ce message ne soit pas filtré.

Remarque : le message d'audit SVRU : Vérification du magasin d'objets Inconnu doit être étroitement surveillé. Cela signifie que des copies inattendues de données 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 tentatives d'altération du contenu ou des défaillances matérielles imminentes.

SYSD : arrêt du nœud

Lorsqu'un service est arrêté avec élégance, ce message est généré pour indiquer que l'arrêt a été demandé. En général, ce message n'est envoyé qu'après un redémarrage ultérieur, car la file d'attente des messages d'audit n'est pas effacée avant l'arrêt. Recherchez le message SYST, envoyé au début de la séquence d'arrêt, si le service n'a pas redémarré.

Code	Champ	Description
RSLT	Nettoyer l'arrêt	La nature de l'arrêt : SUCS : le système s'est arrêté correctement.

Le message n'indique pas si le serveur hôte est arrêté, seul le service de génération de rapports. Le RSLT d'un système SYSD ne peut pas indiquer un arrêt "non planifié", car le message est généré uniquement par des arrêts "propres".

SYST : arrêt du nœud

Lorsqu'un service est correctement arrêté, ce message est généré pour indiquer que l'arrêt a été demandé et que le service a lancé sa séquence d'arrêt. SYST peut être utilisé pour déterminer si l'arrêt a été demandé, avant le redémarrage du service (contrairement à SYSD, qui est généralement envoyé après le redémarrage du service).

Code	Champ	Description
RSLT	Nettoyer l'arrêt	La nature de l'arrêt : SUCS : le système s'est arrêté correctement.

Le message n'indique pas si le serveur hôte est arrêté, seul le service de génération de rapports. Le code RSLT d'un message SYST ne peut pas indiquer un arrêt « non planifié », car le message n'est généré que par des arrêts « propres ».

SYSU : démarrage du nœud

Lors du redémarrage d'un service, ce message est généré pour indiquer si l'arrêt précédent était propre (commandé) ou désordonné (inattendu).

Code	Champ	Description
RSLT	Nettoyer l'arrêt	La nature de l'arrêt : SUCS : le système a été arrêté proprement. DSDN : le système n'a pas été arrêté complètement. VRGN : le système a été démarré pour la première fois après l'installation du serveur (ou la réinstallation).

Le message n'indique pas si le serveur hôte a été démarré, seul le service de génération de rapports. Ce message peut être utilisé pour :

- Détecter la discontinuité dans la piste d'audit.
- Déterminez si un service échoue pendant le fonctionnement (étant donné que la nature distribuée du système StorageGRID peut masquer ces défaillances). Server Manager redémarre automatiquement un service en panne.

VLST : perte du volume généré par l'utilisateur

Ce message est émis chaque fois que le `/proc/CMSI/Volume_Lost` la commande est exécutée.

Code	Champ	Description
VOL	Identificateur de volume inférieur	L'extrémité inférieure de la plage de volumes affectés ou un seul volume.
LU	Identificateur de volume supérieur	L'extrémité supérieure de la plage de volume affectée. Égal à VOLL si un seul volume.
NON	ID de nœud source	ID de nœud sur lequel les emplacements ont été perdus.
LTYP	Type d'emplacement	'CLDI' (en ligne) ou 'CLNL' (Nearline). Si ce n'est pas le cas, la valeur par défaut est « CLDI ».
RSLT	Résultat	Toujours 'AUCUN'. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message. 'AUCUN' est utilisé plutôt que 'UCS' pour que ce message ne soit pas filtré.

WDEL : SUPPRESSION rapide

Lorsqu'un client Swift émet une transaction DE SUPPRESSION, une demande est faite pour supprimer l'objet ou le conteneur spécifié. Ce message est émis par le serveur si la transaction a réussi.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les conteneurs n'incluent pas ce champ.
CSIZ	Taille du contenu	Taille de l'objet supprimé en octets. Les opérations sur les conteneurs n'incluent pas ce champ.

Code	Champ	Description
HTRH	En-tête de requête HTTP	Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration. **Remarque :** `X-Forwarded-For` est automatiquement inclus si elle est présente dans la demande et si `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	Horodatage Unix, en microsecondes, indiquant quand l'objet a été modifié pour la dernière fois.
RSLT	Code de résultat	Résultat de la transaction DE SUPPRESSION. Le résultat est toujours : CMC : réussi
SAIP	Adresse IP du client requérant	Adresse IP de l'application client qui a fait la demande.
TEMPS	Temps	Temps de traitement total de la demande en microsecondes.
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
WACC	ID de compte Swift	ID de compte unique tel que spécifié par le système StorageGRID.
CONEM	Conteneur Swift	Nom du conteneur Swift.
WOBJ	Objet Swift	Identifiant de l'objet Swift. Les opérations sur les conteneurs n'incluent pas ce champ.

Code	Champ	Description
WUSR	Utilisateur du compte Swift	Nom d'utilisateur du compte Swift qui identifie de manière unique le client effectuant la transaction.

WGET: SWIFT GET

Lorsqu'un client Swift émet une transaction GET, une demande est faite pour récupérer un objet, répertorier les objets dans un conteneur ou répertorier les conteneurs dans un compte. Ce message est émis par le serveur si la transaction a réussi.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les comptes et les conteneurs n'incluent pas ce champ.
CSIZ	Taille du contenu	Taille de l'objet récupéré en octets. Les opérations sur les comptes et les conteneurs n'incluent pas ce champ.
HTRH	En-tête de requête HTTP	Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration. **Remarque :** `X-Forwarded-For` est automatiquement inclus si elle est présente dans la demande et si `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 CMC : réussi
SAIP	Adresse IP du client requérant	Adresse IP de l'application client qui a fait la demande.
TEMPS	Temps	Temps de traitement total de la demande en microsecondes.

Code	Champ	Description
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
WACC	ID de compte Swift	ID de compte unique tel que spécifié par le système StorageGRID.
CONEM	Conteneur Swift	Nom du conteneur Swift. Les opérations sur les comptes n'incluent pas ce champ.
WOBJ	Objet Swift	Identifiant de l'objet Swift. Les opérations sur les comptes et les conteneurs n'incluent pas ce champ.
WUSR	Utilisateur du compte Swift	Nom d'utilisateur du compte Swift qui identifie de manière unique le client effectuant la transaction.

WHEA: TÊTE SWIFT

Lorsqu'un client Swift émet une transaction DE TÊTE, une demande est faite pour vérifier l'existence d'un compte, d'un conteneur ou d'un objet, et pour récupérer toutes les métadonnées pertinentes. Ce message est émis par le serveur si la transaction a réussi.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les comptes et les conteneurs n'incluent pas ce champ.
CSIZ	Taille du contenu	Taille de l'objet récupéré en octets. Les opérations sur les comptes et les conteneurs n'incluent pas ce champ.

Code	Champ	Description
HTRH	En-tête de requête HTTP	Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration. **Remarque :** `X-Forwarded-For` est automatiquement inclus si elle est présente dans la demande et si `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 DE TÊTE. Le résultat est toujours : CMC : réussi
SAIP	Adresse IP du client requérant	Adresse IP de l'application client qui a fait la demande.
TEMPS	Temps	Temps de traitement total de la demande en microsecondes.
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
WACC	ID de compte Swift	ID de compte unique tel que spécifié par le système StorageGRID.
CONEM	Conteneur Swift	Nom du conteneur Swift. Les opérations sur les comptes n'incluent pas ce champ.
WOBJ	Objet Swift	Identifiant de l'objet Swift. Les opérations sur les comptes et les conteneurs n'incluent pas ce champ.
WUSR	Utilisateur du compte Swift	Nom d'utilisateur du compte Swift qui identifie de manière unique le client effectuant la transaction.

WPUT : PUT SWIFT

Lorsqu'un client Swift émet une transaction PUT, une demande est faite pour créer un objet ou un conteneur. Ce message est émis par le serveur si la transaction a réussi.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les conteneurs n'incluent pas ce champ.
CSIZ	Taille du contenu	Taille de l'objet récupéré en octets. Les opérations sur les conteneurs n'incluent pas ce champ.
HTRH	En-tête de requête HTTP	Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration. **Remarque :** `X-Forwarded-For` est automatiquement inclus si elle est présente dans la demande et si `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	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 : CMC : réussi
SAIP	Adresse IP du client requérant	Adresse IP de l'application client qui a fait la demande.
TEMPS	Temps	Temps de traitement total de la demande en microsecondes.
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.

Code	Champ	Description
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
WACC	ID de compte Swift	ID de compte unique tel que spécifié par le système StorageGRID.
CONEM	Conteneur Swift	Nom du conteneur Swift.
WOBJ	Objet Swift	Identifiant de l'objet Swift. Les opérations sur les conteneurs n'incluent pas ce champ.
WUSR	Utilisateur du compte Swift	Nom d'utilisateur du compte Swift qui identifie de manière unique le client effectuant la transaction.

Informations sur le copyright

Copyright © 2025 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

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

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

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site http://www.netapp.com/TM sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.