Dépanner un système StorageGRID

StorageGRID

NetApp
October 03, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/storagegrid-115/troubleshoot/verifying-object-integrity.html on October 03, 2025. Always check docs.netapp.com for the latest.

Sommaire

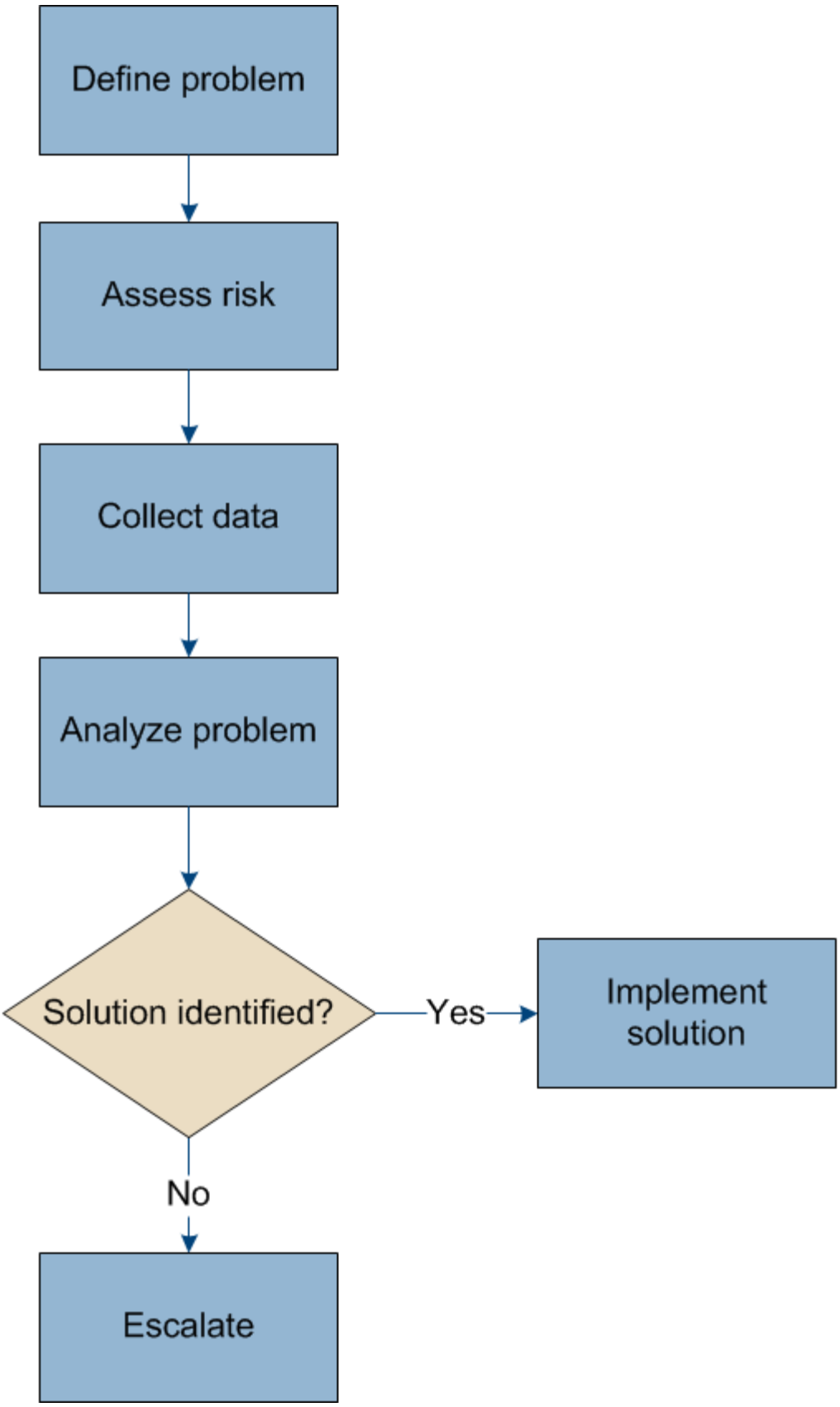
Dépanner un système StorageGRID . . . 1
Présentation de la détection des problèmes . . . 1
Définition du problème . . . 2
Évaluation du risque et de l'impact sur le système . . . 3
Collecte des données . . . 4
Analyse des données . . . 8
Liste de contrôle des informations de réaffectation . . . 8
Résolution des problèmes d'objet et de stockage . . . 10
Confirmation de l'emplacement des données d'objet . . . 10
Défaillances de stockage d'objets (volume de stockage) . . . 12
Vérification de l'intégrité des objets . . . 14
Dépannage des données d'objet perdues ou manquantes . . . 21
Dépannage de l'alerte de stockage de données d'objet faible . . . 34
Dépannage de l'alarme Storage Status (SSTS) . . . 36
Résolution des problèmes de transmission des messages des services de plate-forme (alarme SMTT) 41
Résolution des problèmes de métadonnées . . . 42
Dépannage de l'alerte de stockage de métadonnées faible . . . 42
Dépannage de l'alarme Services : état - Cassandra (SVST) . . . 44
Dépannage des erreurs de mémoire Cassandra (alarme SMTT) . . . 48
Dépannage des erreurs de certificat . . . 49
Résolution des problèmes liés au nœud d'administration et à l'interface utilisateur . . . 51
Dépannage des erreurs de connexion . . . 51
Résolution des problèmes liés à l'interface utilisateur . . . 54
Vérification de l'état d'un nœud d'administration non disponible . . . 55
Résolution des problèmes de réseau, de matériel et de plate-forme . . . 56
Dépannage des erreurs « 422: Entité impossible à traiter » . . . 56
Dépannage de l'alerte de non-concordance de MTU du réseau Grid . . . 57
Dépannage de l'alarme d'erreur de réception réseau (NRER) . . . 59
Dépannage des erreurs de synchronisation de l'heure . . . 61
Linux : problèmes de connectivité réseau . . . 61
Linux : l'état du nœud est « orphelin » . . . 62
Linux : dépannage de la prise en charge IPv6 . . . 62

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

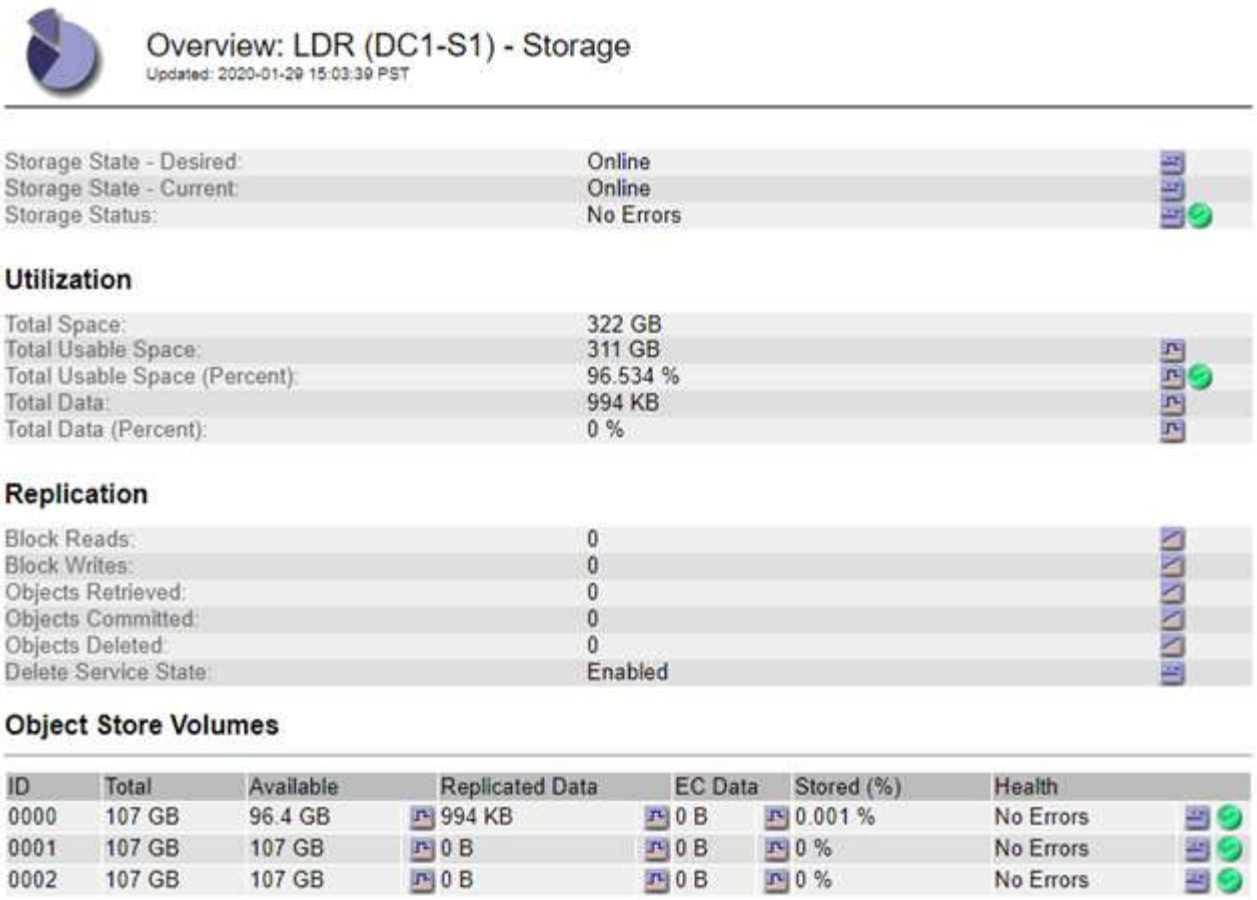
Mount Point	Device	Status	Size	Available	Write Cache Status
/	croot	Online	21.00 GB	14.25 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.39 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sds	Online	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 :

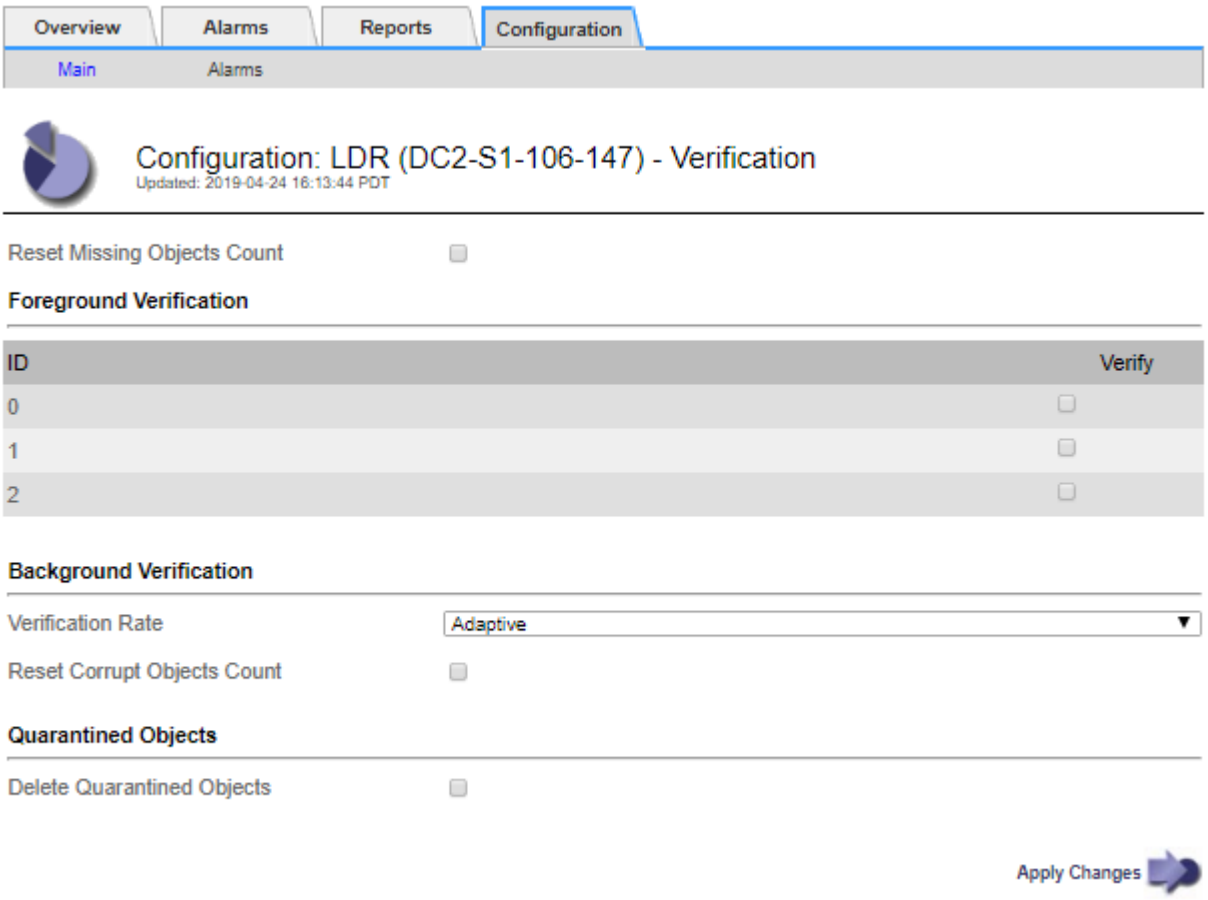
- Adaptatif : paramètre par défaut. La tâche est conçue pour vérifier à un maximum de 4 Mo/s ou 10 objets/s (selon la première limite dépassée).

- 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.

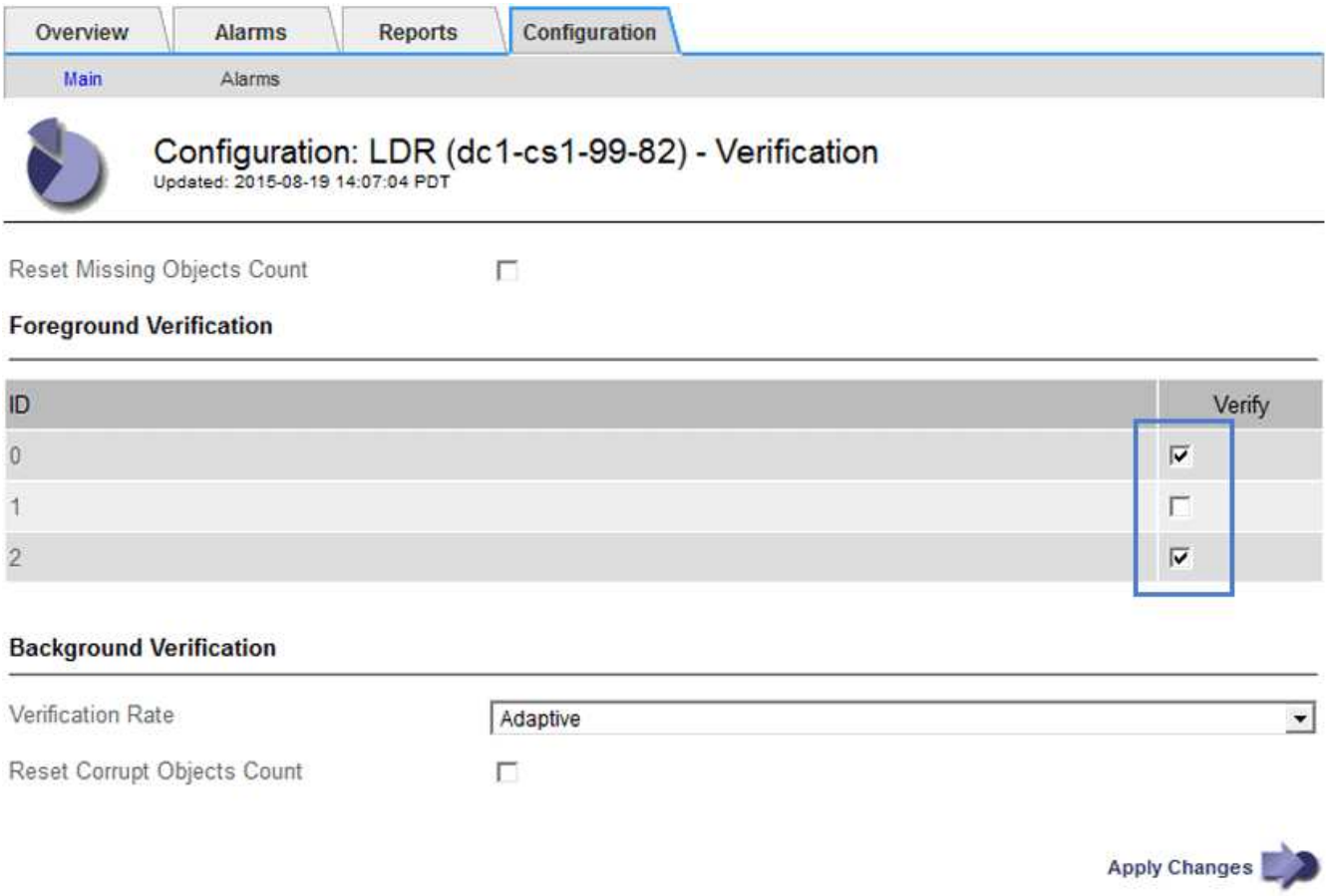
Si la vérification au premier plan trouve des données d'objet manquantes, le système StorageGRID tente de les remplacer. Si une copie de remplacement ne peut pas être effectuée, l'alarme OBJETS PERDUS peut être déclenchée.

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.

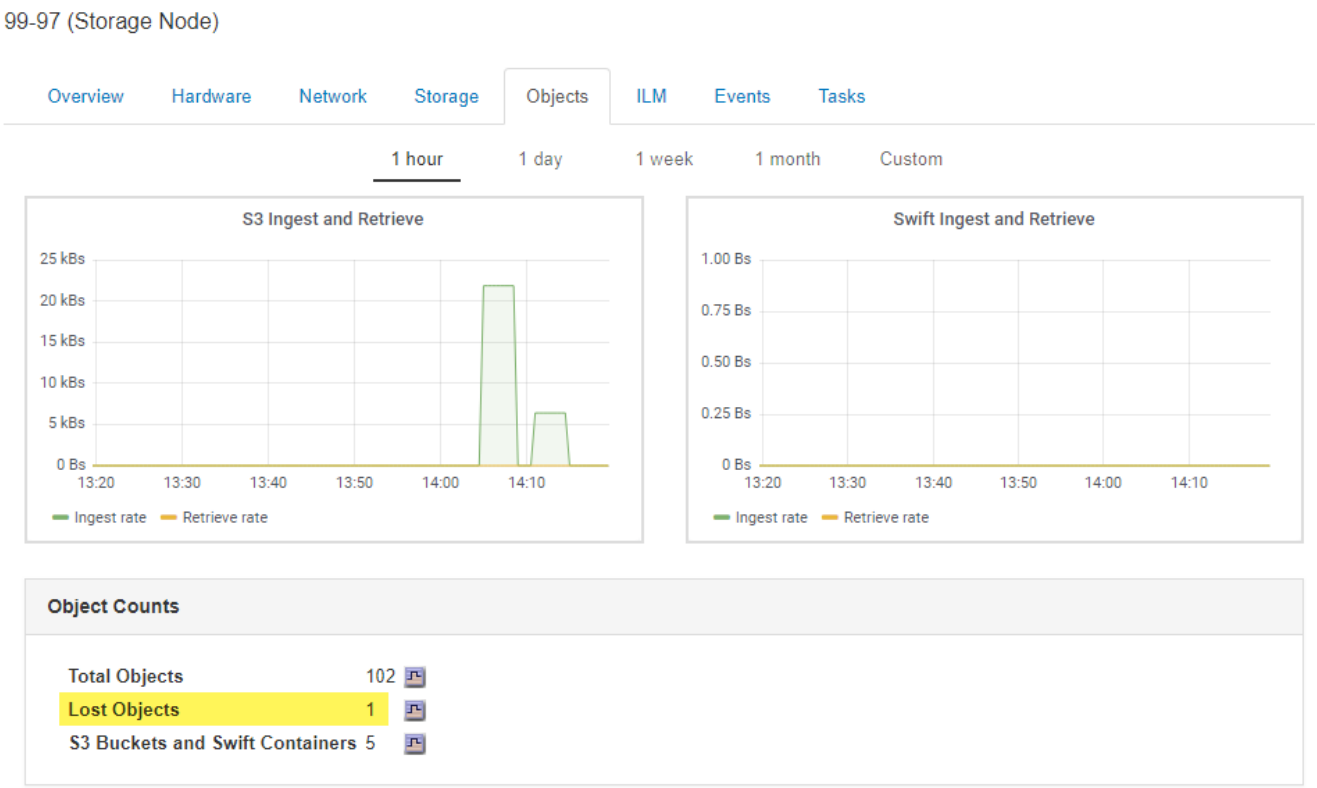
Recherchez immédiatement les alarmes ou les alertes relatives aux objets perdus. Vous devrez peut-être prendre des mesures pour éviter d'autres pertes de données. Dans certains cas, vous pourrez peut-être restaurer un objet perdu si vous prenez une action d'invite.

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 :

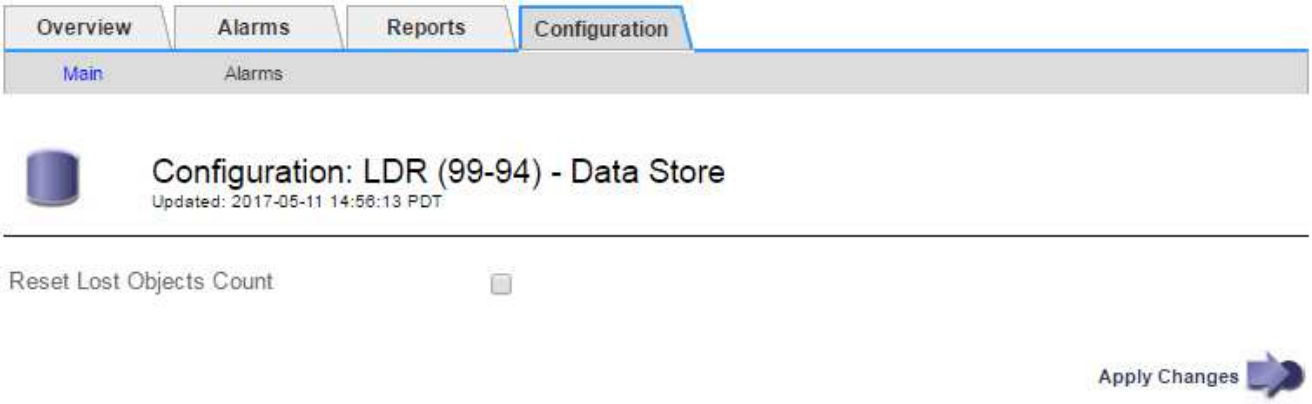
- **Support** > **Outils** > **topologie de grille** > ***site*** **>** ***nœud de stockage*** > **LDR** > **Data Store** > **Présentation** > **main**
- **Support** > **Outils** > **topologie de grille** > ***site*** **>** ***nœud de stockage*** > **DDS** > **Data Store** > **Présentation** > **main**

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.

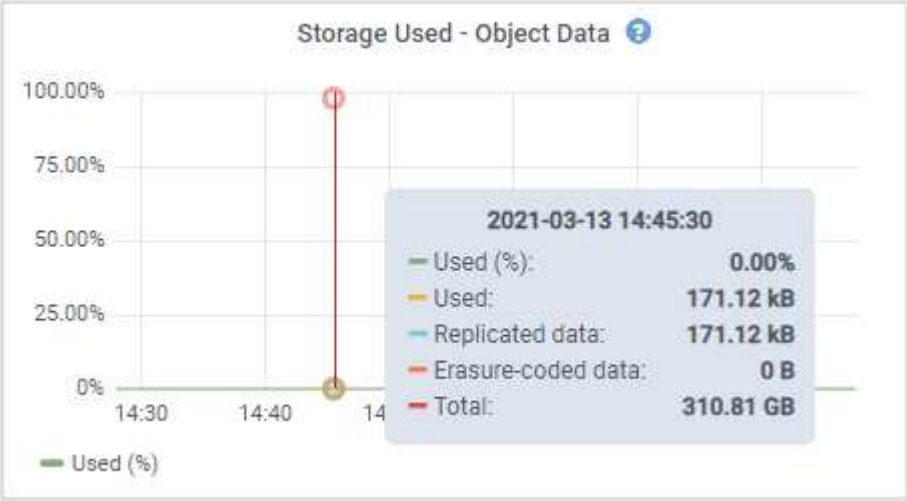
3. Vérifiez les détails dans la boîte de dialogue et notez ce qui suit :
   - Temps déclenché
   - Le nom du site et du noeud
   - Valeurs actuelles des mesures de cette alerte
4. Sélectionnez **Nodes** > ***Storage Node ou site*** > **Storage**.
5. Placez le curseur de la souris sur le graphique stockage 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)

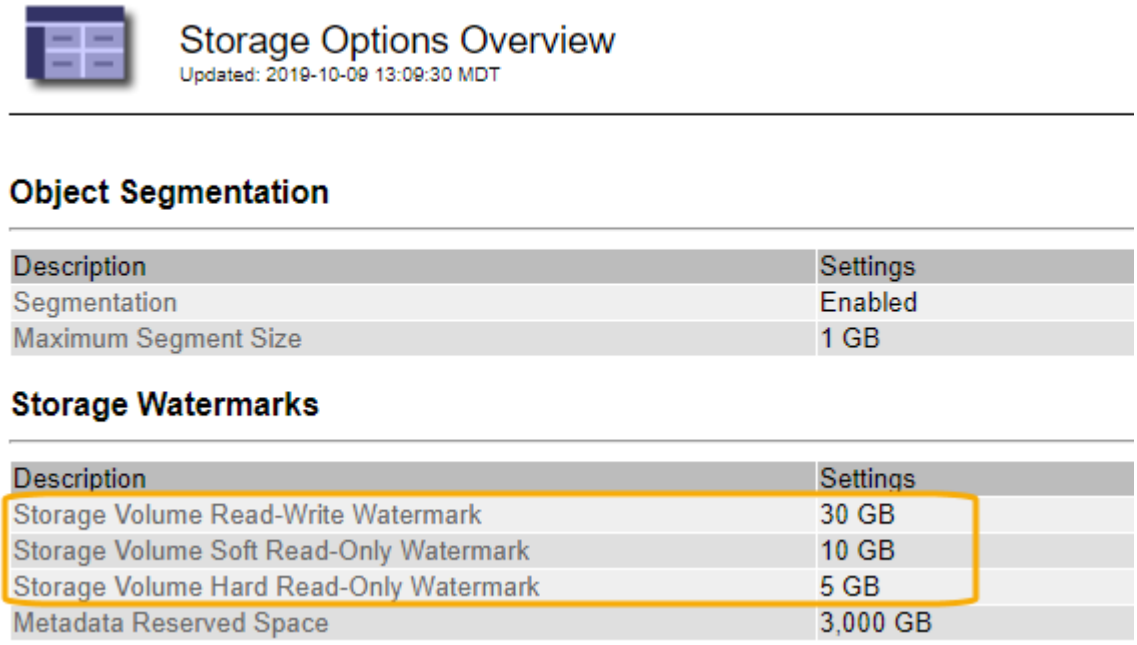
L'alarme Storage Status (SSTS) (État du stockage) est déclenchée si un nœud de stockage ne dispose pas d'espace disponible suffisant pour le stockage d'objets.

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

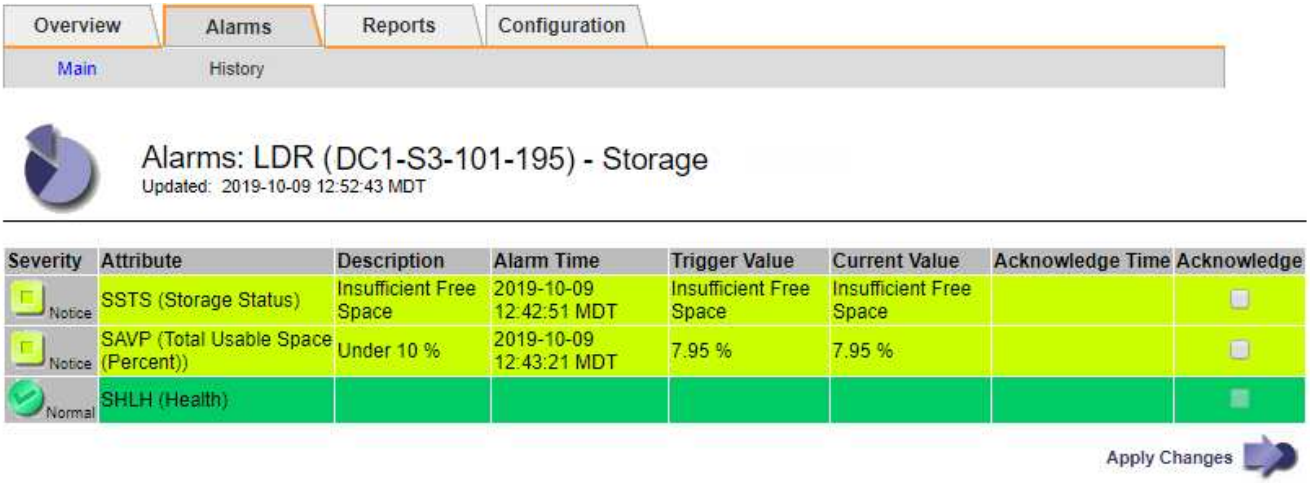
Par exemple, supposons que le filigrane de volume de stockage en lecture seule soit défini sur 10 Go, ce qui est sa valeur par défaut. L'alarme SSTS est déclenchée si moins de 10 Go d'espace utilisable reste sur chaque volume de stockage du nœud de stockage. Si l'un des volumes dispose d'au moins 10 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.

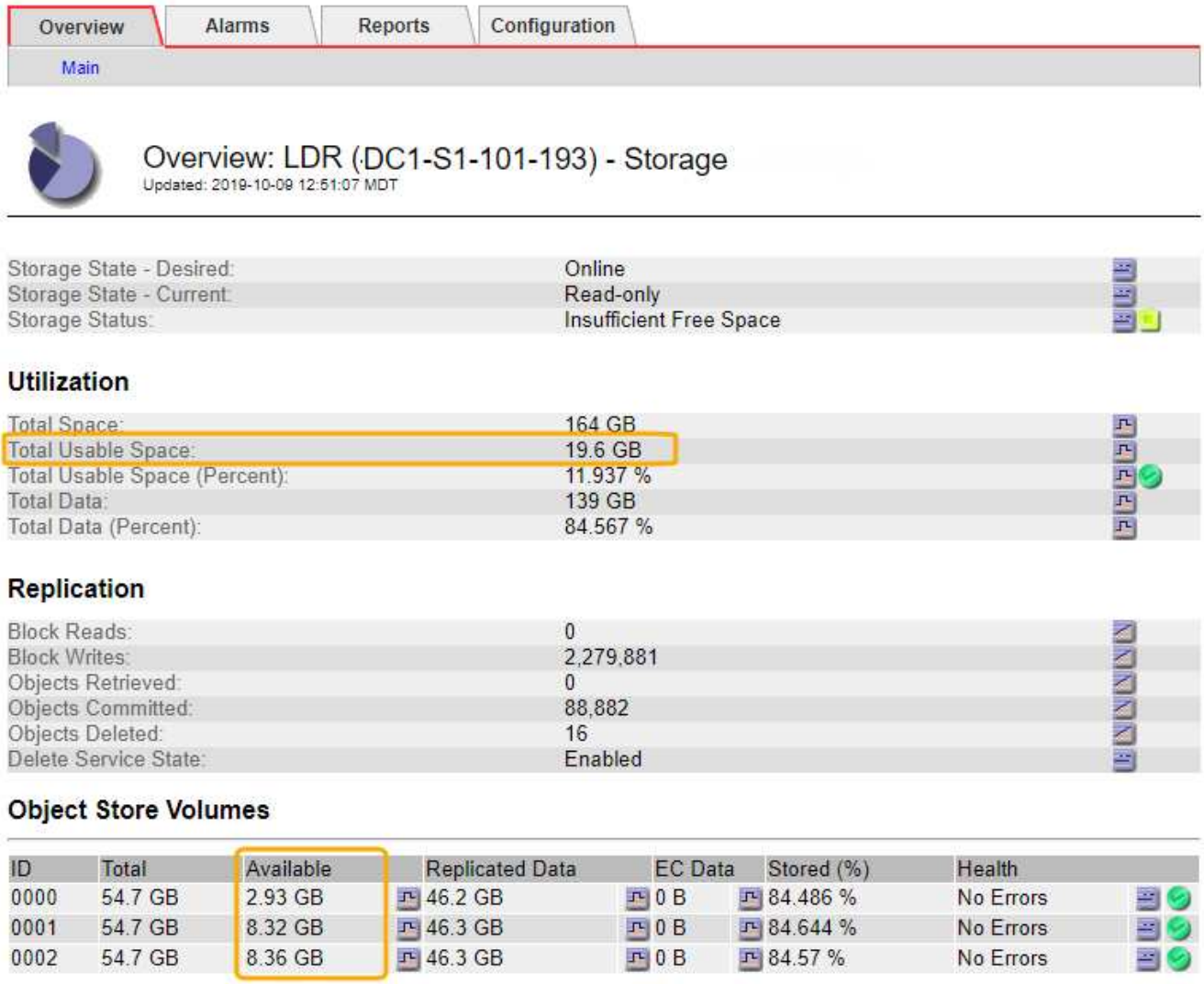
   La page topologie de la grille s'affiche. L'onglet alarmes affiche les alarmes actives pour le nœud et le service que vous avez sélectionnés.



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.

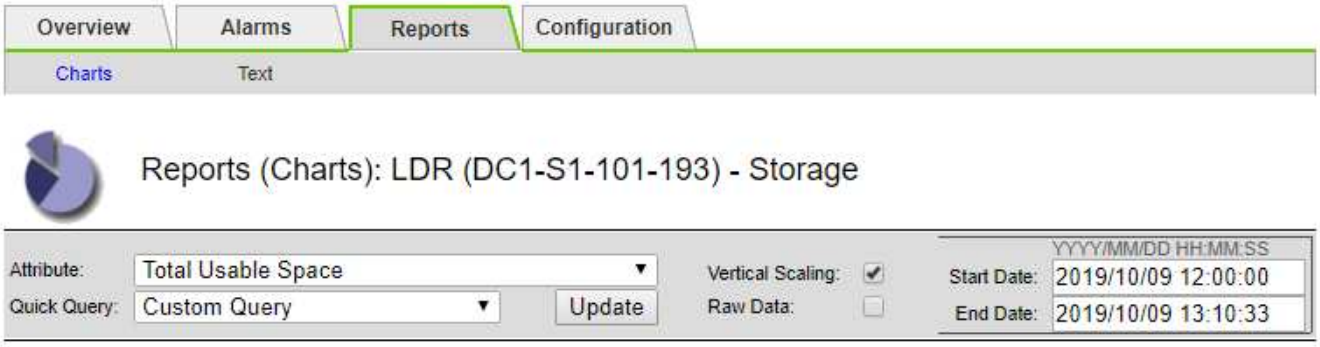
3. Pour déterminer la quantité d'espace utilisable réellement disponible, sélectionnez **LDR Storage Overview** et recherchez l'attribut Total Usable (STAS).

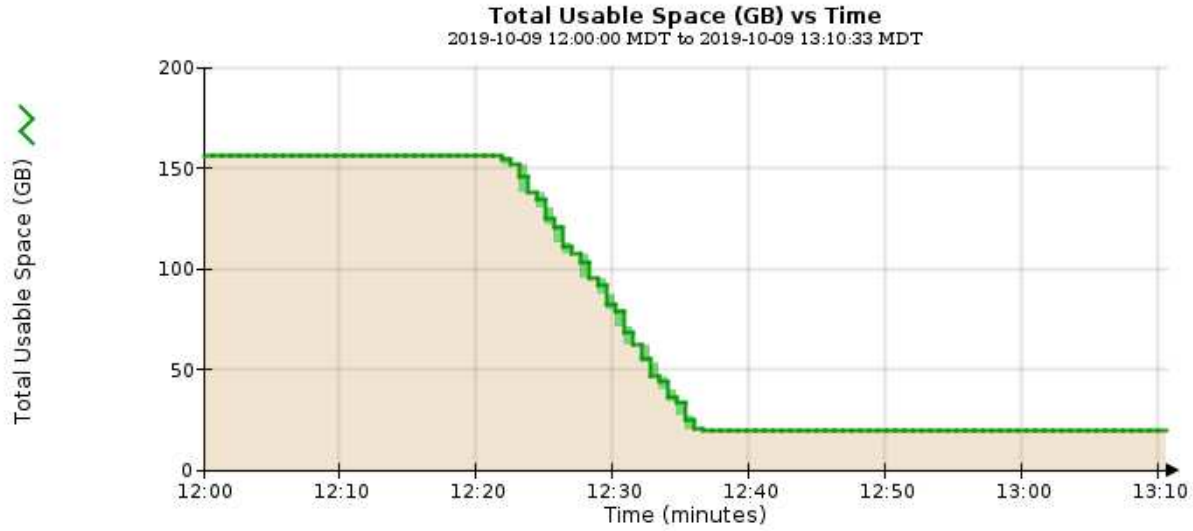


Dans cet exemple, seuls 19.6 Go d'espace de 164 Go sur ce nœud de stockage restent disponibles. Notez que la valeur totale est la somme des valeurs **disponibles** pour les trois volumes du magasin d'objets. L'alarme SSTS a été déclenchée car chacun des trois volumes de stockage avait moins de 10 Go 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.

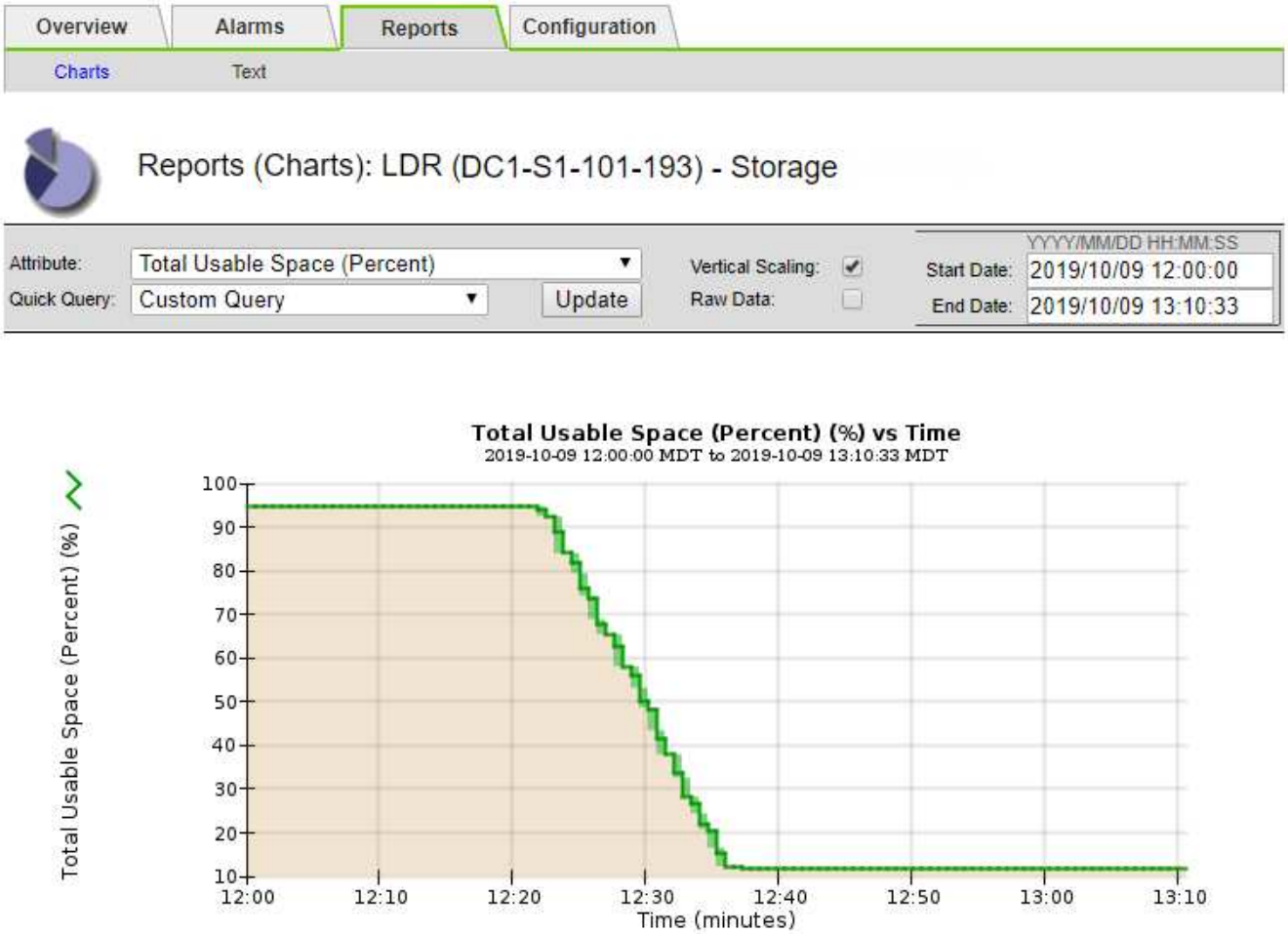
   Dans cet exemple, l'espace utilisable total est passé d'environ 155 Go à 12:00 à 20 Go à 12:35, ce qui correspond à l'heure à laquelle l'alarme SSTS a été déclenchée.





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

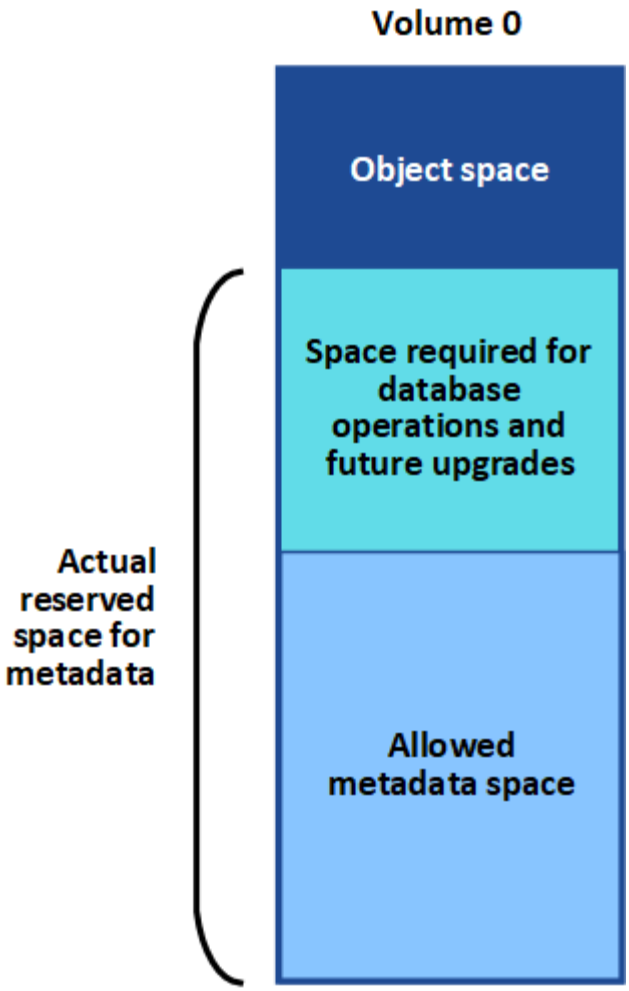
Si l'alerte **stockage de métadonnées faible** est déclenchée, vous devez ajouter de nouveaux nœuds de stockage.

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.

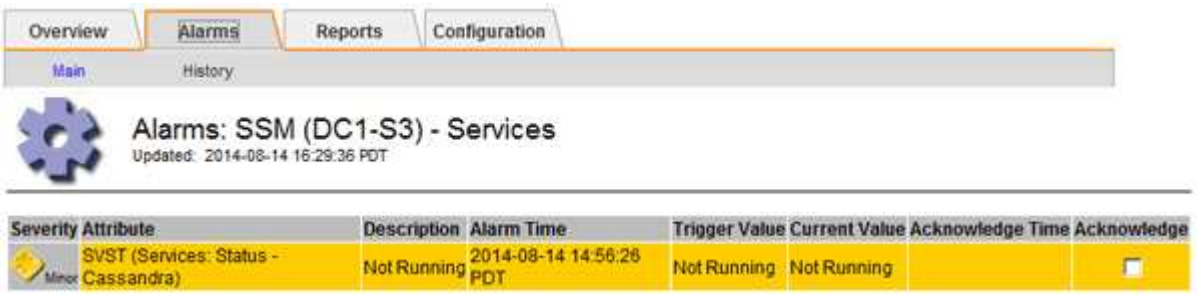
"Exécution des diagnostics"

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.

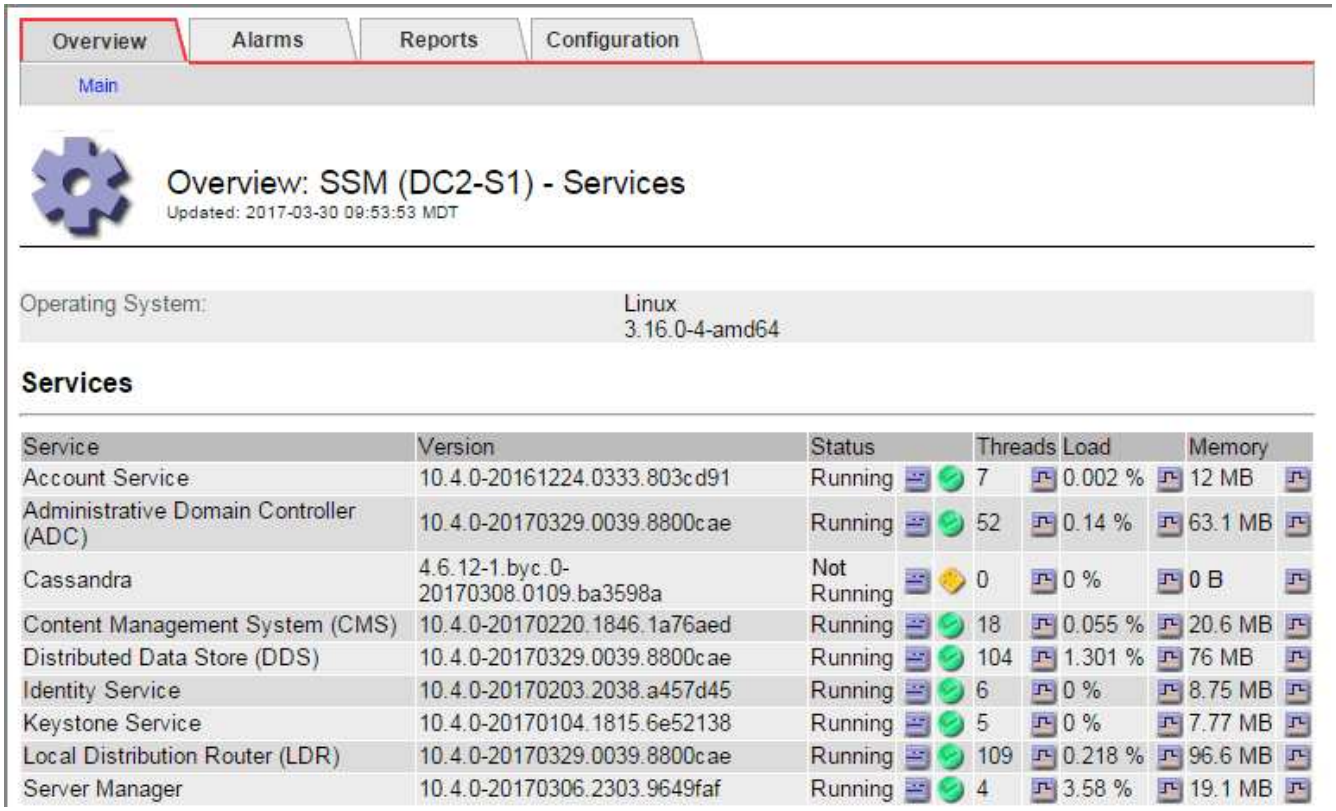
Étapes

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.

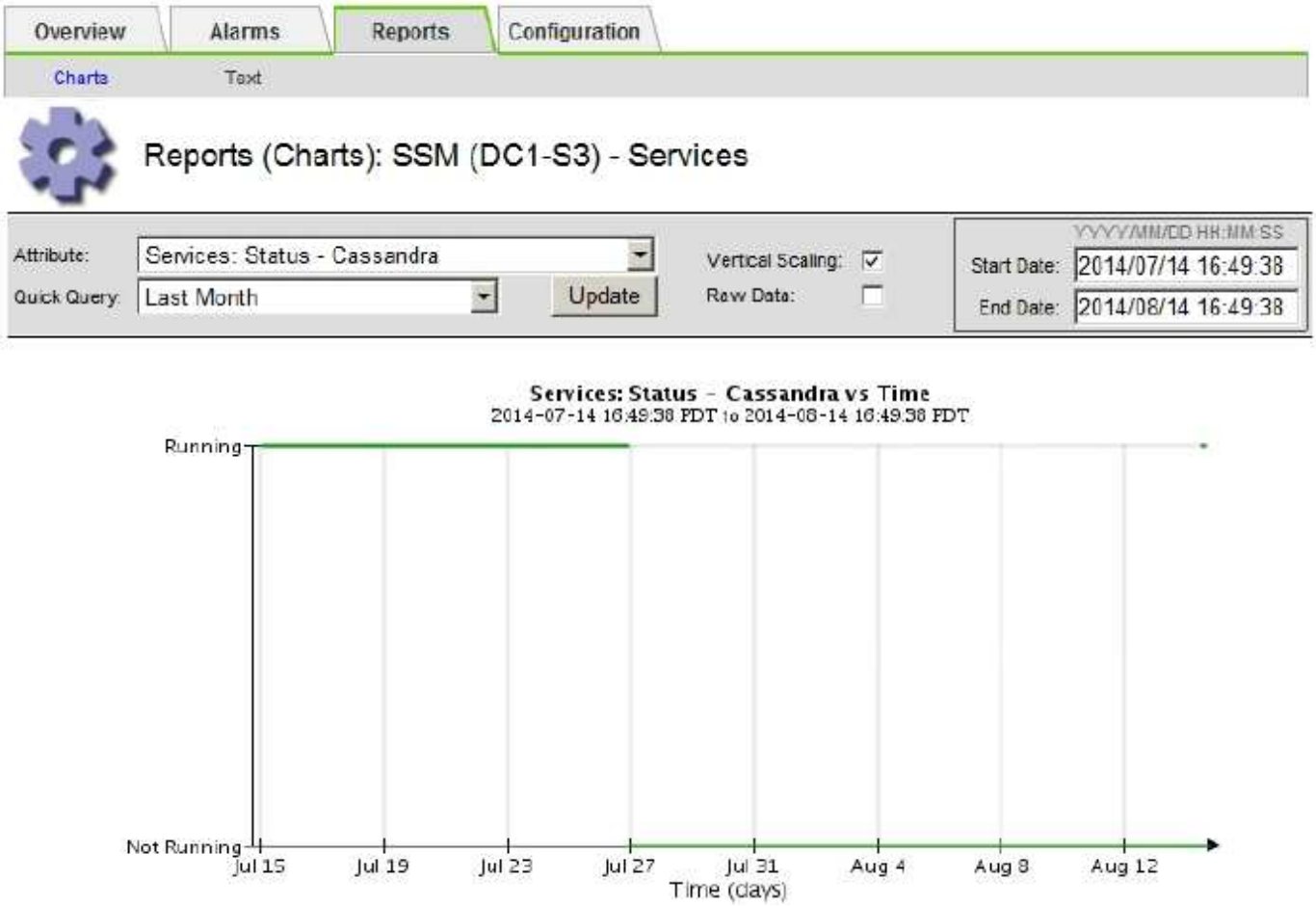
3. Pour le tableau Cassandra :
   a. Sélectionnez **support** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***site*** > ***Storage Node*** > **SSM** > **Services** > **Rapports** > **diagrammes**.
   b. Sélectionnez **attribut** > **Service : état - Cassandra**.
   c. Pour **Date de début**, 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.

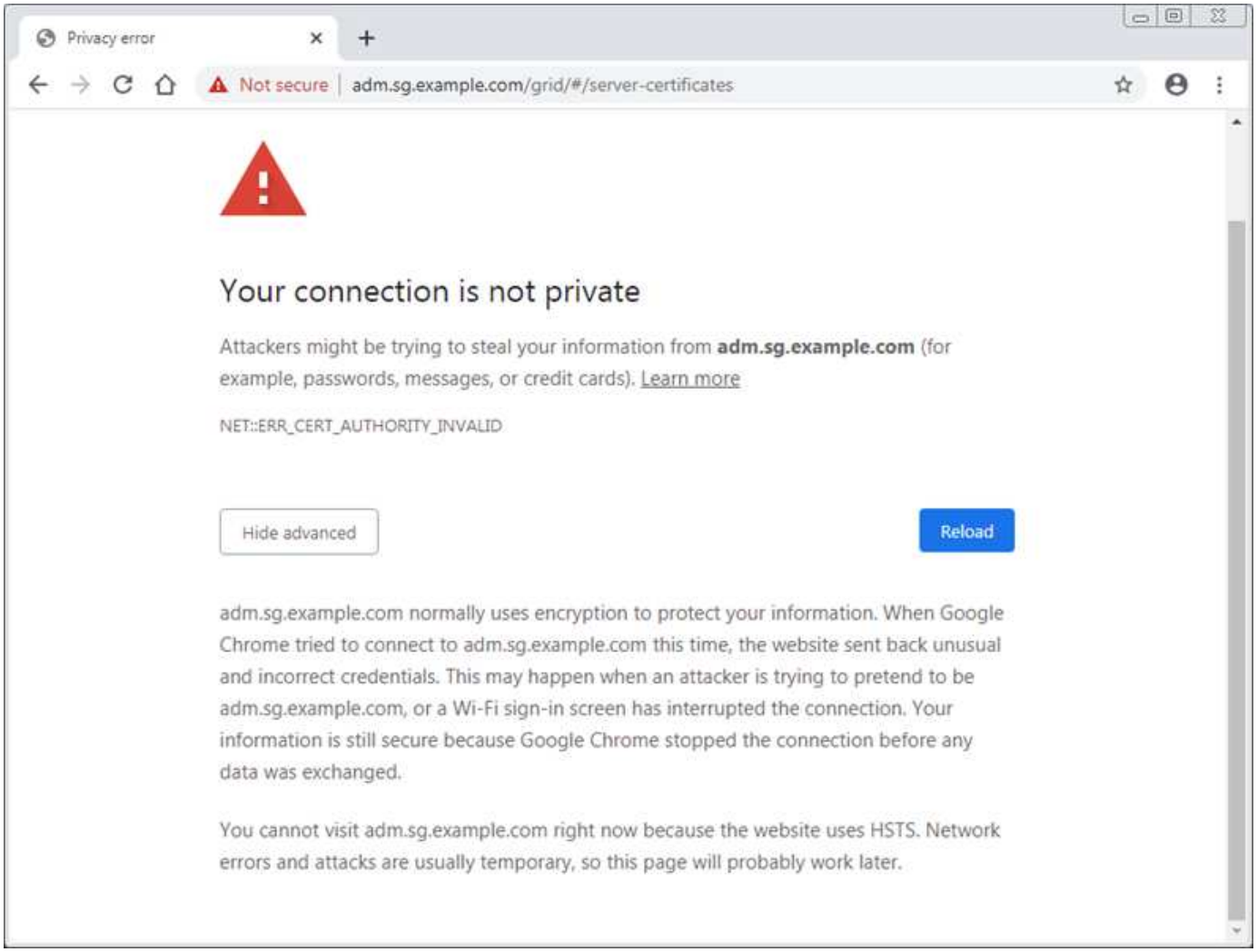
Description de la tâche

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

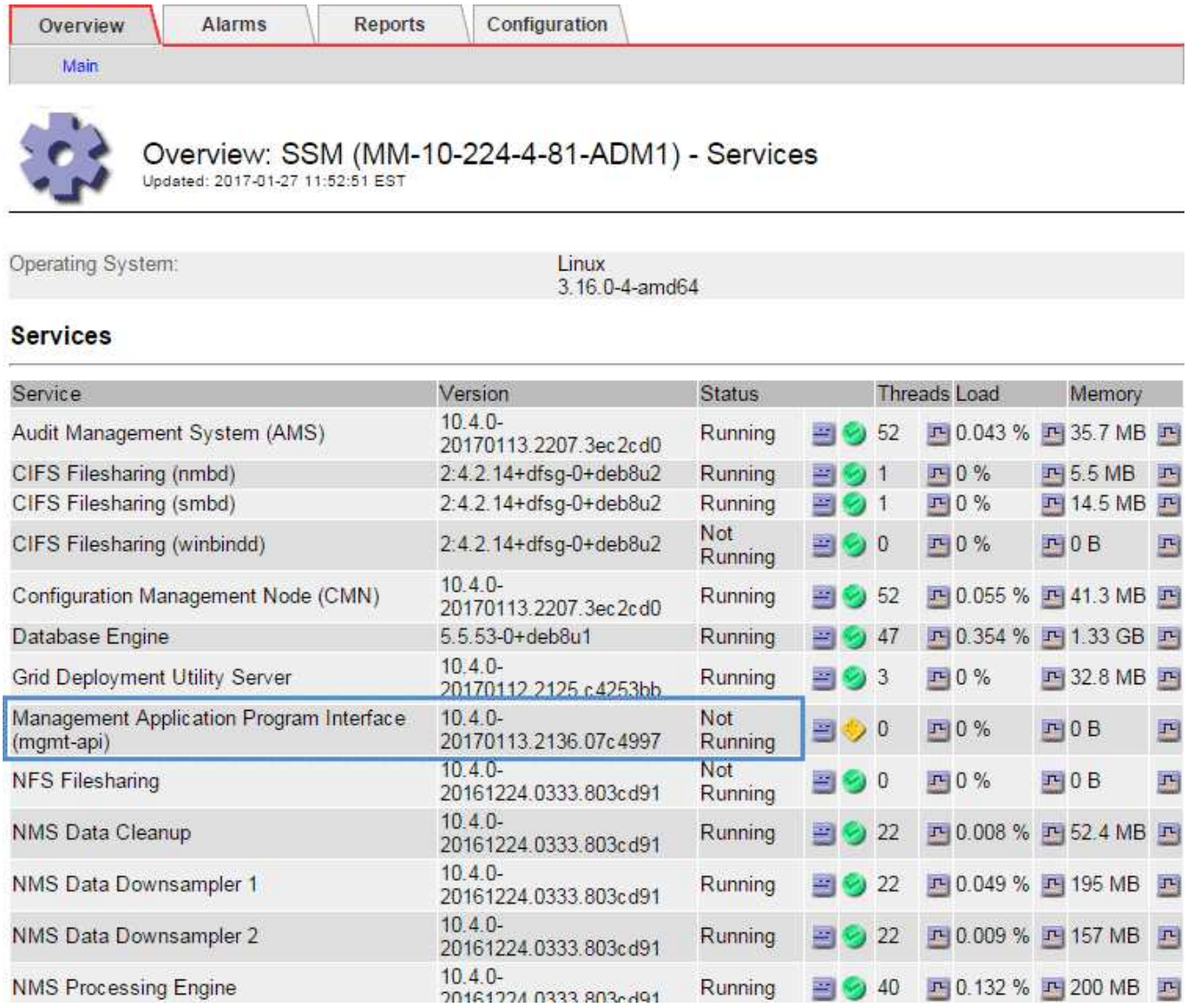
Si le système StorageGRID inclut plusieurs nœuds d'administration, vous pouvez utiliser un autre nœud d'administration pour vérifier l'état d'un nœud d'administration non disponible.

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
   ```

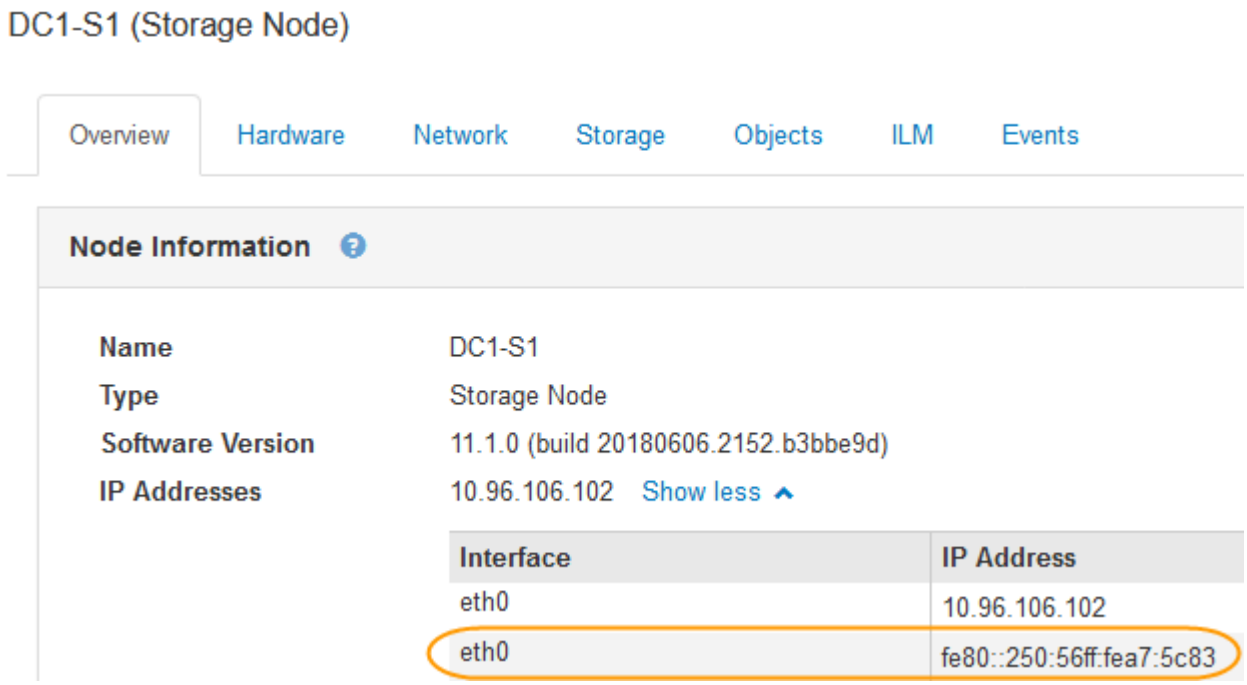
Linux : dépannage de la prise en charge IPv6

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
```

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.