Rapports techniques

StorageGRID solutions and resources

NetApp
October 01, 2026

This PDF was generated from https://docs.netapp.com/fr-fr/storagegrid-enable/technical-reports/index.html on October 01, 2026. Always check docs.netapp.com for the latest.

Sommaire

Rapports techniques . . . 1
Présentation des rapports techniques de StorageGRID . . . 1
NetApp StorageGRID et l'analytique Big Data . . . 1
Utilisations de NetApp StorageGRID . . . 1
Pourquoi choisir StorageGRID pour les data Lakes ? . . . 2
Étude comparative des entrepôts de données et des Lakehouses avec le stockage objet S3 : étude comparative . . . 3
Réglage Hadoop S3A . . . 6
Qu'est-ce que Hadoop ? . . . 6
Connecteur HDFS et S3A Hadoop . . . 7
Réglage du connecteur S3A Hadoop . . . 7
Tr-4871 : configurez StorageGRID pour la sauvegarde et la restauration avec CommVault . . . 12
Sauvegardez et restaurez les données à l'aide de StorageGRID et de CommVault . . . 12
Présentation de la solution testée . . . 14
Conseils sur le dimensionnement de StorageGRID . . . 16
Exécutez une tâche de protection des données . . . 18
Passez en revue les tests de performances de base . . . 26
Recommandation de niveau de cohérence des compartiments . . . 27
Tr-4626 : équilibreurs de charge . . . 28
Utilisez des équilibreurs de charge tiers avec StorageGRID . . . 28
Utiliser les équilibreurs de charge StorageGRID . . . 29
Découvrez comment implémenter des certificats SSL pour HTTPS dans StorageGRID . . . 30
Configurez un équilibreur de charge tiers fiable dans StorageGRID . . . 31
En savoir plus sur les équilibreurs de charge du gestionnaire de trafic local . . . 31
Découvrez quelques utilisations des configurations StorageGRID . . . 35
Valider la connexion SSL dans StorageGRID . . . 38
Comprendre les exigences globales d'équilibrage de charge pour StorageGRID . . . 38
Tr-4645 : fonctions de sécurité . . . 39
Sécurisation des données et des métadonnées StorageGRID dans un magasin d'objets . . . 39
Sécurité de l'accès aux données . . . 41
Sécurité des objets et des métadonnées . . . 49
Fonctions de sécurité de l'administration . . . 52
Fonctions de sécurité de la plate-forme . . . 56
Intégration au cloud . . . 58
Tr-4921 : défense contre les ransomware . . . 59
Protégez les objets StorageGRID S3 contre les attaques par ransomware . . . 59
Protégez vos données contre les ransomwares à l'aide d'un verrouillage objet . . . 59
Protection contre les ransomwares à l'aide d'un compartiment répliqué avec gestion des versions . . . 63
Défense anti-ransomware à l'aide du contrôle des versions avec une politique IAM de protection . . . 66
Enquête et correction des ransomwares . . . 69
Tr-4765 : StorageGRID du moniteur . . . 71
Introduction à la surveillance StorageGRID . . . 71
Utilisez le tableau de bord GMI pour surveiller StorageGRID . . . 72

Utilisez les alertes pour surveiller StorageGRID . . . 73
Surveillance avancée dans StorageGRID . . . 74
Accédez aux metrics à l'aide de CURL dans StorageGRID . . . 77
Affichez les metrics à l'aide du tableau de bord Grafana dans StorageGRID . . . 78
Utilisez les stratégies de classification du trafic dans StorageGRID . . . 79
Utilisez les journaux d'audit pour surveiller StorageGRID . . . 82
Utilisez l'application StorageGRID pour Splunk . . . 82
Tr-4882 : installation d'une grille métallique StorageGRID . . . 82
Introduction à l'installation de StorageGRID . . . 82
Conditions préalables à l'installation de StorageGRID . . . 83
Installez Docker pour StorageGRID . . . 92
Préparez les fichiers de configuration des nœuds pour StorageGRID . . . 93
Installez les dépendances et les packages StorageGRID . . . 96
Validez les fichiers de configuration StorageGRID . . . 96
Démarrez le service d'hôte StorageGRID . . . 98
Configurez le gestionnaire de grille dans StorageGRID . . . 99
Ajoutez les détails de la licence StorageGRID . . . 100
Ajouter des sites à StorageGRID . . . 101
Spécifiez les sous-réseaux de réseau de grille pour StorageGRID . . . 102
Approuver les nœuds grid pour StorageGRID . . . 103
Spécifiez les détails du serveur NTP pour StorageGRID . . . 108
Spécifiez les détails du serveur DNS pour StorageGRID . . . 109
Spécifiez les mots de passe système pour StorageGRID . . . 110
Vérifiez la configuration et terminez l'installation de StorageGRID . . . 111
Mettez à niveau les nœuds bare-Metal dans StorageGRID . . . 113
Tr-4907 : configurer StorageGRID avec veritas Enterprise Vault . . . 114
Introduction à la configuration de StorageGRID pour le basculement de site . . . 114
Configurer StorageGRID et veritas Enterprise Vault . . . 115
Configuration du verrouillage objet StorageGRID S3 pour le stockage WORM . . . 120
Configurez le basculement de site StorageGRID pour la reprise après incident . . . 124

Rapports techniques

Présentation des rapports techniques de StorageGRID

NetApp StorageGRID est une suite de stockage objet Software-defined qui prend en charge un large éventail d'utilisations dans les environnements multiclouds publics, privés et hybrides. StorageGRID offre une prise en charge native de l'API Amazon S3 et propose des innovations de pointe, telles que la gestion automatisée du cycle de vie, pour stocker, sécuriser, protéger et conserver les données non structurées de manière économique sur de longues périodes.

StorageGRID fournit une documentation qui couvre les bonnes pratiques et les recommandations pour plusieurs fonctionnalités et intégrations StorageGRID.

NetApp StorageGRID et l'analytique Big Data

L'analytique des big data est l'un des cas d'utilisation les plus courants des lacs de données basés sur le stockage objet. Lors du choix d'une plateforme analytique, comprendre comment les technologies d'entrepôt de données et de lakehouse interagissent avec le stockage objet S3 peut vous aider à optimiser les performances, l'évolutivité et l'efficacité opérationnelle. StorageGRID fournit un stockage objet compatible S3 pour les charges de travail analytiques, y compris des plateformes telles que Apache Spark, Dremio, Trino et Starburst.

Utilisations de NetApp StorageGRID

La solution de stockage objet NetApp StorageGRID offre évolutivité, disponibilité des données, sécurité et hautes performances. Les entreprises de toutes tailles et de tous secteurs utilisent StorageGRID S3 pour un large éventail d'utilisations. Étudions quelques scénarios types :

Analytique Big Data : StorageGRID S3 est fréquemment utilisé comme data Lake, où les entreprises stockent de grandes quantités de données structurées et non structurées à des fins d'analyse à l'aide d'outils tels que Apache Spark, Splunk Smartstore et Dremio.

Tiering des données : les clients NetApp utilisent la fonctionnalité FabricPool d'ONTAP pour déplacer automatiquement les données entre un niveau local haute performance et StorageGRID. Le Tiering libère un stockage Flash coûteux pour les données actives tout en maintenant les données inactives disponibles dans un stockage objet à faible coût. Cela optimise les performances et les économies.

Sauvegarde des données et reprise après incident : les entreprises peuvent utiliser StorageGRID S3 comme une solution fiable et économique pour sauvegarder des données critiques et les restaurer en cas d'incident.

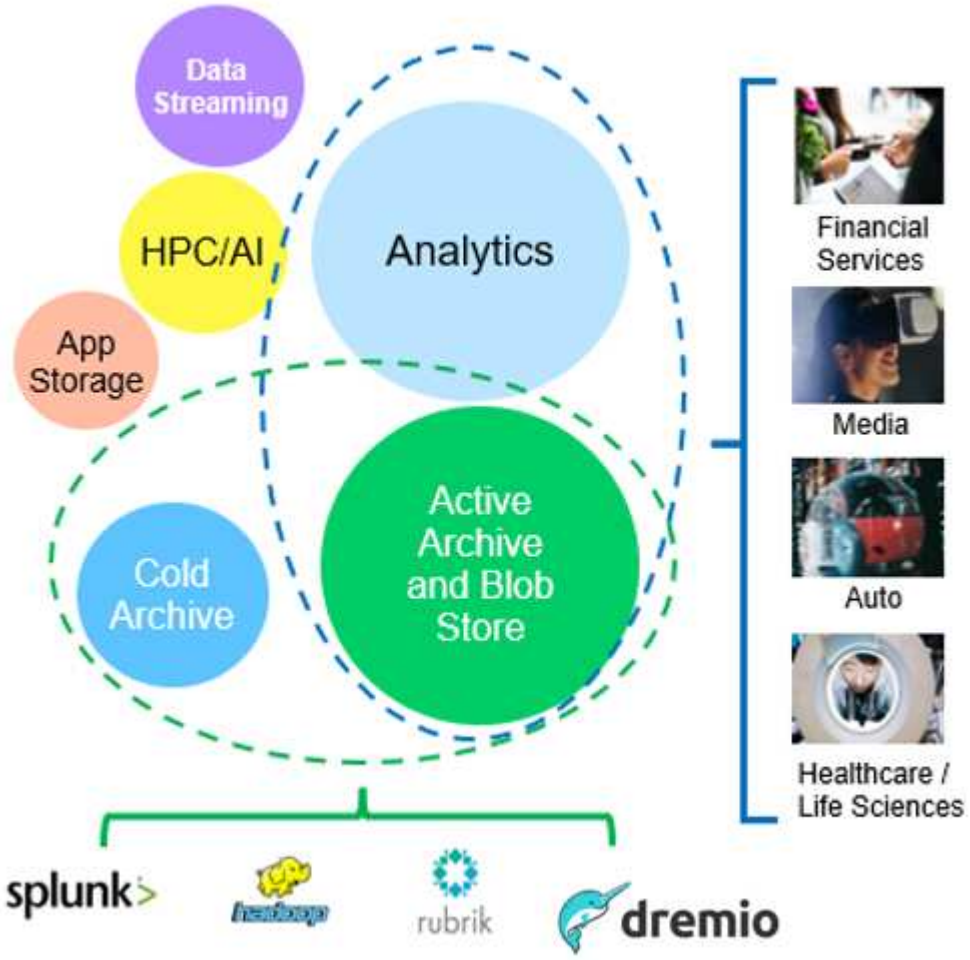
Stockage des données pour les applications : StorageGRID S3 peut être utilisé comme backend de stockage pour les applications, ce qui permet aux développeurs de stocker et de récupérer facilement des fichiers, des images, des vidéos et d'autres types de données.

Diffusion de contenu : StorageGRID S3 peut être utilisé pour stocker et fournir aux utilisateurs du monde entier du contenu statique, des fichiers multimédias et des téléchargements logiciels, en exploitant la

répartition géographique et l'espace de noms global de StorageGRID pour une diffusion de contenu rapide et fiable.

Archives de données : StorageGRID offre différents types de stockage et prend en charge la hiérarchisation vers des options de stockage public à faible coût à long terme, en faisant une solution idéale pour l'archivage et la conservation à long terme des données qui doivent être conservées à des fins de conformité ou d'historique.

Cas d'utilisation du stockage objet



Parmi ces cas d'usage, l'analytique Big Data est l'un des plus utilisés, et son utilisation est en hausse.

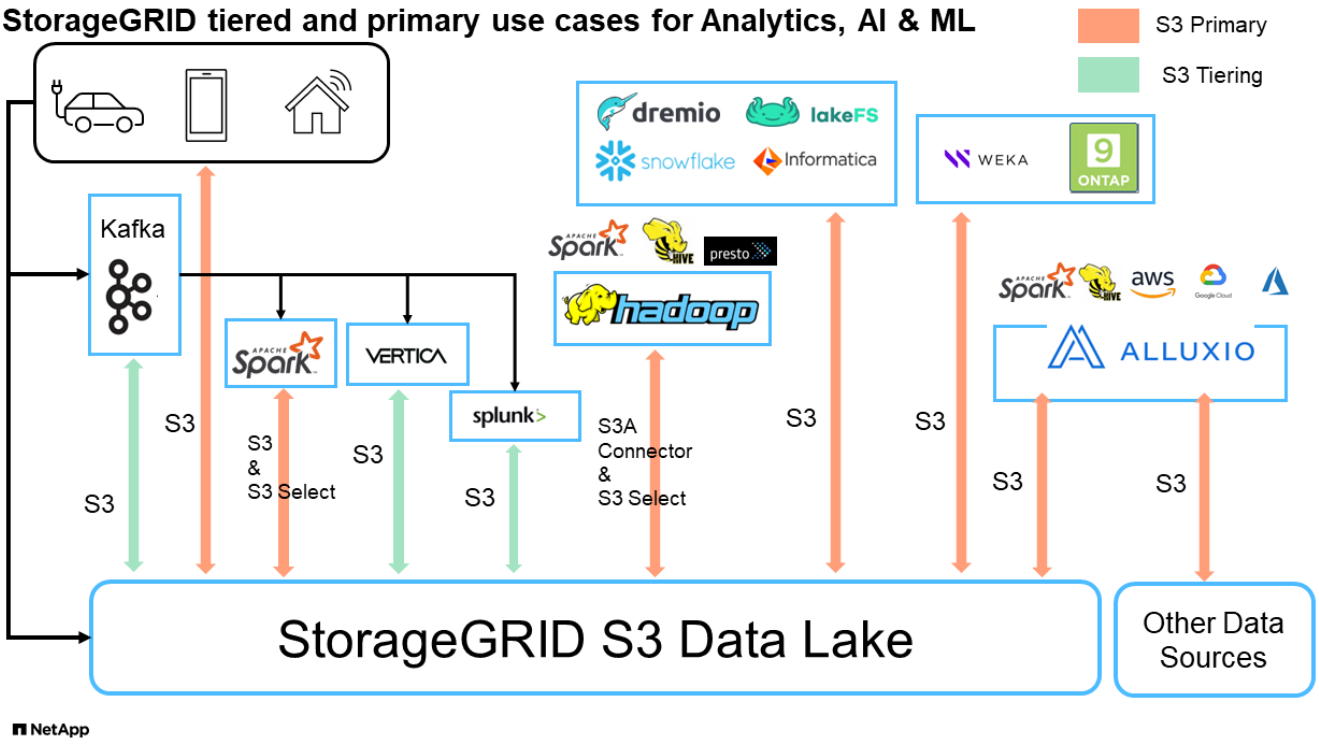
Pourquoi choisir StorageGRID pour les data Lakes ?

- Collaboration renforcée : colocation multisite partagée massive avec accès API standard
- Coûts d'exploitation réduits : simplicité opérationnelle d'une seule architecture à autorétablissement
- Évolutivité : contrairement aux solutions Hadoop et d'entrepôt de données classiques, le stockage objet StorageGRID S3 dissocie le stockage des ressources de calcul et de données pour vous permettre de faire évoluer vos besoins de stockage au fur et à mesure de leur croissance.
- Durabilité et fiabilité : StorageGRID garantit une durabilité de 99.999999999 %, ce qui signifie que les données stockées sont hautement résistantes à la perte de données. Il assure également une haute

disponibilité, garantissant ainsi un accès permanent aux données.

- Sécurité : StorageGRID offre plusieurs fonctionnalités de sécurité, notamment le chiffrement, les règles de contrôle d'accès, la gestion du cycle de vie des données, le verrouillage d'objets et la gestion des versions pour protéger les données stockées dans des compartiments S3

StorageGRID S3 Data Lakes



Étude comparative des entrepôts de données et des Lakehouses avec le stockage objet S3 : étude comparative

Cet article présente une analyse comparative complète de divers écosystèmes d'entrepôts de données et de lacs de données utilisant NetApp StorageGRID. L'objectif est de déterminer quel système offre les meilleures performances avec le stockage d'objets S3. Consultez cet "Apache Iceberg : guide de référence" pour en savoir plus sur les architectures d'entrepôts de données/lacs de données et les formats de tables (Parquet et Iceberg).

- Outil de référence - TPC-DS - https://www.tpc.org/tpcds/
- Les écosystèmes Big Data
  - Cluster de machines virtuelles, chacune avec 128 G de RAM et 24 vCPU, stockage SSD pour le disque système
  - Hadoop 3.3.5 avec Hive 3.1.3 (1 nœud de nom + 4 nœuds de données)
  - Delta Lake avec Spark 3.2.0 (1 maître + 4 employés) et Hadoop 3.3.5
  - Dremio v25.2 (1 coordinateur + 5 exécuteurs)
  - Trino v438 (1 coordinateur + 5 travailleurs)
  - Starburst v453 (1 coordinateur + 5 travailleurs)
- Stockage objet

- NetApp® StorageGRID® 11.8 avec 3 x SG6060 + 1 équilibreur de charge SG1000
- Protection d'objet : 2 copies (le résultat est similaire à EC 2+1)

- Taille de base de données : 1 000 Go
- Le cache a été désactivé dans tous les écosystèmes pour chaque test de requête utilisant le format parquet. Pour le format Iceberg, nous avons comparé le nombre de requêtes GET S3 et le temps total d'interrogation entre les scénarios avec mise en cache désactivée et activée.

TPC-DS comprend 99 requêtes SQL complexes conçues pour l'analyse comparative. Nous avons mesuré le temps total nécessaire à l'exécution des 99 requêtes et réalisé une analyse détaillée en examinant le type et le nombre de requêtes S3. Nos tests ont comparé l'efficacité de deux formats de table courants : parquet et Iceberg.

Résultat de la requête TPC-DS avec le format de table parquet

Écosystème	Ruche	Delta Lake	Dremio	Trino	En étoile
Requêtes TPCDS 99 nombre total de minutes	1084 [1]	55	36	32	28
Répartition des demandes S3	OBTENEZ	1,117,184	2,074,610	3 939 690	1 504 212
1 495 039	observation: Tous les ACCÈS à la gamme	Plage de 80 % de 2 Ko à 2 Mo à partir d'objets de 32 Mo, 50 à 100 requêtes/sec	Plage de 73 % inférieure à 100 Ko pour les objets de 32 Mo, 1000 à 1400 requêtes/sec	90 % plage d'octets de 1 Mo provenant d'objets de 256 Mo, 2500 à 3000 requêtes/sec	Taille GET de la plage : 50 % en dessous de 100 Ko, 16 % autour de 1 Mo, 27 % 2 Mo - 9 Mo, 3500 - 4000 requêtes/sec
Taille GET de la plage : 50 % en dessous de 100 Ko, 16 % autour de 1 Mo, 27 % 2 Mo - 9 Mo, 4000 à 5000 requêtes/sec	Liste des objets	312,053	24,158	120	509
512	TÊTE (objet inexistant)	156,027	12,103	96	0

Écosystème	Ruche	Delta Lake	Dremio	Trino	En étoile
0	TÊTE (objet existant)	982,126	922,732	0	0
0	Nombre total de demandes	2,567,390	3,033,603	3 939,906	1 504 721

[1] Hive Impossible de compléter la requête numéro 72

Résultat de la requête TPC-DS avec format de table Iceberg

Écosystème	Dremio	Trino	En étoile
Requêtes TPCDS 99 + minutes totales (cache désactivé)	22	28	22
Requêtes TPCDS 99 + minutes totales [2] (mémoire cache activée)	16	28	21,5
Répartition des demandes S3	OBTENIR (cache désactivé)	1 985 922	938 639
931 582	OBTENIR (cache activé)	611 347	30 158
3 281	observation: Tous les ACCÈS à la gamme	Taille GET de plage : 67 % 1 Mo, 15 % 100 Ko, 10 % 500 Ko, 3500 à 4500 requêtes/sec	Taille GET de la plage : 42 % en dessous de 100 Ko, 17 % autour de 1 Mo, 33 % 2 Mo - 9 Mo, 3500 - 4000 requêtes/sec
Taille GET de la plage : 43 % en dessous de 100 Ko, 17 % autour de 1 Mo, 33 % 2 Mo - 9 Mo, 4000 - 5000 requêtes/sec	Liste des objets	1465	0
0	TÊTE (objet inexistant)	1464	0
0	TÊTE (objet existant)	3 702	509
509	Nombre total de requêtes (cache désactivé)	1 992 553	939 148

[2] les performances de Trino/Starburst sont des engorgements dus aux ressources de calcul ; l'ajout de RAM au cluster réduit le temps total de requête.

Comme le montre le premier tableau, Hive est beaucoup plus lente que les autres écosystèmes de maisons de données modernes. Nous avons observé qu'Hive a envoyé un grand nombre de requêtes d'objets de liste S3, qui sont généralement lentes sur toutes les plateformes de stockage objet, en particulier lorsqu'il s'agit de compartiments contenant de nombreux objets. Cela augmente considérablement la durée globale des

requêtes. En outre, les écosystèmes de lakehouse modernes peuvent envoyer un grand nombre de requêtes GET en parallèle, allant de 2,000 à 5,000 requêtes par seconde, contre 50 à 100 requêtes par seconde de Hive. La copie de système de fichiers standard de Hive et Hadoop S3A contribue à la lenteur d'Hive lors de l'interaction avec le stockage objet S3.

L'utilisation d'Hadoop (HDFS ou le stockage objet S3) avec Hive ou Spark nécessite une connaissance approfondie de Hadoop et Hive/Spark, ainsi qu'une compréhension des interactions entre les paramètres de chaque service. Ensemble, ils ont plus de 1,000 réglages, dont beaucoup sont liés et ne peuvent pas être modifiés indépendamment. Trouver la combinaison optimale de paramètres et de valeurs nécessite beaucoup de temps et d'efforts.

En comparant les résultats du parquet et de l'Iceberg, nous constatons que le format du tableau est un facteur de performance important. Le format de table Iceberg est plus efficace que le parquet en termes de nombre de requêtes S3, avec 35 à 50 % de demandes en moins par rapport au format parquet.

Les performances de Dremio, Trino ou Starburst sont principalement déterminées par la puissance de calcul du cluster. Bien que les trois utilisent le connecteur S3A pour la connexion de stockage objet S3, ils ne nécessitent pas Hadoop et la plupart des paramètres fs.s3a de Hadoop ne sont pas utilisés par ces systèmes. Cela simplifie le réglage des performances, éliminant ainsi la nécessité d'apprendre et de tester les différents paramètres Hadoop S3A.

À partir de ce résultat du banc d'essai, nous pouvons conclure que le système d'analytique Big Data optimisé pour les workloads S3 constitue un facteur de performance majeur. Les blanchisseurs modernes optimisent l'exécution des requêtes, utilisent efficacement les métadonnées et fournissent un accès transparent aux données S3. Ils offrent ainsi de meilleures performances que Hive avec le stockage S3.

Reportez-vous à cette "page" section pour configurer la source de données Dremio S3 avec StorageGRID.

Cliquez sur les liens ci-dessous pour découvrir comment StorageGRID et Dremio travaillent en collaboration pour fournir une infrastructure de data Lake moderne et efficace, et comment NetApp a migré de Hive + HDFS vers Dremio + StorageGRID pour améliorer considérablement l'efficacité de l'analyse Big Data.

- "Optimisez les performances de vos Big Data avec NetApp StorageGRID"
- "Infrastructure de data Lake moderne, puissante et efficace avec StorageGRID et Dremio"
- "Comment NetApp redéfinit l'expérience client avec l'analytique des produits"

Réglage Hadoop S3A

Par Angela Cheng

Le connecteur Hadoop S3A facilite l'interaction transparente entre les applications Hadoop et le stockage objet S3. Le réglage du connecteur Hadoop S3A est essentiel pour optimiser les performances lorsque vous travaillez avec le stockage objet S3. Avant d'entrer dans les détails d'ajustement, analysons très bien Hadoop et ses composants.

Qu'est-ce que Hadoop ?

Hadoop est une structure open source puissante conçue pour gérer le traitement et le stockage de données à grande échelle. Il permet le stockage distribué et le traitement parallèle sur des clusters d'ordinateurs.

Ces trois composants sont les suivants :

- **Hadoop HDFS (Hadoop Distributed File System)** : gère le stockage, décode les données en blocs et les

distribue entre les nœuds.

- **Hadoop MapReduce** : responsable du traitement des données en divisant les tâches en petits blocs et en les exécutant en parallèle.
- **FIL Hadoop (encore un autre négociateur de ressources):** "Gère les ressources et planifie les tâches de manière efficace"

Connecteur HDFS et S3A Hadoop

HDFS est un composant essentiel de l'écosystème Hadoop, qui joue un rôle essentiel dans l'efficacité du traitement des Big Data. HDFS assure un stockage et une gestion fiables. Elle assure un traitement parallèle et un stockage des données optimisé, ce qui accélère l'accès aux données et leur analyse.

Dans le traitement du Big Data, HDFS se distingue par son excellente tolérance aux pannes pour le stockage de datasets volumineux. Pour cela, il s'agit de la réplication des données. Il peut stocker et gérer d'importants volumes de données structurées et non structurées dans un environnement de data warehouse. De plus, il s'intègre en toute transparence aux principales structures de traitement des Big Data, comme Apache Spark, Hive, Pig et Flink, pour un traitement des données évolutif et efficace. Il est compatible avec les systèmes d'exploitation Unix (Linux), ce qui en fait un choix idéal pour les entreprises qui préfèrent utiliser des environnements Linux pour leur traitement Big Data.

Comme le volume de données s'est accru au fil du temps, l'approche consistant à ajouter de nouvelles machines au cluster Hadoop avec leurs propres ressources de calcul et de stockage s'avère inefficace. L'évolutivité linéaire engendre des défis pour utiliser les ressources efficacement et gérer l'infrastructure.

Pour relever ces défis, le connecteur Hadoop S3A offre des E/S haute performance par rapport au stockage objet S3. L'implémentation d'un workflow Hadoop avec S3A vous permet d'exploiter le stockage objet en tant que référentiel de données et de séparer les ressources de calcul et de stockage. Vous pouvez ainsi faire évoluer indépendamment les ressources de calcul et de stockage. Grâce à la dissociation du calcul et du stockage, vous pouvez également dédier la bonne quantité de ressources pour vos tâches de calcul et fournir la capacité requise en fonction de la taille de votre jeu de données. Par conséquent, vous pouvez réduire votre TCO global pour les workflows Hadoop.

Réglage du connecteur S3A Hadoop

S3 se comporte différemment de HDFS et certaines tentatives de préservation de l'apparence d'un système de fichiers ne sont pas totalement optimales. Des ajustements/tests/tests rigoureux sont nécessaires pour optimiser l'utilisation des ressources S3.

Les options Hadoop présentées dans ce document sont basées sur Hadoop 3.3.5, voir "Hadoop 3.3.5 core-site.xml" pour toutes les options disponibles.

Remarque – la valeur par défaut de certains paramètres Hadoop fs.s3a est différente dans chaque version de Hadoop. Vérifiez la valeur par défaut spécifique à votre version Hadoop actuelle. Si ces paramètres ne sont pas spécifiés dans Hadoop core-site.xml, la valeur par défaut sera utilisée. Vous pouvez remplacer la valeur au moment de l'exécution à l'aide des options de configuration Spark ou Hive.

Vous devez accéder à cette page "Page Apache Hadoop" pour comprendre chaque option fs.s3a. Si possible, testez-les dans un cluster Hadoop non productif pour trouver les valeurs optimales.

Vous devriez lire "Optimisation des performances lors de l'utilisation du connecteur S3A" pour obtenir d'autres recommandations de réglage.

Examinons quelques points clés à prendre en compte :

1. Compression des données

N'activez pas la compression StorageGRID. La plupart des systèmes Big Data utilisent l'option GET de plage d'octets au lieu de récupérer l'objet entier. L'utilisation de la plage d'octets GET avec des objets compressés dégrade considérablement les performances GET.

2. S3A committers

En général, le Comitter Magic s3a est recommandé. Se reporter à ceci "Page des options de renvoi S3A courantes" pour mieux comprendre le comitter magique et ses paramètres s3a associés.

Magic Committer :

Le Magic Committer s'appuie spécifiquement sur S3Guard pour offrir des listes de répertoires cohérentes sur le magasin d'objets S3.

Avec S3 cohérent (ce qui est désormais le cas), le Magic Committer peut être utilisé en toute sécurité avec n'importe quel compartiment S3.

Choix et expérimentation :

Selon votre cas d'utilisation, vous pouvez choisir entre la variable de transfert (qui s'appuie sur un système de fichiers HDFS de cluster) et la variable Magic Committer.

Testez les deux pour déterminer celle qui convient le mieux à votre workload et à vos besoins.

En résumé, les committers S3A constituent une solution au défi fondamental de l'engagement de sortie cohérent, haute performance et fiable pour S3. Leur conception interne garantit un transfert de données efficace tout en préservant l'intégrité des données.

Option	Meaning	Default (Hadoop 3.3.5)
fs.s3a.committer.name	Committer to create for output to S3A, one of: "file", "directory", "partitioned", "magic".	file
fs.s3a.buffer.dir	Local filesystem directory for data being written and/or staged.	${env.LOCAL_DIRS:-${hadoop.tmp.dir}}/s3a
fs.s3a.committer.magic.enabled	Enable "magic committer" support in the filesystem.	true
fs.s3a.committer.abort.pending.uploads	list and abort all pending uploads under the destination path when the job is committed or aborted.	true
fs.s3a.committer.threads	Number of threads in committers for parallel operations on files.	8
fs.s3a.committer.generate.uuid	Generate a Job UUID if none is passed down from Spark	false
fs.s3a.committer.require.uuid	Require the Job UUID to be passed down from Spark	false
mapreduce.fileoutputcommitter.marksuccessfuljobs	Write a _SUCCESS file on the successful completion of the job.	true
mapreduce.outputcommitter.factory.scheme.s3a	The committer factory to use when writing data to S3A filesystems. If mapreduce.outputcommitter.factory.class is set, it will override this property. (This property is set in mapred-default.xml)	org.apache.hadoop.fs.s3a.commit.S3ACommitterFactory

3. Threads, tailles de pool de connexions et taille de bloc

- Chaque client **S3A** interagissant avec un seul compartiment dispose de son propre pool dédié de

connexions HTTP 1.1 ouvertes et de threads pour les opérations de téléchargement et de copie.

- "Vous pouvez régler la taille de ces pools de manière à trouver un équilibre entre les performances et l'utilisation de la mémoire/des threads".
- Lors du téléchargement de données vers S3, elles sont divisées en blocs. La taille de bloc par défaut est de 32 Mo. Vous pouvez personnaliser cette valeur en définissant la propriété fs.s3a.block.size.
- Des blocs plus volumineux peuvent améliorer les performances lors du chargement de données volumineuses en réduisant la surcharge liée à la gestion des pièces à part multiple lors du téléchargement. La valeur recommandée est de 256 Mo ou plus pour les jeux de données volumineux.

Option	Meaning	Default (Hadoop 3.3.5)
fs.s3a.threads.max	The total number of threads available in the filesystem for data uploads *or any other queued filesystem operation*.	64
fs.s3a.connection.maximum	Controls the maximum number of simultaneous connections to S3. This must be bigger than the value of fs.s3a.threads.max so as to stop threads being blocked waiting for new HTTPS connections. Why not equal? The AWS SDK transfer manager also uses these connections.	96
fs.s3a.max.total.tasks	The number of operations which can be queued for execution. This is in addition to the number of active threads in fs.s3a.threads.max.	32
fs.s3a.committer.threads	Number of threads in committers for parallel operations on files (upload, commit, abort, delete...)	8
fs.s3a.executor.capacity	The maximum number of submitted tasks which is a single operation (e.g. rename(), delete()) may submit simultaneously for execution -excluding the IO-heavy block uploads, whose capacity is set in "fs.s3a.fast.upload.active.blocks" All tasks are submitted to the shared thread pool whose size is set in "fs.s3a.threads.max"; the value of capacity should be less than that of the thread pool itself, as the goal is to stop a single operation from overloading that thread pool.	16
fs.s3a.fast.upload.active.blocks (see also related fs.s3a.fast.upload.buffer option)	Maximum Number of blocks a single output stream can have active (uploading, or queued to the central FileSystem instance's pool of queued operations. This stops a single stream overloading the shared thread pool.	4
fs.s3a.block.size	Block size to use when reading files using s3a: file system. A suffix from the set {K,M,G,T,P} may be used to scale the numeric value.	32MB (tested 1TB data set with 256MB and 512MB block size shows significant improvement in both read and write)

4. Téléchargement partitionné

s3a committers **toujours** utiliser MPU (téléchargement partitionné) pour charger des données dans le compartiment s3. Ceci est nécessaire pour permettre : l'échec de tâche, l'exécution spéculative des tâches et les abandons de travail avant la validation. Voici quelques spécifications clés relatives aux téléchargements partitionnés :

- Taille maximale des objets : 5 Tio (téraoctets).
- Nombre maximum de pièces par téléchargement: 10,000.

- Numéros de pièce : compris entre 1 et 10,000 (inclus).
- Taille de la pièce : entre 5 Mio et 5 Gio. En particulier, il n'existe pas de limite de taille minimale pour la dernière partie de votre téléchargement partitionné.

L'utilisation d'une taille de pièce plus petite pour les téléchargements partitionnés S3 présente à la fois des avantages et des inconvénients.

Avantages :

- Récupération rapide à partir des problèmes réseau : lorsque vous chargez des pièces plus petites, l'impact du redémarrage d'un téléchargement échoué en raison d'une erreur réseau est réduit. Si une pièce échoue, il vous suffit de télécharger à nouveau cette pièce spécifique plutôt que l'objet entier.
- Meilleure parallélisation : plus de pièces peuvent être téléchargées en parallèle, ce qui permet de tirer parti du multithreading ou des connexions simultanées. Cette parallélisation améliore les performances, en particulier pour les fichiers volumineux.

Désavantage :

- Surcharge réseau : une taille de pièce plus petite signifie plus de parties à télécharger, chaque partie nécessite sa propre requête HTTP. Le nombre de requêtes HTTP augmente la charge de lancement et de traitement des requêtes individuelles. La gestion d'un grand nombre de petites pièces peut avoir un impact sur les performances.
- Complexité : la gestion de la commande, le suivi des pièces et la garantie de la réussite des téléchargements peuvent s'avérer fastidieux. Si le téléchargement doit être abandonné, tous les articles déjà téléchargés doivent être suivis et purgés.

Pour Hadoop, la taille de pièce de 256 Mo ou plus est recommandée pour fs.s3a.multipart.size. Définissez toujours la valeur fs.s3a.mutipart.threshold sur 2 x fs.s3a.multipart.size. Par exemple, si fs.s3a.multipart.size = 256M, fs.s3a.mutlipart.threshold doit être de 512M.

Utiliser une taille de pièce plus grande pour un jeu de données volumineux. Il est important de choisir une taille de pièce qui équilibre ces facteurs en fonction de votre cas d'utilisation et des conditions réseau spécifiques.

Un téléchargement partitionné est un "processus en trois étapes":

1. Le téléchargement est lancé, StorageGRID renvoie un ID de téléchargement
2. Les parties d'objet sont chargées à l'aide de l'ID de téléchargement
3. Une fois toutes les parties d'objet chargées, envoie une demande de téléchargement partitionné complète avec upload-ID StorageGRID construit l'objet à partir des pièces téléchargées, et le client peut accéder à l'objet.

Si la demande complète de téléchargement partitionné n'est pas envoyée correctement, les pièces restent dans StorageGRID et ne créeront aucun objet. Cela se produit lorsque les travaux sont interrompus, en échec ou abandonnés. Les pièces restent dans la grille jusqu'à ce que le téléchargement partitionné soit terminé ou abandonné ou que StorageGRID purge ces pièces si 15 jours se sont écoulés depuis le lancement du téléchargement. S'il y a beaucoup (quelques centaines de milliers à plusieurs millions) de téléchargements partitionnés en cours dans un compartiment, lorsque Hadoop envoie des « téléchargements partiaux-listes » (cette requête ne filtre pas par identifiant de téléchargement), la demande peut prendre un certain temps ou finir par se terminer. Vous pouvez envisager de définir fs.s3a.mutipart.purge sur TRUE avec une valeur fs.s3a.multipart.purge.age appropriée (par exemple, 5 à 7 jours, n'utilisez pas la valeur par défaut de 86400, c'est-à-dire 1 jour). Ou faites appel au support NetApp pour étudier la situation.

Option	Meaning	Default (Hadoop 3.3.5)
fs.s3a.multipart.size	How big (in bytes) to split upload or copy operations up into. A suffix from the set {K,M,G,T,P} may be used to scale the numeric value.	64M
fs.s3a.multipart.threshold	How big (in bytes) to split upload or copy operations up into. This also controls the partition size in renamed files, as rename() involves copying the source file(s). A suffix from the set {K,M,G,T,P} may be used to scale the numeric value.	128M
fs.s3a.multipart.purge	True if you want to purge existing multipart uploads that may not have been completed/aborted correctly. The corresponding purge age is defined in fs.s3a.multipart.purge.age. If set, when the filesystem is instantiated then all outstanding uploads older than the purge age will be terminated -across the entire bucket. This will impact multipart uploads by other applications and users. so should be used sparingly, with an age value chosen to stop failed uploads, without breaking ongoing operations.	false
fs.s3a.multipart.purge.age	Minimum age in seconds of multipart uploads to purge on startup if "fs.s3a.multipart.purge" is true	86400

5. Mémoire tampon pour écrire les données en mémoire

Pour améliorer les performances, vous pouvez mettre en mémoire tampon l'écriture des données en mémoire avant de les télécharger dans S3. Cela permet de réduire le nombre d'écritures de petite taille et d'améliorer l'efficacité.

Option	Meaning	Default (Hadoop 3.3.5)
fs.s3a.fast.upload.buffer	The buffering mechanism to for data being written. Values: disk, array, bytebuffer. "disk" will use the directories listed in fs.s3a.buffer.dir as the location(s) to save data prior to being uploaded. "array" uses arrays in the JVM heap "bytebuffer" uses off-heap memory within the JVM. Both "array" and "bytebuffer" will consume memory in a single stream up to the number of blocks set by: fs.s3a.multipart.size * fs.s3a.fast.upload.active.blocks. If using either of these mechanisms, keep this value low The total number of threads performing work across all threads is set by fs.s3a.threads.max, with fs.s3a.max.total.tasks values setting the number of queued work items.	disk

N’oubliez pas que S3 et HDFS fonctionnent différemment. Des ajustements/tests/expériences minutieux sont nécessaires pour utiliser de manière optimale les ressources S3.

Tr-4871 : configurez StorageGRID pour la sauvegarde et la restauration avec CommVault

Sauvegardez et restaurez les données à l’aide de StorageGRID et de CommVault

CommVault et NetApp se sont associés pour créer une solution commune de protection des données qui combine le logiciel CommVault Complete Backup and Recovery pour NetApp et le logiciel NetApp StorageGRID pour le stockage cloud. CommVault Complete Backup and Recovery et NetApp StorageGRID proposent des solutions uniques et faciles à utiliser qui s’associent pour répondre aux exigences de croissance rapide des données et à celles de réglementations toujours plus strictes à travers le monde.

De nombreuses entreprises souhaitent migrer leur stockage dans le cloud, faire évoluer leurs systèmes et automatiser leurs règles de conservation des données à long terme. Réputé pour sa résilience, son évolutivité, ses avantages opérationnels et ses économies, le stockage objet basé dans le cloud en fait un choix naturel comme cible pour votre sauvegarde. CommVault et NetApp ont certifié conjointement leur solution combinée en 2014. Depuis, ils ont développé une intégration plus étroite entre leurs deux solutions. Des clients de tous types dans le monde ont adopté la solution combinée CommVault Complete Backup and Recovery and StorageGRID.

À propos de CommVault et StorageGRID

Le logiciel CommVault Complete Backup and Recovery est une solution haute performance de gestion des données et des informations intégrée, conçue dès le départ sur une plateforme unique et dotée d’une base de code unifiée. Toutes ses fonctions partagent des technologies back-end, offrant ainsi les avantages et avantages inégalés d’une approche entièrement intégrée de protection, de gestion et d’accès à vos données. Le logiciel contient des modules pour protéger, archiver, analyser, répliquer et rechercher vos données. Les modules partagent un ensemble commun de services back-end et de fonctionnalités avancées qui interagissent en toute transparence les uns avec les autres. Cette solution aborde tous les aspects de la gestion des données dans votre entreprise, tout en offrant une évolutivité illimitée et un contrôle sans précédent des données et des informations.

NetApp StorageGRID, en tant que Tier cloud CommVault, est une solution de stockage objet de cloud hybride d’entreprise. Vous pouvez le déployer sur de nombreux sites, que ce soit sur une appliance dédiée ou en tant que déploiement Software-defined. StorageGRID vous permet d’établir des règles de gestion des données qui déterminent le mode de stockage et de protection des données. StorageGRID collecte les informations dont vous avez besoin pour développer et appliquer des règles. Il examine un large éventail de caractéristiques et de besoins, y compris les performances, la durabilité, la disponibilité, l’emplacement géographique, longévité et coût. Elles sont intégralement conservées et protégées lors de leur déplacement entre différents sites et au fur et à mesure du vieillissement.

Le moteur de règles intelligent StorageGRID vous aide à choisir l’une des options suivantes :

- Utiliser le code d’effacement pour sauvegarder les données sur plusieurs sites à des fins de résilience.
- Pour copier des objets vers des sites distants afin de minimiser la latence et le coût du WAN.

Lorsque StorageGRID stocke un objet, vous y accédez en tant qu’objet unique, quel que soit son emplacement et le nombre de copies existantes. Ce comportement est crucial pour la reprise d’activité, car

grâce à lui, même si une copie de sauvegarde de vos données est corrompue, StorageGRID peut restaurer vos données.

La conservation des données de sauvegarde dans votre stockage primaire peut s'avérer coûteuse. Avec NetApp StorageGRID, vous libérez de l'espace sur votre stockage primaire en migrant les données de sauvegarde inactives vers StorageGRID, tout en bénéficiant des nombreuses fonctionnalités de StorageGRID. La valeur des données de sauvegarde évolue au fil du temps, tout comme le coût de leur stockage. StorageGRID réduit le coût du stockage primaire tout en augmentant la durabilité des données.

Fonctionnalités clés

Principales fonctionnalités de la plateforme logicielle CommVault :

- Une solution complète de protection des données prenant en charge tous les principaux systèmes d'exploitation, applications et bases de données sur des serveurs virtuels et physiques, des systèmes NAS, des infrastructures cloud et des appareils mobiles.
- Gestion simplifiée via une console unique : vous pouvez afficher, gérer et accéder à toutes les fonctions, à toutes les données et à toutes les informations de l'entreprise.
- Plusieurs méthodes de protection, notamment la sauvegarde et l'archivage des données, la gestion de snapshots, la réplication des données et l'indexation du contenu à des fins d'e-Discovery.
- Gestion du stockage efficace grâce à la déduplication pour le stockage sur disque et cloud.
- Intégration aux baies de stockage NetApp telles que AFF, FAS, NetApp HCI et E-Series et aux systèmes de stockage scale-out NetApp SolidFire®. Intégration également au logiciel NetApp Cloud Volumes ONTAP pour automatiser la création de copies NetApp Snapshot™ indexées sur les applications, sur l'ensemble du portefeuille de stockage NetApp.
- Une gestion complète de l'infrastructure virtuelle qui prend en charge les principaux hyperviseurs virtuels sur site et plateformes d'hyperscaler de cloud public.
- Des fonctionnalités de sécurité avancées pour limiter l'accès aux données stratégiques, fournir des fonctionnalités de gestion granulaire et fournir aux utilisateurs Active Directory un accès Single Sign-on.
- Une gestion des données basée sur des règles qui vous permet de gérer vos données en fonction de vos besoins et non de votre emplacement physique.
- Une expérience utilisateur de pointe qui permet à vos utilisateurs de protéger, de rechercher et de restaurer leurs propres données.
- L'automatisation par API vous permet d'utiliser des outils tiers tels que vRealize Automation ou Service Now pour gérer vos opérations de protection et de récupération des données.

Pour plus de détails sur les charges de travail prises en charge, consultez "Technologies prises en charge par CommVault".

Options de sauvegarde

Lorsque vous implémentez le logiciel CommVault Complete Backup and Recovery avec le stockage cloud, vous disposez de deux options de sauvegarde :

- Sauvegarde sur une cible de disque primaire et sauvegarde également une copie auxiliaire sur un stockage cloud.
- Sauvegarde dans le cloud en tant que cible principale.

Auparavant, le stockage cloud ou objet était considéré comme trop faible pour être utilisé pour la sauvegarde principale. L'utilisation d'une cible de disque primaire a permis aux clients d'accélérer les processus de

sauvegarde et de restauration, et de conserver une copie auxiliaire dans le cloud en tant que sauvegarde à froid. StorageGRID est la nouvelle génération de stockage objet. StorageGRID offre des performances élevées et un débit massif, ainsi que des performances et une flexibilité bien supérieures à celles des autres fournisseurs de stockage objet.

Le tableau suivant répertorie les avantages de chaque option de sauvegarde avec StorageGRID :

	Sauvegarde principale sur disque et copie auxiliaire sur StorageGRID	**Sauvegarde principale vers StorageGRID**
Performance	Délai de restauration le plus rapide, via un montage en direct ou une restauration en direct : idéal pour les workloads de niveau 0/niveau 1.	Ne peut pas être utilisé pour les opérations de montage en direct ou de restauration en direct. Idéal pour les opérations de restauration en streaming et pour la conservation à long terme.
Architecture de déploiement	Utilisation de la technologie 100 % Flash ou d'un disque mécanique comme premier palier d'atterrissage de sauvegarde. StorageGRID est utilisé comme Tier secondaire.	Simplifie le déploiement en utilisant StorageGRID comme cible de sauvegarde complète.
Fonctionnalités avancées (restauration en direct)	Pris en charge	Non pris en charge

Où trouver des informations complémentaires

Pour en savoir plus sur les informations données dans ce livre blanc, consultez ces documents et/ou sites web :

- Centre de documentation StorageGRID 11.9 + https://docs.netapp.com/us-en/storagegrid/
- Documentation produit NetApp https://docs.netapp.com
- Documentation Commvault + https://documentation.commvault.com/2024e/software/index.html

Présentation de la solution testée

La solution testée combine les solutions CommVault et NetApp pour offrir une solution commune puissante.

Configuration de la solution

Dans la configuration de laboratoire, l'environnement StorageGRID se composait de quatre appliances NetApp StorageGRID SG5712, d'un nœud d'administration principal virtuel et d'un nœud de passerelle virtuelle. L'appliance SG5712 est l'option d'entrée de gamme, une configuration de base. Le choix d'appliances plus performantes, telles que NetApp StorageGRID SG5760 ou SG6060, peut considérablement améliorer les performances. Consultez votre architecte de solutions NetApp StorageGRID pour obtenir de l'aide sur le dimensionnement.

Pour sa règle de protection des données, StorageGRID utilise une règle de gestion du cycle de vie intégrée afin de gérer et de protéger les données. Les règles ILM sont évaluées dans une règle de haut en bas. Nous

avons implémenté la politique ILM présentée dans le tableau suivant :

Règle ILM	Qualificatifs	Comportement d'ingestion
Code d'effacement 2+1	Objets de plus de 200 Ko	Équilibré
2 copies	Tous les objets	Double allocation

La règle ILM 2 Copy est la règle par défaut. La règle Erasure Coding 2+1 a été appliquée pour ce test à tout objet de 200 Ko ou plus. La règle par défaut a été appliquée aux objets inférieurs à 200 Ko. L'application des règles de cette manière est une bonne pratique StorageGRID.

Spécifications matérielles de la baie StorageGRID

Le tableau suivant décrit le matériel NetApp StorageGRID utilisé dans ce test. L'appliance StorageGRID SG5712 avec mise en réseau 10 Gbits/s est l'option d'entrée de gamme et représente une configuration de base. Éventuellement, le SG5712 peut être configuré pour une mise en réseau de 25 Gbit/s.

Sous-jacent	Quantité	Disque	Capacité exploitable	Le réseau
Appliances StorageGRID SG5712	4	48 x 4 To (disque dur SAS secondaire)	136 TO	10 Gbit/s

Le choix d'options d'appliance hautes performances, telles que les appliances NetApp StorageGRID SG5760, SG6060 et 100 % Flash SGF6112 peut apporter des avantages significatifs en matière de performance. Consultez votre architecte de solutions NetApp StorageGRID pour obtenir de l'aide sur le dimensionnement.

Configuration logicielle requise pour CommVault et StorageGRID

Les tableaux suivants répertorient les logiciels requis pour les logiciels CommVault et NetApp StorageGRID installés sur le logiciel VMware à des fins de test. Quatre gestionnaires de transmission de données MediaAgent et un serveur CommServe ont été installés. Lors du test, une mise en réseau de 10 Gbits/s a été mise en œuvre pour l'infrastructure VMware. Le tableau suivant

Le tableau suivant répertorie la configuration système totale requise pour le logiciel CommVault :

Composant	Quantité	Datastore	Taille	Total	Nombre total d'IOPS requises
Serveur CommServe	1	OS	500 GO	500 GO	s/o
		SQL	500 GO	500 GO	s/o
MediaAgent	4	Processeur virtuel (vCPU)	16	64	s/o
		RAM	128 GO	512	s/o
		OS	500 GO	2 TO	s/o
		Cache d'index	2 TO	8 TO	200+
		DDB	2 TO	8 TO	200 000 000 K

Dans l'environnement de test, un nœud d'administration principal virtuel et un nœud de passerelle virtuelle ont

été déployés sur VMware sur une baie de stockage NetApp E-Series E2812. Chaque nœud se trouvait sur un serveur distinct avec les exigences minimales relatives à l'environnement de production décrites dans le tableau suivant :

Le tableau suivant répertorie les conditions requises pour les nœuds d'administration virtuelle et les nœuds de passerelle StorageGRID :

Type de nœud	Quantité	VCPU	RAM	Stockage
Nœud de passerelle	1	8	24 GO	LUN de 100 Gb pour le système d'exploitation
Nœud d'administration	1	8	24 GO	LUN de 100 Gb pour le système d'exploitation LUN de 200 Go pour les tables de nœuds d'administration LUN de 200 Go pour le journal d'audit du nœud d'administration

Conseils sur le dimensionnement de StorageGRID

Pour en savoir plus sur le dimensionnement de votre environnement, consultez vos spécialistes de la protection des données NetApp. Les spécialistes de la protection des données NetApp peuvent utiliser le calculateur de stockage de sauvegarde total CommVault pour estimer les exigences de l'infrastructure de sauvegarde. Cet outil requiert un accès au CommVault Partner Portal. Inscrivez-vous pour y accéder, si nécessaire.

Entrées de dimensionnement CommVault

Les tâches suivantes peuvent être utilisées pour effectuer la découverte du dimensionnement de la solution de protection des données :

- Identifiez les charges de travail du système ou des applications/bases de données et la capacité frontale correspondante (en téraoctets [To]) à protéger.
- Identifiez le workload de machines virtuelles/fichiers et une capacité front-end similaire (To) à protéger.
- Identifier les exigences de conservation à court et à long terme.
- Identifier le taux de modification quotidien en % pour les datasets/workloads identifiés
- Identification de la croissance des données prévue au cours des 12, 24 et 36 prochains mois
- Définissez les objectifs RTO et RPO pour la protection et la restauration des données en fonction des besoins de l'entreprise.

Lorsque ces informations sont disponibles, le dimensionnement de l'infrastructure de sauvegarde peut être effectué, ce qui entraîne la répartition des capacités de stockage requises.

Conseils sur le dimensionnement de StorageGRID

Avant d'effectuer le dimensionnement NetApp StorageGRID, tenez compte des aspects suivants de votre charge de travail :

- Capacité exploitable
- Mode WORM
- Taille moyenne des objets
- Exigences en matière de performances
- Règle ILM appliquée

La capacité utilisable doit tenir compte de la taille de la charge de travail de sauvegarde que vous avez basculée vers StorageGRID et du calendrier de conservation.

Le mode WORM sera-t-il activé ou non ? Une fois WORM activé dans CommVault, le verrouillage d'objet est configuré sur StorageGRID. Cela augmente la capacité de stockage objet requise. La capacité requise varie en fonction de la durée de conservation et du nombre de modifications d'objet apportées à chaque sauvegarde.

La taille moyenne d'objet est un paramètre d'entrée qui facilite le dimensionnement des performances dans un environnement StorageGRID. La taille moyenne des objets utilisés pour une charge de travail CommVault dépend du type de sauvegarde.

Le tableau suivant répertorie la taille moyenne des objets par type de sauvegarde et décrit ce que le processus de restauration lit à partir du magasin d'objets :

Type de sauvegarde	Taille moyenne de l'objet	Restaurer le comportement
Effectuer une copie auxiliaire dans StorageGRID	32 MO	Lecture complète de l'objet 32 Mo
Orienter la sauvegarde vers StorageGRID (déduplication activée)	8 MO	Lecture aléatoire 1 Mo
Dirigez la sauvegarde vers StorageGRID (déduplication désactivée)	32 MO	Lecture complète de l'objet 32 Mo

En outre, la compréhension de vos besoins en performances pour les sauvegardes complètes et les sauvegardes incrémentielles vous aide à déterminer le dimensionnement des nœuds de stockage StorageGRID. Les méthodes de protection des données de la règle de gestion du cycle de vie des informations (ILM) de StorageGRID déterminent la capacité requise pour stocker les sauvegardes CommVault et affectent le dimensionnement de la grille.

La réplication ILM de StorageGRID est l'un des deux mécanismes utilisés par StorageGRID pour stocker les données en mode objet. Lorsque StorageGRID attribue des objets à une règle ILM de réplication des données, le système crée des copies exactes des données des objets et les stocke sur des nœuds de stockage.

Le codage d'effacement est la deuxième méthode utilisée par StorageGRID pour stocker les données d'objet. Lorsque StorageGRID attribue des objets à une règle ILM configurée pour créer des copies avec code d'effacement, elle coupe les données en mode objet en fragments de données. Il calcule ensuite des fragments de parité supplémentaires et stocke chaque fragment sur un nœud de stockage différent. Lorsqu'un objet est accédé, il est réassemblé à l'aide des fragments stockés. En cas de corruption ou de perte d'un

fragment de données ou de parité, l'algorithme de code d'effacement peut recréer ce fragment à l'aide d'un sous-ensemble des fragments de données et de parité restants.

Les deux mécanismes nécessitent différentes quantités de stockage, comme le démontrent ces exemples :

- Si vous stockez deux copies répliquées, la surcharge de stockage double.
- Si vous stockez une copie avec code d'effacement 2+1, votre surconsommation de stockage est multipliée par 1.5.

Pour la solution testée, un déploiement StorageGRID d'entrée de gamme sur un seul site a été utilisé :

- Nœud d'administration : machine virtuelle VMware (VM)
- Équilibreur de charge : VMware VM
- Nœuds de stockage : 4 x SG5712 avec disques de 4 To
- Nœud d'administration principal et nœud de passerelle : machines virtuelles VMware avec des exigences minimales en termes de charge de travail de production

StorageGRID prend également en charge les équilibreurs de charge tiers.

StorageGRID est généralement déployé sur deux sites ou plus, avec des règles de protection des données qui répliquent les données afin d'éviter les défaillances au niveau des nœuds et des sites. En sauvegardant vos données sur StorageGRID, elles sont protégées par plusieurs copies ou par un code d'effacement qui sépare et réassemble les données de manière fiable à l'aide d'un algorithme.

Vous pouvez utiliser l'outil de dimensionnement "Fusion" pour dimensionner votre grille.

Évolutivité

Pour étendre un système NetApp StorageGRID, il est possible d'ajouter du stockage aux nœuds de stockage, d'ajouter de nouveaux nœuds grid à un site déjà en place ou d'ajouter un nouveau site de data Center. Les expansions ne nécessitent aucune interruption du fonctionnement du système.
StorageGRID fait évoluer les performances en utilisant soit des nœuds de performance plus élevée pour les nœuds de stockage, soit l'appliance physique qui exécute l'équilibreur de charge et les nœuds d'administration, soit en ajoutant simplement des nœuds supplémentaires.

Pour plus d'informations sur l'extension du système StorageGRID, reportez-vous àla section "Guide d'extension StorageGRID 11.9".

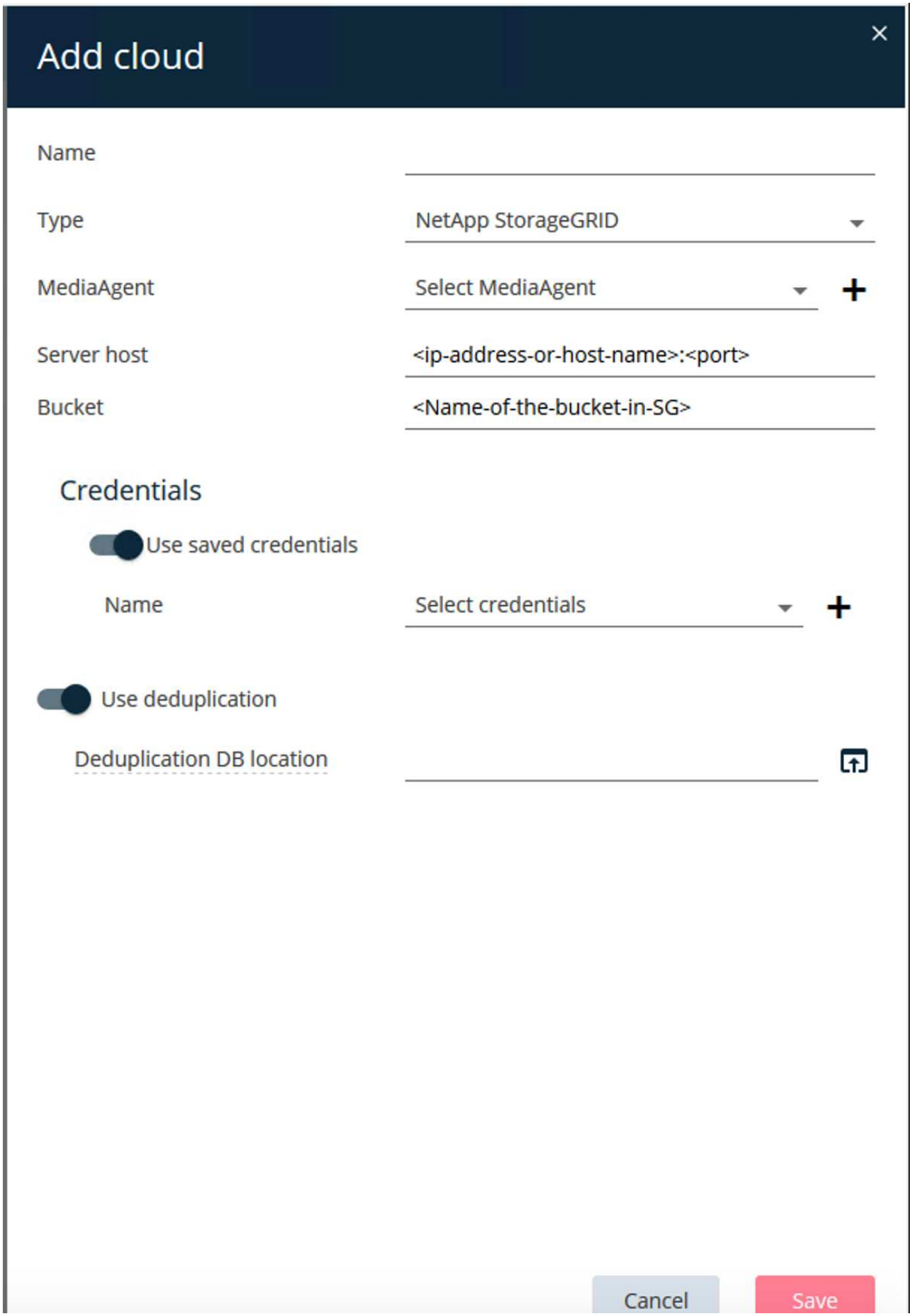
Exécutez une tâche de protection des données

Pour configurer StorageGRID avec CommVault Complete Backup and Recovery pour NetApp, les étapes suivantes ont été effectuées pour ajouter StorageGRID en tant que bibliothèque cloud dans le logiciel CommVault.

Étape 1 : configurer CommVault avec StorageGRID

Étapes

1. Connectez-vous au Centre de commande CommVault. Dans le panneau de gauche, cliquez sur stockage > Cloud > Ajouter pour afficher la boîte de dialogue Ajouter un nuage et y répondre :


Add cloud
Name
Type
NetApp StorageGRID
MediaAgent
Select MediaAgent
Server host
<ip-address-or-host-name>:<port>
Bucket
<Name-of-the-bucket-in-SG>
Credentials
Use saved credentials
Name
Select credentials
Use deduplication
Deduplication DB location
Cancel
Save

2. Sous Type, sélectionnez NetApp StorageGRID.
3. Pour MediaAgent, sélectionnez tous les éléments associés à la bibliothèque cloud.
4. Pour hôte serveur, entrez l'adresse IP ou le nom d'hôte du noeud final StorageGRID et le numéro de port.

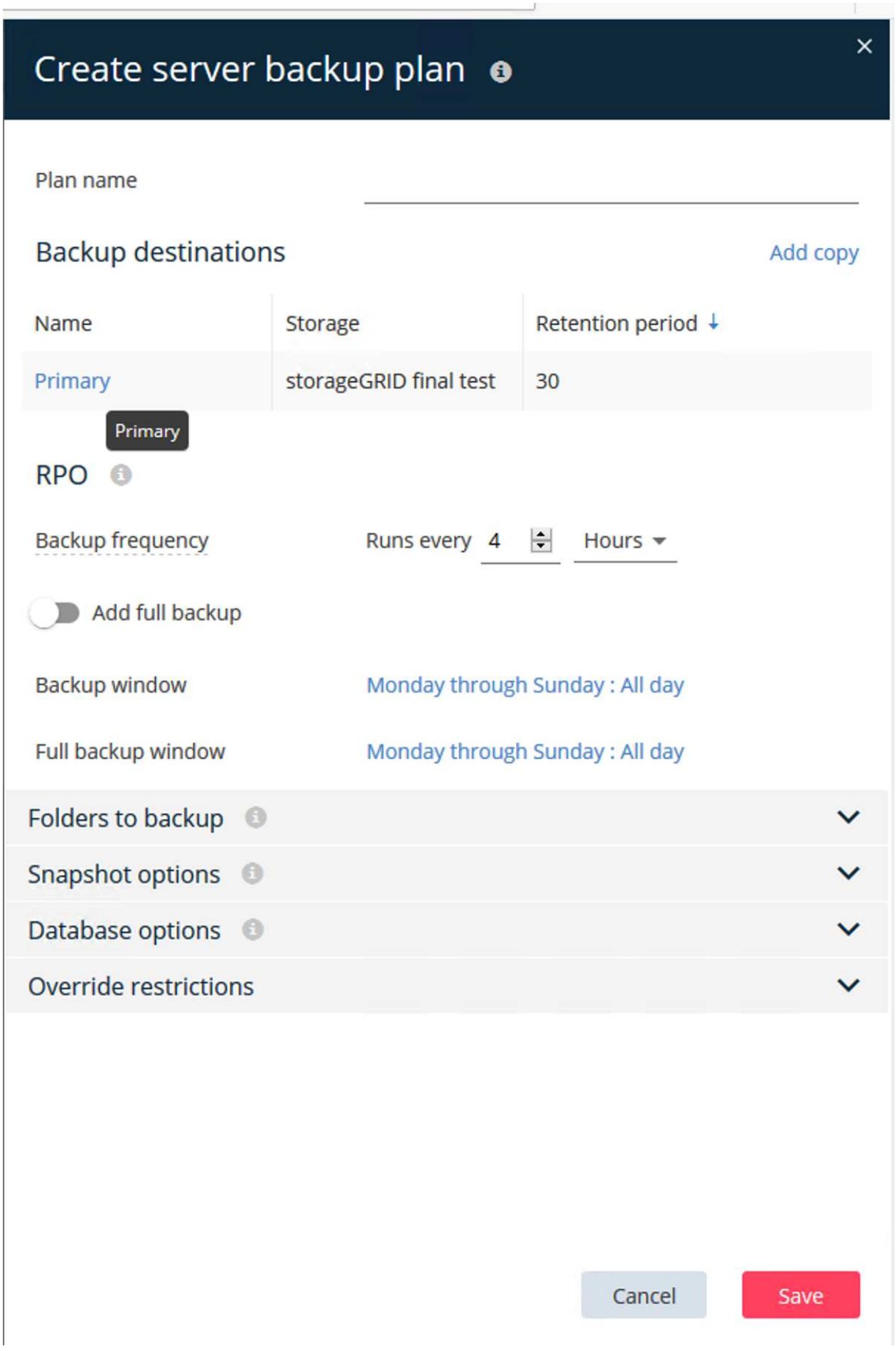
   Suivez les étapes de la documentation StorageGRID sur "comment configurer un terminal d'équilibrage de charge (port)". Assurez-vous que vous disposez d'un port HTTPS avec un certificat auto-signé et que vous disposez de l'adresse IP ou du nom de domaine du noeud final StorageGRID.

5. Si vous souhaitez utiliser la déduplication, activez cette option et indiquez le chemin d'accès à l'emplacement de la base de données de déduplication.
6. Cliquez sur Enregistrer.

Étape 2 : créez un plan de sauvegarde avec StorageGRID comme cible principale

Étapes

1. Dans le panneau de gauche, sélectionnez gérer > plans pour afficher la boîte de dialogue Créer un plan de sauvegarde du serveur et y répondre.

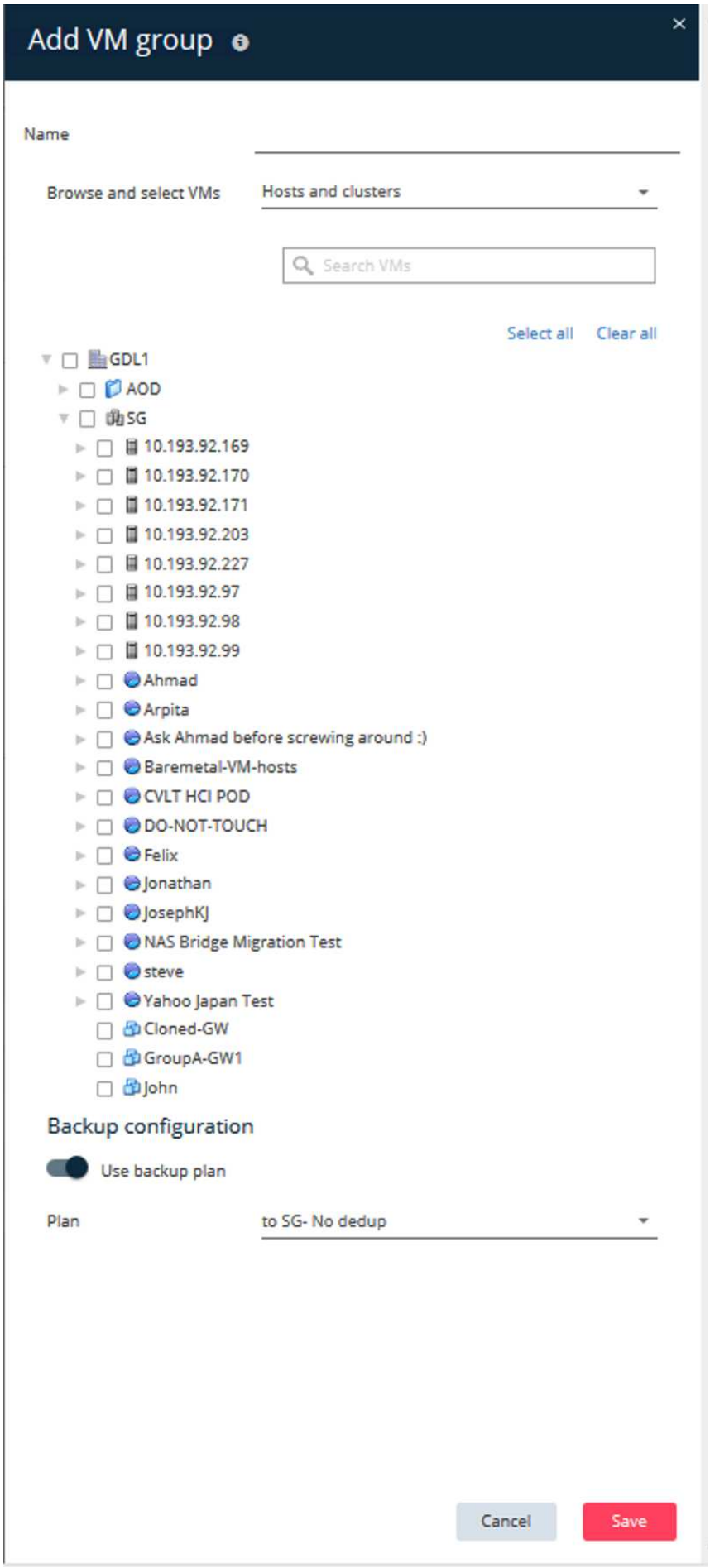

Create server backup plan
Plan name
Backup destinations
Add copy
Name
Storage
Retention period
Primary
storageGRID final test
30
Primary
RPO
Backup frequency
Runs every 4
Hours
Add full backup
Backup window
Monday through Sunday : All day
Full backup window
Monday through Sunday : All day
Folders to backup
Snapshot options
Database options
Override restrictions
Cancel
Save

2. Entrez un nom de plan.
3. Sélectionnez la destination de sauvegarde du stockage StorageGRID simple Storage Service (S3) que vous avez créée précédemment.
4. Saisissez la période de conservation des sauvegardes et l'objectif de point de récupération (RPO) souhaités.
5. Cliquez sur Enregistrer.

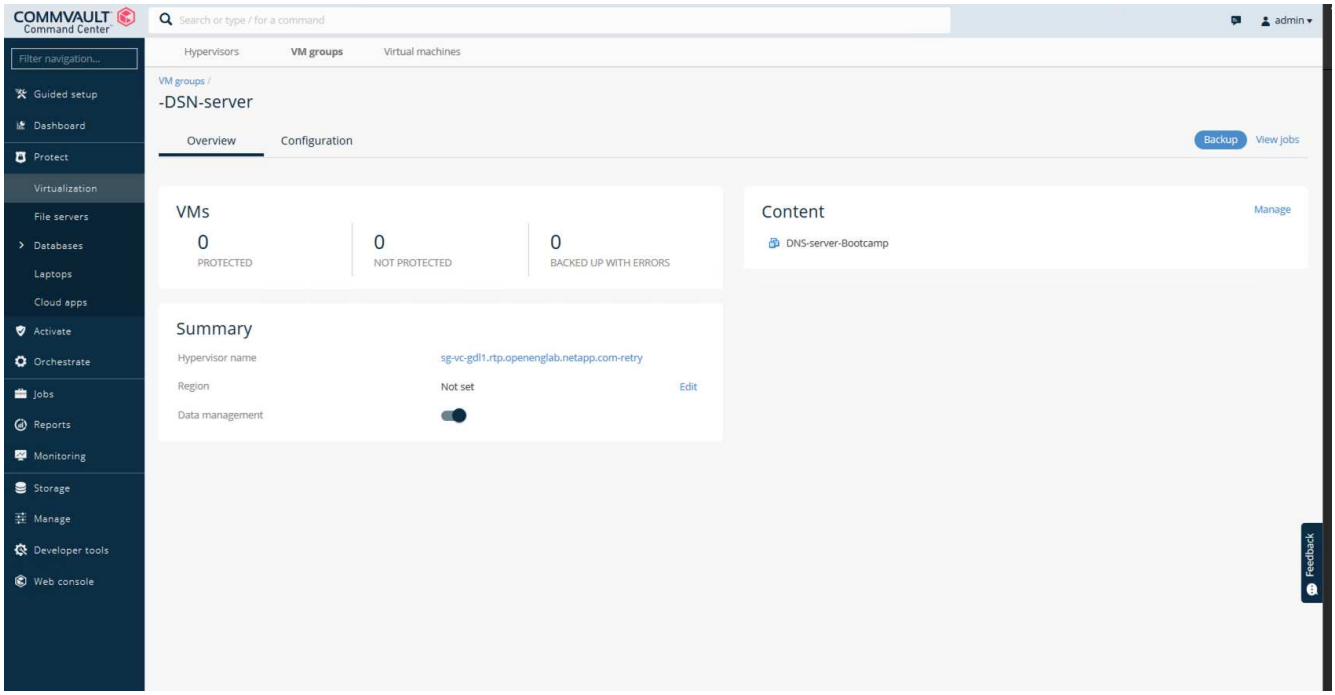
Étape 3 : démarrez une tâche de sauvegarde pour protéger vos workloads

Étapes

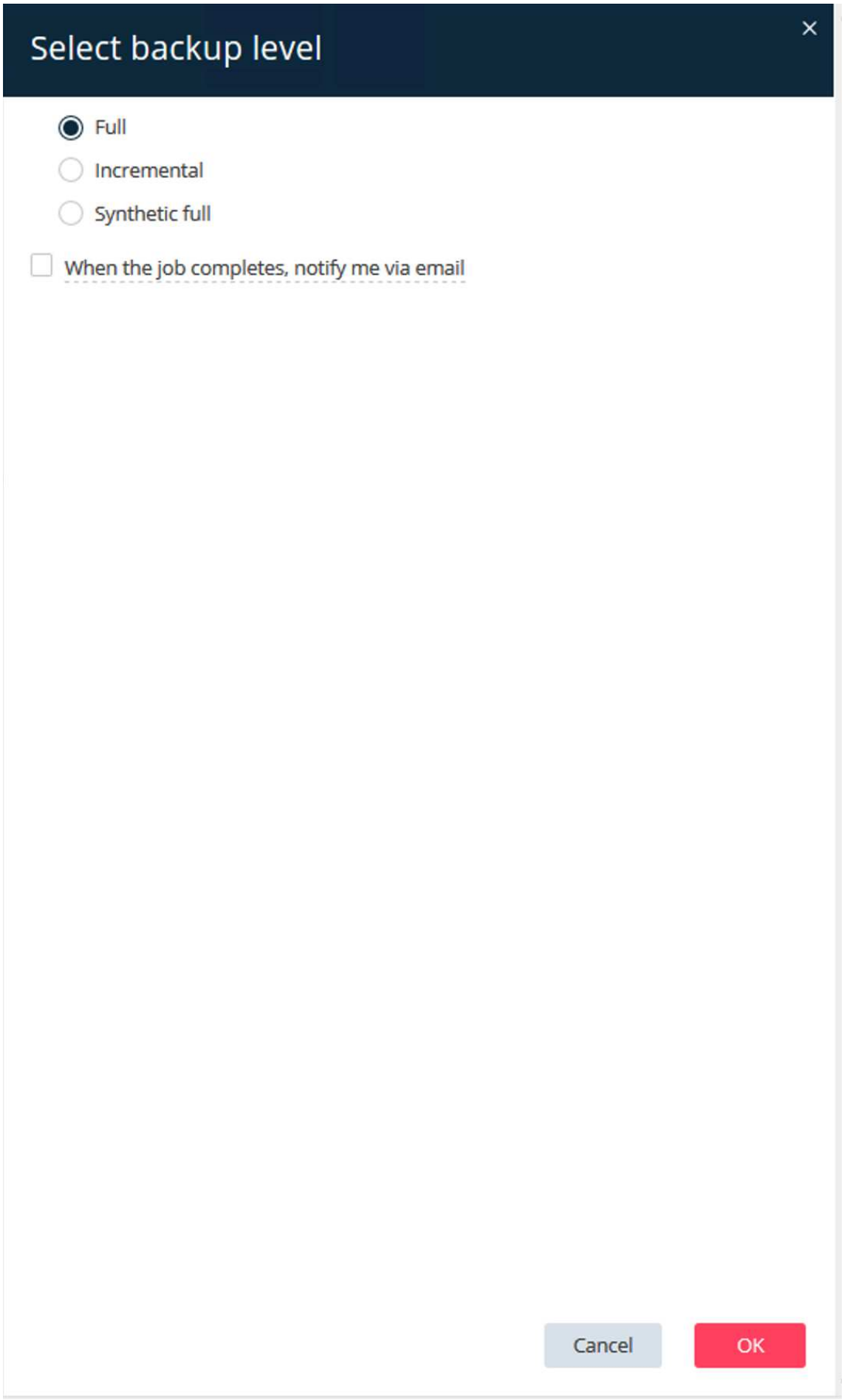
1. Dans CommVault Command Center, accédez à protection > virtualisation.
2. Ajoutez un hyperviseur VMware vCenter Server.
3. Cliquez sur l'hyperviseur que vous venez d'ajouter.
4. Cliquez sur Ajouter un groupe de machines virtuelles pour répondre à la boîte de dialogue Ajouter un groupe de machines virtuelles afin de voir l'environnement vCenter que vous prévoyez de protéger.


Add VM group
Name
Browse and select VMs
Hosts and clusters
Search VMs
Select all
Clear all
GDL1
AOD
SG
10.193.92.169
10.193.92.170
10.193.92.171
10.193.92.203
10.193.92.227
10.193.92.97
10.193.92.98
10.193.92.99
Ahmad
Arpita
Ask Ahmad before screwing around :)
Baremetal-VM-hosts
CVLT HCI POD
DO-NOT-TOUCH
Felix
Jonathan
JosephKJ
NAS Bridge Migration Test
steve
Yahoo Japan Test
Cloned-GW
GroupA-GW1
John
Backup configuration
Use backup plan
Plan
to SG- No dedup
Cancel
Save

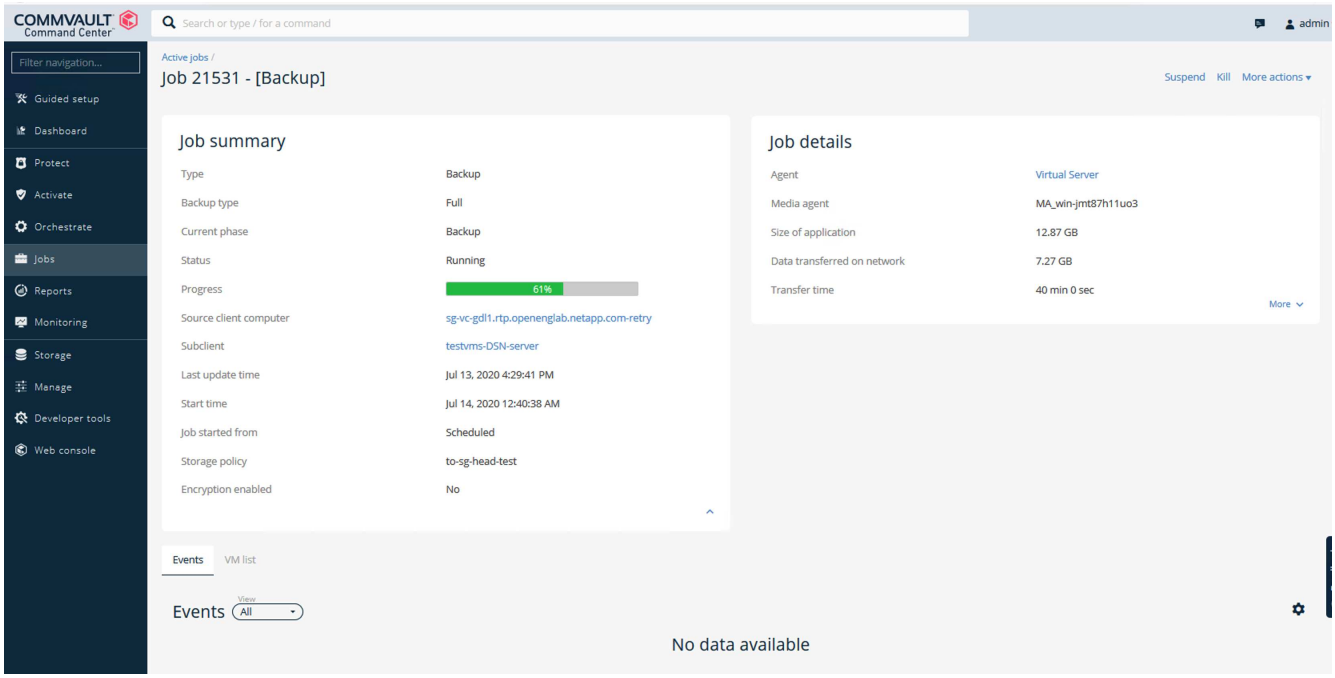
5. Sélectionnez un datastore, une machine virtuelle ou un ensemble de machines virtuelles, puis entrez son nom.
6. Sélectionnez le plan de sauvegarde que vous avez créé dans la tâche précédente.
7. Cliquez sur Enregistrer pour afficher le groupe de machines virtuelles que vous avez créé.
8. Dans le coin supérieur droit de la fenêtre VM group, sélectionnez Backup :



9. Sélectionnez Full comme niveau de sauvegarde, (facultatif) demandez un e-mail lorsque la sauvegarde est terminée, puis cliquez sur OK pour lancer votre tâche de sauvegarde :


Select backup level
Full
Incremental
Synthetic full
When the job completes, notify me via email
Cancel
OK

10. Accédez à la page de résumé du travail pour afficher les mesures du travail :



Passez en revue les tests de performances de base

Lors de l'opération de copie auxiliaire, quatre Commvault MediaAgents ont sauvegardé les données sur un système NetApp AFF A300 et une copie auxiliaire a été créée sur NetApp StorageGRID.

Les tests ont été réalisés avec 100 machines virtuelles et 1000 machines virtuelles, les deux tests portant sur 50/50 combinaisons de machines virtuelles Windows et CentOS. Le tableau suivant présente les résultats de nos tests de performances de base :

Fonctionnement	Vitesse de secours	Vitesse de restauration
Copie aux	2 To/heure	1.27 To/heure
Direct vers et depuis l'objet (déduplication activée)	2.2 To/heure	1.22 To/heure

Pour tester les performances de suppression des données, 2.5 millions d'objets ont été supprimés. Comme le montrent les Figures 2 et 3, l'exécution de la suppression s'est terminée en moins de 3 heures et a libéré plus de 80 To d'espace. La séquence de suppression a démarré à 10:30 AM.

Figure 1 : suppression de 2.5 millions (80 To) d'objets en moins de 3 heures.

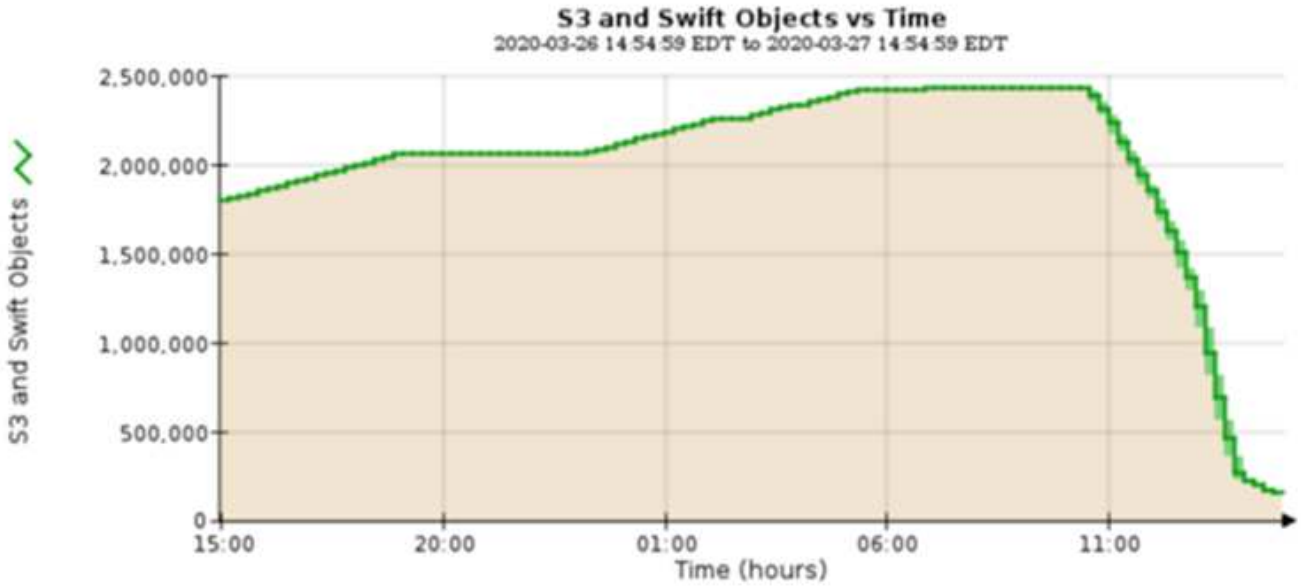
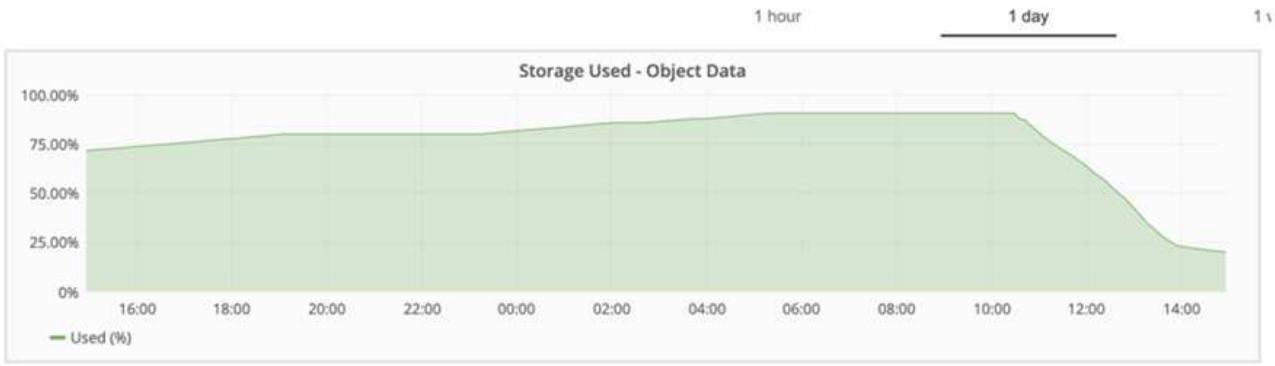


Figure 2 : libération de 80 To de stockage en moins de 3 heures.



Recommandation de niveau de cohérence des compartiments

NetApp StorageGRID permet à l'utilisateur final de sélectionner le niveau de cohérence des opérations effectuées sur les objets dans des compartiments simple Storage Service (S3).

CommVault MediaAgents sont les Data Movers d'un environnement CommVault. Dans la plupart des cas, les MediaAgents sont configurés pour écrire localement sur un site StorageGRID principal. Pour cette raison, un niveau de cohérence élevé est recommandé au sein d'un site primaire local. Lorsque vous définissez un niveau de cohérence sur les compartiments CommVault créés dans StorageGRID, veillez à respecter les consignes suivantes.

Si vous disposez d'une version de CommVault antérieure à 11.0.0 - Service Pack 16, envisagez de mettre à niveau CommVault vers la version la plus récente. Si ce n'est pas une option, assurez-vous de suivre les directives pour votre version.

- Versions CommVault antérieures à 11.0.0 - Service Pack 16.* dans les versions antérieures à 11.0.0 - Service Pack 16, CommVault effectue des opérations S3 HEAD et GET sur des objets inexistants dans le cadre du processus de restauration et de nettoyage. Définissez le niveau de cohérence du compartiment sur site forte pour atteindre un niveau de cohérence optimal pour les sauvegardes CommVault vers

StorageGRID.

- CommVault versions 11.0.0 - Service Pack 16 et ultérieures.* dans les versions 11.0.0 - Service Pack 16 et ultérieures, le nombre d'opérations S3 HEAD et GET effectuées sur des objets inexistants est réduit. Définissez le niveau de cohérence du compartiment par défaut sur lecture après nouvelle écriture afin d'assurer une cohérence élevée dans l'environnement CommVault et StorageGRID.

Tr-4626 : équilibreurs de charge

Utilisez des équilibreurs de charge tiers avec StorageGRID

En savoir plus sur le rôle d'équilibreurs de charge globaux ou tiers dans des systèmes de stockage objet tels que StorageGRID.

Conseils généraux pour la mise en œuvre de NetApp® StorageGRID® avec des équilibreurs de charge tiers.

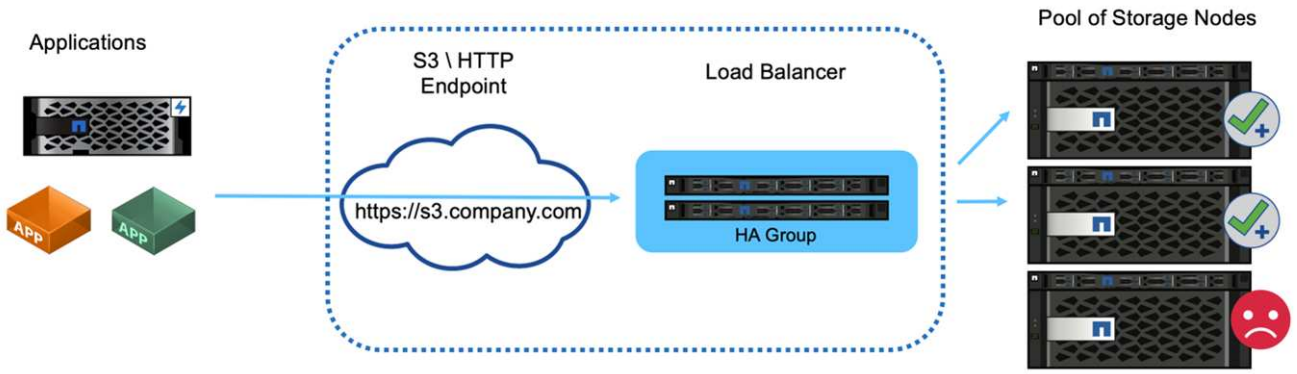
Le stockage objet est synonyme de stockage cloud et, comme vous le feriez, les applications qui exploitent le stockage cloud utilisent une adresse URL. Derrière cette URL simple, StorageGRID peut faire évoluer la capacité, les performances et la durabilité dans un seul site ou sur des sites dispersés géographiquement. L'équilibreur de charge constitue le principal facteur de simplicité.

L'objectif de ce document est d'informer les clients StorageGRID des options d'équilibreur de charge et de fournir des conseils généraux sur la configuration d'équilibreurs de charge tiers.

Principes de base de l'équilibreur de charge

Les équilibreurs de charge sont un composant essentiel d'un système de stockage objet haute performance tel que StorageGRID. StorageGRID est constitué de plusieurs nœuds de stockage, chacun pouvant présenter l'intégralité de l'espace de noms simple Storage Service (S3) d'une instance StorageGRID donnée. Les équilibreurs de charge créent un terminal extrêmement disponible derrière lequel nous pouvons placer les nœuds StorageGRID. StorageGRID est unique en son genre parmi les systèmes de stockage objet compatibles avec S3, dans la mesure où il fournit son propre équilibreur de charge, mais il prend également en charge des équilibreurs de charge tiers ou à usage générique tels que F5, Citrix NetScaler, HA Proxy, NGINX, etc.

La figure suivante utilise l'exemple URL/ nom de domaine complet (FQDN) « s3.company.com". L'équilibreur de charge crée une adresse IP virtuelle (VIP) qui résout le nom de domaine complet via DNS, puis dirige toutes les requêtes des applications vers un pool de nœuds StorageGRID. L'équilibreur de charge vérifie l'état de chaque nœud et établit uniquement les connexions aux nœuds sains.



La figure présente l'équilibreur de charge fourni par StorageGRID, mais le concept est le même pour les

équilibreurs de charge tiers. Les applications établissent une session HTTP à l'aide du VIP sur l'équilibreur de charge et le trafic passe par l'équilibreur de charge aux nœuds de stockage. Par défaut, l'ensemble du trafic, de l'application à l'équilibreur de charge et de l'équilibreur de charge au nœud de stockage, est chiffré via HTTPS. HTTP est une option prise en charge.

Équilibreurs de charge locaux et globaux

Il existe deux types d'équilibreurs de charge :

- **Gestionnaires locaux du trafic (LTM)**. Répartit les connexions sur un pool de nœuds dans un seul site.
- **Equilibreur de charge de service global (GSLB)**. Répartit les connexions sur plusieurs sites, assurant ainsi un équilibrage de charge efficace pour les équilibreurs de charge LTM. Considérez un GSLB comme un serveur DNS intelligent. Lorsqu'un client demande une URL de point de terminaison StorageGRID, le GSLB la résout au VIP d'un LTM en fonction de sa disponibilité ou d'autres facteurs (par exemple, quel site peut fournir une latence plus faible à l'application). Bien qu'un LTM soit toujours requis, un GSLB est facultatif selon le nombre de sites StorageGRID et les exigences de vos applications.

Où trouver des informations complémentaires

Pour en savoir plus sur les informations données dans ce livre blanc, consultez ces documents et/ou sites web :

- Centre de documentation NetApp StorageGRIDhttps://docs.netapp.com/us-en/storagegrid/[]
- Accompagnement NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-enable/
- Considérations relatives à la conception de l'équilibreur de charge StorageGRID f5 https://www.netapp.com/blog/storagegrid-f5-load-balancer-design-considerations/
- Loadbalancer.org—Équilibrage de charge NetApp StorageGRID https://www.loadbalancer.org/applications/netapp-storagegrid/
- Kemp—NetApp StorageGRID d'équilibrage de charge https://support.kemptechnologies.com/hc/en-us/articles/360045186451-NetApp-StorageGRID

Utiliser les équilibreurs de charge StorageGRID

Découvrez le rôle d'un équilibreur de charge de nœud de passerelle StorageGRID .

Conseils généraux pour la mise en œuvre des nœuds de passerelle NetApp® StorageGRID®.

Équilibreur de charge des nœuds de passerelle StorageGRID par rapport à un équilibreur de charge tiers

En effet, StorageGRID est une fonctionnalité exclusive des fournisseurs de stockage objet compatibles avec S3, car elle offre un équilibreur de charge natif disponible en tant qu'appliance, VM ou conteneur dédiés. L'équilibreur de charge fourni par StorageGRID est également appelé nœud de passerelle.

Pour les clients qui ne possèdent pas encore d'équilibreur de charge, comme F5, Citrix, etc., l'implémentation d'un équilibreur de charge tiers peut s'avérer très complexe. L'équilibreur de charge StorageGRID simplifie considérablement les opérations d'équilibrage de charge.

Le nœud de passerelle est un équilibreur de charge haute performance, extrêmement disponible et haute performance. Les clients peuvent choisir d'implémenter le nœud de passerelle, l'équilibreur de charge tiers, ou même les deux, dans le même grid. Le nœud de passerelle est un gestionnaire de trafic local par rapport à un GSLB.

L'équilibreur de charge StorageGRID offre les avantages suivants :

- **Simplicité**. Configuration automatique des pools de ressources, vérifications de l'état, correctifs et maintenance, le tout géré par StorageGRID.
- **Performance**. L'équilibreur de charge StorageGRID est dédié à StorageGRID, peut fournir une mise en cache hautes performances et vous n'êtes pas en concurrence avec d'autres applications pour la bande passante.
- **Coût**. Les versions de machine virtuelle et de conteneur sont fournies sans frais supplémentaires.
- **Classifications de trafic**. La fonctionnalité Advanced Traffic Classification permet d'appliquer des règles de QoS spécifiques à StorageGRID ainsi qu'une analyse des workloads.
- **Futures fonctionnalités spécifiques à StorageGRID**. StorageGRID va continuer à optimiser et à ajouter des fonctionnalités innovantes à l'équilibreur de charge dans les prochaines versions.

En tant que nœud intégré de StorageGRID, le gestionnaire de trafic local a la possibilité d'utiliser des contrôles de santé avancés pour distribuer les demandes en fonction de l'état de santé, de la charge et de la disponibilité des ressources du nœud de stockage. De plus, il a la capacité de répartir la charge sur plusieurs sites lorsque les coûts de liaison StorageGRID sont définis sur « 0 » entre les sites. Dans le cas où les nœuds de stockage ne sont pas disponibles mais que le nœud de passerelle est disponible sur un site, la charge sera automatiquement dirigée vers un autre site de la grille.

La fonctionnalité de mise en cache de l'équilibreur de charge du nœud de passerelle est destinée à fournir une amélioration substantielle des performances pour certaines charges de travail (telles que la formation de l'IA) qui relisent un ensemble de données plusieurs fois dans le cadre du traitement de ces données. Les nœuds de passerelle de mise en cache peuvent également être déployés physiquement loin du reste de la grille, ce qui permet de meilleures performances et une utilisation réduite du réseau WAN dans certaines charges de travail. Le cache fonctionne en mode de lecture arrière où les écritures ne sont pas mises en cache et ne modifient pas l'état du cache. Chaque nœud de passerelle de mise en cache fonctionne indépendamment de tout autre nœud de passerelle de mise en cache.

Pour plus de détails sur le déploiement du nœud de passerelle StorageGRID , consultez le "Documentation StorageGRID" .

Découvrez comment implémenter des certificats SSL pour HTTPS dans StorageGRID

Comprendre l'importance et les étapes de la mise en œuvre des certificats SSL dans StorageGRID.

Si vous utilisez HTTPS, vous devez disposer d'un certificat SSL (Secure Sockets Layer). Le protocole SSL identifie les clients et les noeuds finaux et les valide comme étant approuvés. SSL assure également le cryptage du trafic. Le certificat SSL doit être approuvé par les clients. Pour ce faire, le certificat SSL peut provenir d'une autorité de certification (CA) de confiance mondiale, telle que DigiCert, d'une autorité de certification privée exécutée dans votre infrastructure ou d'un certificat auto-signé généré par l'hôte.

L'utilisation d'un certificat d'autorité de certification approuvée à l'échelle mondiale est la méthode recommandée, car aucune action supplémentaire côté client n'est requise. Le certificat est chargé dans l'équilibreur de charge ou StorageGRID, et les clients font confiance et se connectent au terminal.

L'utilisation d'une autorité de certification privée nécessite l'ajout de la racine et de tous les certificats subordonnés au client. Le processus d'approbation d'un certificat d'autorité de certification privée peut varier en fonction du système d'exploitation et des applications du client. Par exemple, dans ONTAP for FabricPool, vous devez télécharger individuellement chaque certificat de la chaîne (certificat racine, certificat subordonné,

certificat de point final) sur le cluster ONTAP.

L'utilisation d'un certificat auto-signé exige que le client ait confiance dans le certificat fourni sans aucune autorité de certification pour vérifier l'authenticité. Certaines applications peuvent ne pas accepter de certificats auto-signés et ne pas pouvoir ignorer la vérification.

Le placement du certificat SSL dans le chemin StorageGRID de l'équilibreur de charge du client dépend de l'emplacement où vous avez besoin de la terminaison SSL. Vous pouvez configurer un équilibreur de charge comme point d'extrémité pour le client, puis le chiffrer à nouveau ou le chiffrer à chaud avec un nouveau certificat SSL pour l'équilibreur de charge vers la connexion StorageGRID. Ou vous pouvez passer par le trafic et laisser StorageGRID être le point de terminaison SSL. Si l'équilibreur de charge est le noeud final de terminaison SSL, le certificat est installé sur l'équilibreur de charge et contient le nom du sujet pour le nom DNS/l'URL et tout autre nom URL/DNS pour lequel un client est configuré pour se connecter à la cible StorageGRID via l'équilibreur de charge, y compris les noms de caractères génériques. Si l'équilibreur de charge est configuré pour l'intercommunication, le certificat SSL doit être installé dans StorageGRID. Encore une fois, le certificat doit contenir le nom de l'objet du nom DNS/URL, ainsi que tous les autres noms URL/DNS pour lesquels un client est configuré pour se connecter à la cible StorageGRID via l'équilibreur de charge, y compris les noms de caractères génériques. Il n'est pas nécessaire d'inclure les noms de nœud de stockage individuel sur le certificat, mais uniquement les URL de point final.

Configurez un équilibreur de charge tiers fiable dans StorageGRID

Découvrez comment configurer un équilibreur de charge tiers fiable dans StorageGRID.

Si vous utilisez un ou plusieurs équilibreurs de charge de couche 7 externes et une règle de compartiment S3 ou de groupe basée sur IP, StorageGRID doit déterminer l'adresse IP de l'expéditeur réel. Pour ce faire, il examine l'en-tête X-Forided-for (XFF), qui est inséré dans la demande par l'équilibreur de charge. Étant donné que l'en-tête XFF peut facilement être usurpé dans les requêtes envoyées directement aux nœuds de stockage, StorageGRID doit confirmer que chaque demande est routée par un équilibreur de charge de niveau 7 approuvé. Si StorageGRID ne peut pas faire confiance à la source de la demande, il ignore l'en-tête XFF. Une API de gestion du grid permet de configurer une liste d'équilibreurs de charge externes de couche 7 approuvés. Cette nouvelle API est privée et est susceptible d'être modifiée dans les prochaines versions d'StorageGRID. Pour obtenir les informations les plus récentes, consultez l'article de la base de connaissances, "Comment configurer StorageGRID pour qu'il fonctionne avec des équilibreurs de charge tiers de couche 7".

En savoir plus sur les équilibreurs de charge du gestionnaire de trafic local

Explorez les conseils pour les équilibreurs de charge du gestionnaire de trafic local et déterminez la configuration optimale.

Vous trouverez ci-dessous des conseils généraux pour la configuration d'équilibreurs de charge tiers. Déterminez avec votre administrateur d'équilibreur de charge la configuration optimale pour votre environnement.

Créez un groupe de ressources de nœuds de stockage

Regroupez les nœuds de stockage StorageGRID dans un pool de ressources ou un groupe de services (la terminologie peut varier en fonction des équilibreurs de charge). Les nœuds de stockage StorageGRID présentent l'API S3 sur les ports suivants :

- HTTPS S3 : 18082
- S3 HTTP : 18084

La plupart des clients choisissent de présenter les API sur le serveur virtuel via les ports HTTPS et HTTP standard (443 et 80).

> Chaque site StorageGRID requiert une valeur par défaut de trois nœuds de stockage, deux d'entre eux devant être sains.

Vérification de l'état

Les équilibreurs de charge tiers ont besoin d'une méthode pour déterminer l'état de santé de chaque nœud et son éligibilité à la réception du trafic. NetApp recommande la méthode HTTP `OPTIONS` pour effectuer la vérification de l'état. L'équilibreur de charge envoie des requêtes HTTP `OPTIONS` à chaque nœud de stockage et attend une `200` réponse d'état.

Si aucun nœud de stockage ne fournit `200` de réponse, ce nœud ne peut pas traiter les demandes de stockage. Les exigences de vos applications et de votre entreprise doivent déterminer le délai d'attente de ces vérifications et les actions que votre équilibreur de charge prend.

Par exemple, si trois des quatre nœuds de stockage du data Center 1 sont en panne, vous pouvez diriger l'ensemble du trafic vers le data Center 2.

L'intervalle d'interrogation recommandé est d'une fois par seconde, marquant le nœud hors ligne après trois échecs de vérification.

Exemple de vérification de l'état S3

Dans l'exemple suivant, nous envoyons `OPTIONS` et vérifions pour `200 OK`. Nous l'utilisons `OPTIONS` car Amazon S3) ne prend pas en charge les requêtes non autorisées.

```
curl -X OPTIONS https://10.63.174.75:18082 --verbose --insecure
* Rebuilt URL to: https://10.63.174.75:18082/
*   Trying 10.63.174.75...
* TCP_NODELAY set
* Connected to 10.63.174.75 (10.63.174.75) port 18082 (#0)
* TLS 1.2 connection using TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
* Server certificate: webscale.stl.netapp.com
* Server certificate: NetApp Corp Issuing CA 1
* Server certificate: NetApp Corp Root CA
> OPTIONS / HTTP/1.1
```

```
> Host: 10.63.174.75:18082
> User-Agent: curl/7.51.0
> Accept: /
>
< HTTP/1.1 200 OK
< Date: Mon, 22 May 2017 15:17:30 GMT
< Connection: KEEP-ALIVE
< Server: StorageGRID/10.4.0
< x-amz-request-id: 3023514741
```

Vérifications de l'état des fichiers ou des contenus

En général, NetApp ne recommande pas de vérifications de l'état des systèmes basées sur des fichiers. En général, un petit fichier —`healthcheck.htm`, par exemple, est créé dans un compartiment avec une règle en lecture seule. Ce fichier est ensuite récupéré et évalué par l'équilibreur de charge. Cette approche présente plusieurs inconvénients :

- **Dépendant d'un seul compte.** Si le compte propriétaire du fichier est désactivé, le bilan de santé échoue et aucune demande de stockage n'est traitée.
- **Règles de protection des données.** Par défaut, le schéma de protection des données est une approche à deux copies. Dans ce scénario, si les deux nœuds de stockage hébergeant le fichier de vérification de l'état sont indisponibles, la vérification de l'état échoue et les demandes de stockage ne sont pas envoyées aux nœuds de stockage sains, ce qui rend la grille hors ligne.
- **Bloat du journal d'audit.** L'équilibreur de charge extrait le fichier de chaque nœud de stockage toutes les X minutes, créant ainsi de nombreuses entrées de journal d'audit.
- **Ressource intensive.** L'extraction du fichier de vérification de l'état de santé de chaque nœud toutes les quelques secondes consomme des ressources de réseau et de grille.

Si un contrôle de l'état basé sur le contenu est nécessaire, utilisez un locataire dédié avec un compartiment S3 dédié.

Persistance de la session

La persistance de session, ou persistance, fait référence à la durée pendant laquelle une session HTTP donnée est autorisée à persister. Par défaut, les sessions sont supprimées par les nœuds de stockage au bout de 10 minutes. Une persistance plus longue peut améliorer les performances, car les applications n'ont pas besoin de rétablir leurs sessions pour chaque action. Cependant, garder ces sessions ouvertes consomme des ressources. Si vous déterminez que votre charge de travail sera avantageuse, vous pouvez réduire la persistance des sessions sur un équilibreur de charge tiers.

Adressage virtuel de type hébergé

La méthode par défaut d'AWS S3 est désormais de type hébergement virtuel. StorageGRID et de nombreuses applications prennent toujours en charge le style de chemin, mais il est recommandé d'implémenter la prise en charge de type hébergement virtuel. Les demandes de type hébergement virtuel disposent du compartiment dans le nom de l'hôte.

Pour prendre en charge le style hébergé virtuel, procédez comme suit :

- Prend en charge les recherches DNS génériques : *.s3.company.com

- Utilisez un certificat SSL avec des noms alt d'objet pour prendre en charge le caractère générique : *.s3.company.com certains clients ont exprimé des préoccupations de sécurité concernant l'utilisation de certificats génériques. StorageGRID continue de prendre en charge l'accès de type chemin, tout comme les applications clés telles que FabricPool. Ceci étant dit, certains appels de l'API S3 échouent ou se comportent de manière incorrecte sans prise en charge hébergée virtuelle.

Terminaison SSL

La terminaison SSL présente des avantages en termes de sécurité sur les équilibreurs de charge tiers. Si l'équilibreur de charge est compromis, le grid est compartimenté.

Trois configurations sont prises en charge :

- **Pass-through SSL.** Le certificat SSL est installé sur StorageGRID en tant que certificat de serveur personnalisé.
- **Terminaison et re-cryptage SSL (recommandé).** Cela peut être bénéfique si vous effectuez déjà la gestion des certificats SSL sur l'équilibreur de charge plutôt que d'installer le certificat SSL sur StorageGRID. Cette configuration offre l'avantage de sécurité supplémentaire de limiter la surface d'attaque à l'équilibreur de charge.
- **Terminaison SSL avec HTTP.** Dans cette configuration, SSL est interrompu sur l'équilibreur de charge tiers et la communication entre l'équilibreur de charge et StorageGRID n'est pas chiffrée pour tirer parti du déchargement SSL (avec les bibliothèques SSL intégrées dans les processeurs modernes, cela présente un avantage limité).

Configuration de passage

Si vous préférez configurer votre équilibreur de charge pour le transfert, vous devez installer le certificat sur StorageGRID. Accédez au **Configuration › certificats de serveur › noeuds finaux du service API de stockage objet certificat de serveur**.

Visibilité IP du client source

StorageGRID 11.4 a introduit le concept d'équilibreur de charge tiers fiable. Pour transférer l'adresse IP de l'application client vers StorageGRID, vous devez configurer cette fonction. Pour plus d'informations, voir "Comment configurer StorageGRID pour qu'il fonctionne avec des équilibreurs de charge tiers de couche 7."

Pour activer l'en-tête XFF pour afficher l'adresse IP de l'application client, procédez comme suit :

Étapes

1. Enregistrez l'adresse IP du client dans le journal d'audit.
2. Utilisez `aws:SourceIp` un compartiment S3 ou une règle de groupe.

Stratégies d'équilibrage de charge

La plupart des solutions d'équilibrage de charge offrent plusieurs stratégies d'équilibrage de charge. Les stratégies courantes sont les suivantes :

- **Robin rond.** Une solution universelle, mais avec peu de nœuds et de grands transferts obstruant les nœuds uniques.
- **Connexion minimale.** Convient parfaitement aux charges de travail mixtes et de petite taille qui offrent une distribution égale des connexions à tous les nœuds.

Le choix de l'algorithme devient moins important, car le nombre de nœuds de stockage est de plus en plus important.

Chemin d'accès aux données

Les données transitent par les équilibreurs de charge du gestionnaire de trafic local. StorageGRID ne prend pas en charge le routage direct de serveur (DSR).

Vérification de la distribution des connexions

Pour vérifier que votre méthode répartit la charge uniformément entre les nœuds de stockage, vérifiez les sessions établies sur chaque nœud d'un site donné :

- **Méthode UI.** Aller au **support › Metrics › S3 Overview › LDR HTTP sessions**
- **API métriques.** Utilisation `storagegrid_http_sessions_incoming_currently_established`

Découvrez quelques utilisations des configurations StorageGRID

Explorez les quelques cas d'utilisation des configurations StorageGRID mises en œuvre par les clients et PAR NetApp IT.

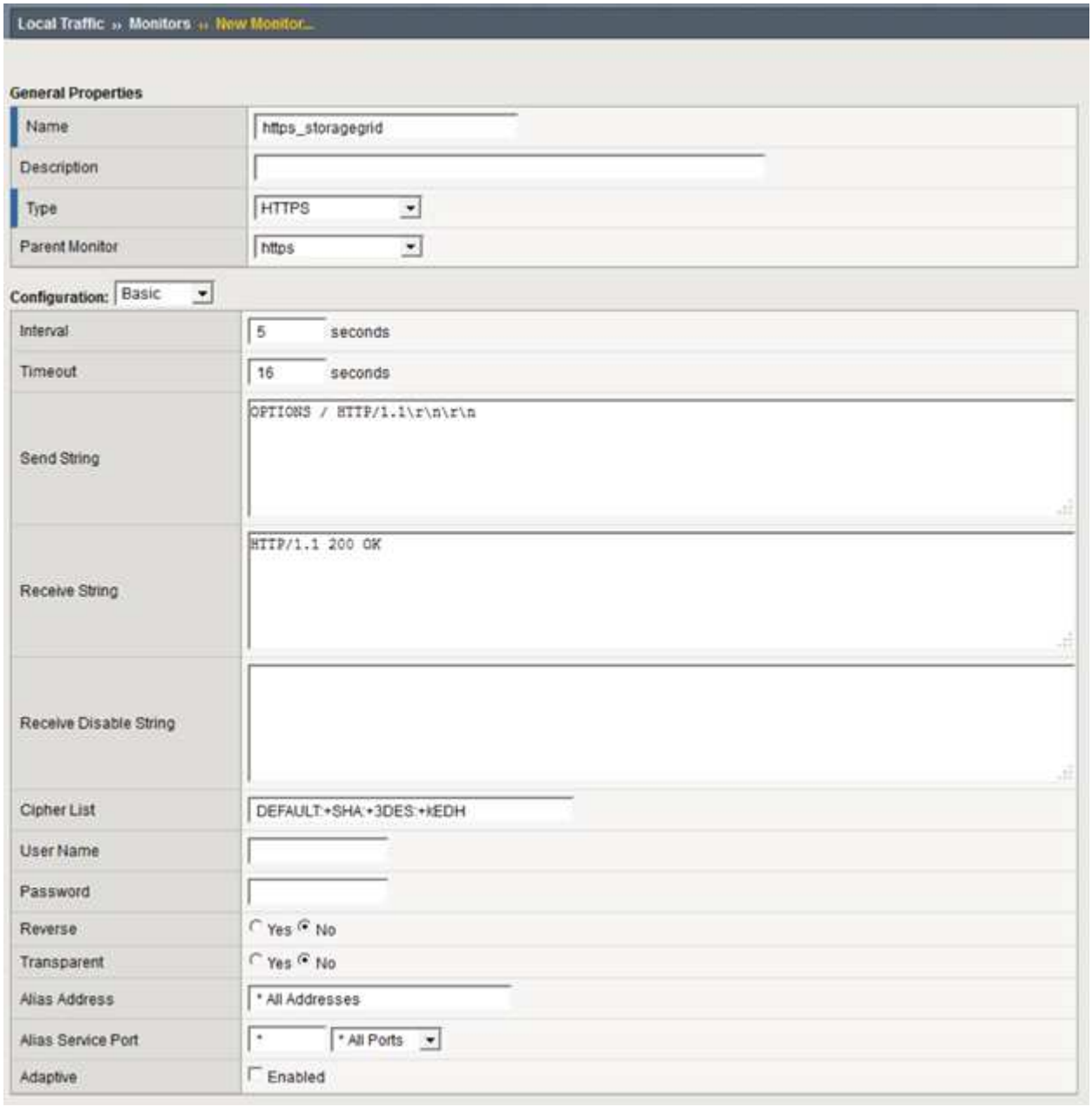
Les exemples suivants illustrent les configurations mises en œuvre par les clients StorageGRID, y compris NetApp IT.

Contrôle DE l'état du gestionnaire du trafic local BIG-IP de F5 pour le compartiment S3

Pour configurer le moniteur de vérification de l'état du gestionnaire de trafic local BIG-IP F5, procédez comme suit :

Étapes

1. Créer un nouveau moniteur.
   a. Dans le champ Type, entrez `HTTPS`.
   b. Configurez l'intervalle et le délai d'attente comme vous le souhaitez.
   c. Dans le champ Envoyer chaîne, entrez `OPTIONS / HTTP/1.1\r\n\r\n`. \r\n sont des retours chariot ; les différentes versions du logiciel BIG-IP nécessitent zéro, un ou deux ensembles de séquences \r\n. Pour plus d'informations, voir https://support.f5.com/csp/article/K10655.
   d. Dans le champ chaîne de réception, entrez : `HTTP/1.1 200 OK`.



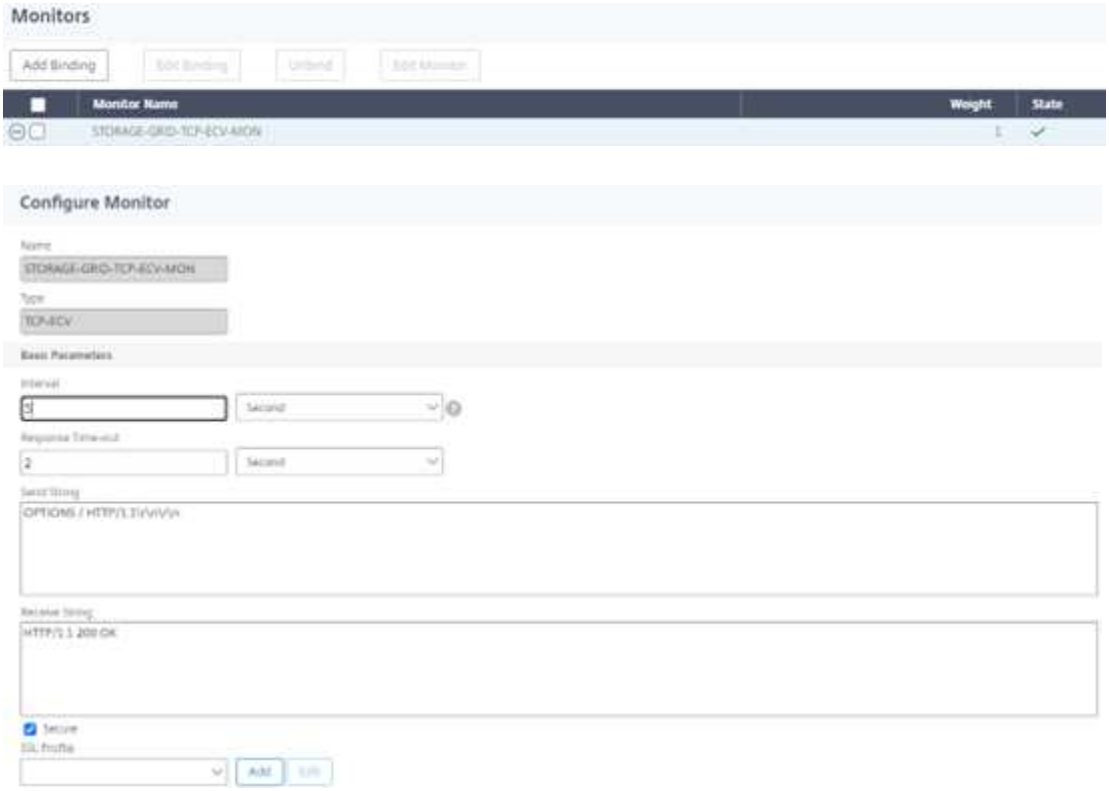
2. Dans Créer un pool, créez un pool pour chaque port requis.
   a. Attribuez le contrôle de l'état que vous avez créé à l'étape précédente.
   b. Sélectionnez une méthode d'équilibrage de charge.
   c. Sélectionnez le port de service : 18082 (S3).
   d. Ajouter des nœuds.

Citrix NetScaler

Citrix NetScaler crée un serveur virtuel pour le terminal de stockage et fait référence aux nœuds de stockage StorageGRID en tant que serveurs d'applications, qui sont ensuite regroupés dans des services.

Utilisez le moniteur de vérification de l'état de santé HTTPS-ECV pour créer un moniteur personnalisé afin d'effectuer le contrôle de l'état de santé recommandé en utilisant les OPTIONS demande et réception `200`. HTTP-ECV est configuré avec une chaîne d'envoi et valide une chaîne de réception.

Pour plus d'informations, consultez la documentation Citrix, "Exemple de configuration pour le moniteur de vérification de l'état HTTP-ECV".



Loadbalancer.org

Loadbalancer.org a réalisé ses propres tests d'intégration avec StorageGRID et dispose d'un guide de configuration complet : https://pdfs.loadbalancer.org/NetApp_StorageGRID_Deployment_Guide.pdf.

Kemp

Kemp a réalisé ses propres tests d'intégration avec StorageGRID et dispose d'un guide de configuration complet : https://kemptechnologies.com/solutions/netapp/.

HABProxy

Configurez HANProxy pour utiliser la demande d'OPTIONS et vérifiez la réponse d'état 200 pour le contrôle d'intégrité dans haproxy.cfg. Vous pouvez remplacer le port de liaison de l'interface frontale par un autre port, tel que 443.

Voici un exemple de terminaison SSL sur HASProxy :

```
frontend s3
       bind *:443 crt /etc/ssl/server.pem ssl
       default_backend s3-serve
rs
backend s3-servers
       balance leastconn
       option httpchk
```

```
        http-check expect status 200
        server dc1-s1 10.63.174.71:18082 ssl verify none check inter 3000
        server dc1-s2 10.63.174.72:18082 ssl verify none check inter 3000
        server dc1-s3 10.63.174.73:18082 ssl verify none check inter 3000
```

Voici un exemple de pass-through SSL :

```
frontend s3
        mode tcp
        bind *:443
        default_backend s3-servers
backend s3-servers
        balance leastconn
        option httpchk
        http-check expect status 200
        server dc1-s1 10.63.174.71:18082 check-ssl verify none inter 3000
        server dc1-s2 10.63.174.72:18082 check-ssl verify none inter 3000
        server dc1-s3 10.63.174.73:18082 check-ssl verify none inter 3000
```

Pour obtenir des exemples complets de configurations pour StorageGRID, reportez-vous à la section "Exemples de configuration HANProxy" sur GitHub.

Valider la connexion SSL dans StorageGRID

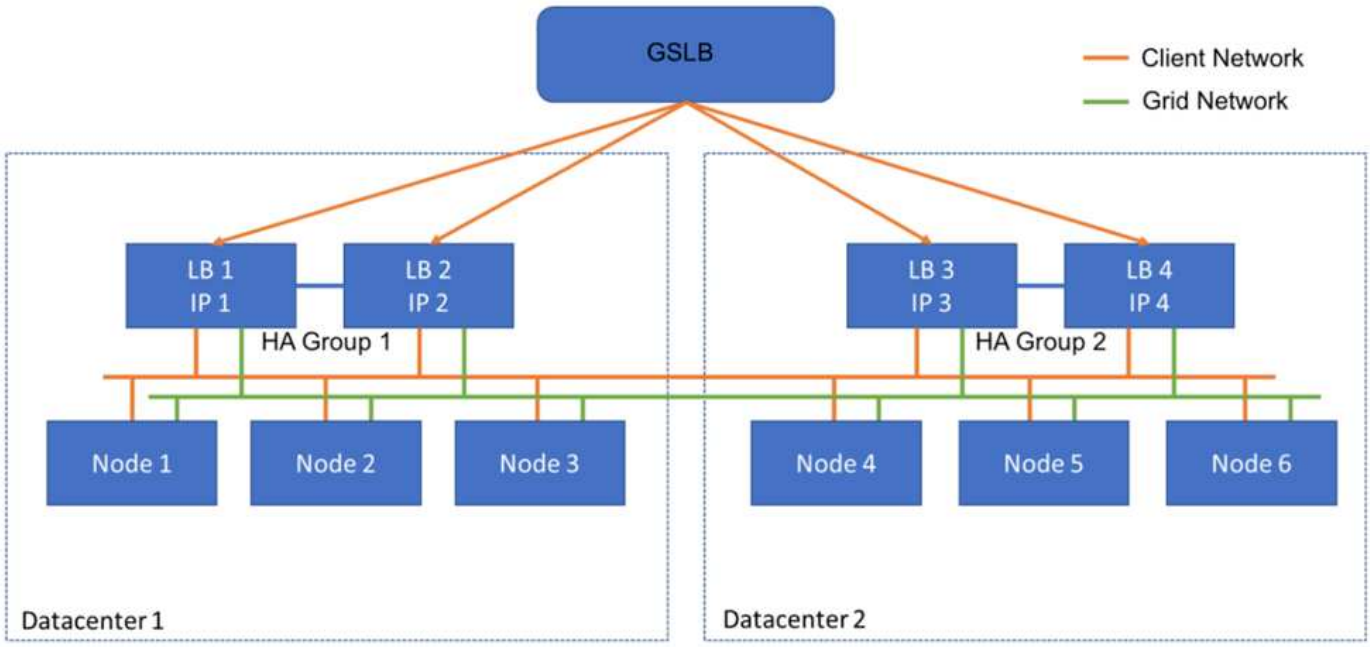
Apprenez à valider la connexion SSL dans StorageGRID.

Une fois votre équilibreur de charge configuré, vous devez valider la connexion à l'aide d'outils tels que OpenSSL et l'interface de ligne de commande AWS. D'autres applications, telles que le navigateur S3, peuvent ignorer les erreurs de configuration SSL.

Comprendre les exigences globales d'équilibrage de charge pour StorageGRID

Explorez les considérations et exigences de conception pour l'équilibrage global de la charge dans StorageGRID.

L'équilibrage global de la charge nécessite l'intégration à DNS pour assurer un routage intelligent sur plusieurs sites StorageGRID. Cette fonction ne relève pas du domaine StorageGRID et doit être fournie par une solution tierce, telle que les produits d'équilibrage de charge mentionnés précédemment et/ou une solution de contrôle du trafic DNS telle qu'Infoblox. Cet équilibrage de charge de niveau supérieur assure le routage intelligent vers le site de destination le plus proche dans l'espace de noms, ainsi que la détection des pannes et la redirection vers le site suivant dans l'espace de noms. Une implémentation GSLB type consiste en un GSLB de niveau supérieur avec des pools de site contenant des équilibreurs de charge site-local. Les équilibreurs de charge de site contiennent des pools de nœuds de stockage sur site local. Cela peut inclure une combinaison d'équilibreurs de charge tiers pour les fonctions GSLB et de StorageGRID fournissant l'équilibrage de charge site-local, ou une combinaison de tiers. Un grand nombre de tiers évoqués précédemment peuvent fournir à la fois un équilibrage de charge GSLB et site-local.



Tr-4645 : fonctions de sécurité

Sécurisation des données et des métadonnées StorageGRID dans un magasin d'objets

Découvrez les fonctions de sécurité intégrées à la solution de stockage objet StorageGRID.

Il s'agit d'un aperçu des nombreuses fonctionnalités de sécurité de NetApp® StorageGRID®, couvrant l'accès aux données, les objets et les métadonnées, l'accès administratif et la sécurité de la plate-forme. Il a été mis à jour pour inclure les dernières fonctionnalités publiées avec StorageGRID 12.0.

La sécurité fait partie intégrante de la solution de stockage objet NetApp StorageGRID. La sécurité est particulièrement importante, car de nombreux types de données riches bien adaptées au stockage objet sont également sensibles, soumises aux réglementations et à la conformité. À mesure que les fonctionnalités StorageGRID continuent d'évoluer, le logiciel met à disposition de nombreuses fonctionnalités de sécurité précieuses pour protéger la stratégie de sécurité de l'entreprise et aider l'entreprise à respecter les bonnes pratiques du secteur.

Cet article présente un aperçu des nombreuses fonctionnalités de sécurité de StorageGRID 12.0, divisées en cinq catégories :

- Sécurité de l'accès aux données
- Fonctionnalités de sécurité des objets et des métadonnées
- Fonctions de sécurité de l'administration
- Fonctions de sécurité de la plate-forme
- Intégration au cloud

Ce document est destiné à être une fiche technique de sécurité : il ne détaille pas comment configurer le système pour prendre en charge les fonctionnalités de sécurité énumérées qui ne sont pas configurées par défaut. Le "Guide de renforcement de la StorageGRID" est disponible sur le site officiel "Documentation

StorageGRID" page.

Outre les fonctionnalités décrites dans ce rapport, StorageGRID suit le "Politique de notification et de réponse aux vulnérabilités de sécurité des produits NetApp". Les vulnérabilités signalées sont vérifiées et traitées conformément au processus de réponse aux incidents de sécurité du produit.

NetApp StorageGRID fournit des fonctionnalités de sécurité avancées pour les cas d'utilisation très exigeants du stockage objet.

Où trouver des informations complémentaires

Pour en savoir plus sur les informations données dans ce livre blanc, consultez ces documents et/ou sites web :

- NetApp StorageGRID : évaluation de la conformité SEC 17a-4(f), FINRA 4511(c) et CFTC 1.31(c)-(d) https://www.netapp.com/media/9041-ar-cohasset-netapp-storagegrid-sec-assessment.pdf
- Certification cryptographique du NetApp StorageGRID NIST FIPS 140-3 https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/5097
- Certification d'entropie NetApp StorageGRID NIST SP 800-90B https://csrc.nist.gov/projects/cryptographic-module-validation-program/entropy-validations/certificate/223
- Certification Critères communs du Centre canadien de cybersécurité pour NetApp StorageGRID https://www.commoncriteriaportal.org/nfs/ccpfiles/files/epfiles/565-LSS%20CT%20v1.0.pdf
- Page de documentation de StorageGRIDhttps://docs.netapp.com/us-en/storagegrid/[]
- Documentation des produits NetApp https://www.netapp.com/support-and-training/documentation/

Termes et acronymes

Cette section fournit des définitions de la terminologie utilisée dans le document.

Terme ou acronyme	Définition
S3	Simple Storage Service.
Client	Application pouvant interagir avec StorageGRID via le protocole S3 d'accès aux données ou le protocole HTTP de gestion.
Administrateur des locataires	Administrateur du compte locataire StorageGRID
Utilisateur locataire	Utilisateur d'un compte de locataire StorageGRID
TLS	Sécurité de la couche de transport
ILM	Gestion du cycle de vie des informations
RÉSEAU LOCAL	Réseau local
Administrateur du grid	Administrateur du système StorageGRID
Grille	Le système StorageGRID
Godet	Un conteneur pour les objets stockés dans S3
LDAP	Protocole d'accès à l'annuaire simplifié
SEC	Securities and Exchange Commission; réglemente les membres de change, les courtiers ou les courtiers

Terme ou acronyme	Définition
FINRA	Autorité de réglementation du secteur financier ; diffère des exigences de format et de support de la règle SEC 17a-4(f)
CFTC	Commissions sur les opérations à terme sur les matières premières; réglemente les opérations à terme sur les matières premières
NIST	Institut national des normes et de la technologie

Sécurité de l’accès aux données

Découvrez les fonctionnalités de sécurité d’accès aux données de StorageGRID.

Fonction	Fonction	Impact	Conformité réglementaire
TLS (transport Layer Security) configurable	TLS établit un protocole de liaison pour la communication entre un client et un nœud de passerelle StorageGRID, un nœud de stockage ou un point d'extrémité d'équilibreur de charge. StorageGRID prend en charge les suites de chiffrement suivantes pour TLS : • TLS_AES_256_GCM_SHA384 • TLS_AES_128_GCM_SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • TLS_AES_256_GCM_SHA384 • DHE-RSA-AES128-GCM-SHA256 • DHE-RSA-AES256-GCM-SHA384 • AES256-GCM-SHA384 • AES128-GCM-SHA256 • TLS_CHACHA20_POLY1305_SHA256 • ECDHE-ECDSA-CHACHA20-POLY1305 • ECDHE-RSA-CHACHA20-POLY1305 TLS v1.2 et 1.3 pris en charge. SSLv3, TLS v1.1 et les versions antérieures ne sont pas pris en charge.	Permet à un client et à StorageGRID de s'identifier et de s'authentifier mutuellement et de communiquer avec confidentialité et intégrité des données. Garantit l'utilisation d'une version TLS récente. Les chiffrements sont désormais configurables sous les paramètres de configuration/sécurité	—

Fonction	Fonction	Impact	Conformité réglementaire
Certificat de serveur configurable (noeud final Load Balancer)	Les administrateurs du grid peuvent configurer les noeuds finaux Load Balancer pour générer ou utiliser un certificat de serveur.	Permet l'utilisation de certificats numériques signés par leur autorité de certification approuvée standard pour authentifier les opérations d'API d'objet entre la grille et le client par point final Load Balancer.	—
Certificat de serveur configurable (terminal API)	Les administrateurs du grid peuvent configurer de manière centralisée tous les terminaux de l'API StorageGRID pour qu'ils utilisent un certificat de serveur signé par l'autorité de certification de confiance de leur entreprise.	Permet l'utilisation de certificats numériques signés par leur autorité de certification standard de confiance pour authentifier les opérations de l'API objet entre un client et la grille.	—

Fonction	Fonction	Impact	Conformité réglementaire
Colocation	StorageGRID prend en charge plusieurs locataires par grille ; chaque locataire dispose de son propre espace de noms. Un locataire utilise le protocole S3. Par défaut, l'accès aux compartiments/conteneurs et aux objets est limité aux utilisateurs au sein du compte. Les locataires peuvent avoir un utilisateur (par exemple, un déploiement d'entreprise, dans lequel chaque utilisateur a son propre compte) ou plusieurs utilisateurs (par exemple, un déploiement de fournisseur de services, dans lequel chaque compte est une entreprise et un client du fournisseur de services). Les utilisateurs peuvent être locaux ou fédérés. Les utilisateurs fédérés sont définis par Active Directory ou LDAP (Lightweight Directory Access Protocol). StorageGRID fournit un tableau de bord par locataire, dans lequel les utilisateurs se connectent à l'aide de leurs informations d'identification de compte locales ou fédérées. Les utilisateurs peuvent accéder à des rapports visualisés sur l'utilisation des locataires par rapport au quota attribué par l'administrateur de la grille, y compris des informations d'utilisation dans les données et objets stockés par compartiments. Les utilisateurs disposant d'autorisations administratives peuvent effectuer des tâches d'administration système au niveau du locataire, telles que la gestion des utilisateurs et des groupes et des clés d'accès.	Permet aux administrateurs StorageGRID d'héberger les données de plusieurs locataires tout en isolant l'accès des locataires et d'établir l'identité des utilisateurs en fédérant les utilisateurs avec un fournisseur d'identité externe, tel qu'Active Directory ou LDAP.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)

Fonction	Fonction	Impact	Conformité réglementaire
Non-répudiation des identifiants d'accès	Chaque opération S3 est identifiée et consignée à l'aide d'un compte de locataire, d'un utilisateur et d'une clé d'accès uniques.	Permet aux administrateurs du grid d'établir les actions d'API exécutées par des individus.	—
Accès anonyme désactivé	Par défaut, l'accès anonyme est désactivé pour les comptes S3. Un demandeur doit disposer d'un droit d'accès valide pour qu'un utilisateur valide du compte de tenant puisse accéder aux compartiments, conteneurs ou objets du compte. L'accès anonyme aux compartiments ou objets S3 peut être activé avec une règle IAM explicite.	Permet aux administrateurs de Grid de désactiver ou de contrôler l'accès anonyme aux compartiments/conteneurs et objets.	—
Conformité WORM	Conçu pour répondre aux exigences de la règle SEC 17a-4(f) et validé par Cohasset. Les clients peuvent assurer la conformité au niveau du compartiment. La conservation peut être étendue, mais jamais réduite. Les règles de gestion du cycle de vie des informations (ILM) appliquent des niveaux minimaux de protection des données.	Permet aux locataires qui ont des exigences réglementaires en matière de conservation des données d'activer la protection WORM sur les objets stockés et les métadonnées d'objet.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)
VER	Les administrateurs du grid peuvent activer le mode WORM au niveau de la grille en activant l'option Désactiver la modification du client, qui empêche les clients d'écraser ou de supprimer des objets ou des métadonnées d'objet dans tous les comptes de locataires. Les administrateurs de locataires S3 peuvent également activer le mode WORM par locataire, compartiment ou préfixe d'objet en spécifiant une règle IAM qui inclut l'autorisation S3 : PutOverwriteObject personnalisée pour le remplacement d'objets et de métadonnées.	Permet aux administrateurs du grid et aux locataires de contrôler la protection WORM sur les objets stockés et les métadonnées d'objet.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)

Fonction	Fonction	Impact	Conformité réglementaire
Gestion des clés de cryptage du serveur hôte KM	Les administrateurs du grid peuvent configurer un ou plusieurs serveurs de gestion externe des clés (KMS) dans Grid Manager afin que les clés de chiffrement soient attribuées aux services StorageGRID et aux appliances de stockage. Chaque serveur hôte KMS ou cluster de serveurs hôtes KMS utilise le protocole KMIP (Key Management Interoperability Protocol) pour fournir une clé de chiffrement aux nœuds de l'appliance sur le site StorageGRID associé.	Vous pouvez chiffrer les données au repos. Une fois les volumes de l'appliance chiffrés, vous ne pouvez pas accéder aux données de l'appliance sauf si le nœud peut communiquer avec le serveur hôte KMS.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)
Basculement automatique	StorageGRID fournit une redondance intégrée et un basculement automatisé. L'accès aux comptes de locataires, aux compartiments et aux objets peut continuer même en cas de pannes multiples, depuis des disques ou des nœuds jusqu'à des sites entiers. StorageGRID est conscient des ressources et redirige automatiquement les requêtes vers les nœuds disponibles et les emplacements de données. Les sites StorageGRID peuvent même fonctionner en mode iskattered. En cas de panne de réseau étendu, un site est déconnecté du reste du système, les lectures et écritures peuvent continuer avec les ressources locales, et la réplication reprend automatiquement lorsque le réseau WAN est restauré.	Permet aux administrateurs du grid de répondre aux exigences de disponibilité, aux contrats de niveau de service et aux autres obligations contractuelles et de mettre en œuvre des plans de continuité de l'activité.	—

Fonction	Fonction	Impact	Conformité réglementaire
Fonctions de sécurité d'accès aux données spécifiques à S3	Signature AWS version 2 et version 4	La signature des requêtes d'API permet d'authentifier les opérations de l'API S3. Amazon prend en charge deux versions de Signature version 2 et version 4. Le processus de signature vérifie l'identité du demandeur, protège les données en transit et les protège contre les attaques de relecture potentielles.	S'aligne sur la recommandation AWS pour Signature version 4 et permet une rétrocompatibilité avec les anciennes applications avec Signature version 2.
—	Verrouillage d'objet S3	La fonctionnalité de verrouillage objet S3 d'StorageGRID est une solution de protection objet équivalente au verrouillage objet S3 dans Amazon S3.	Permet aux locataires de créer des compartiments avec S3 Object Lock activé pour se conformer aux réglementations exigeant la conservation de certains objets pendant une durée fixe ou indéfiniment.
Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)	Stockage sécurisé des identifiants S3	Les clés d'accès S3 sont stockées dans un format protégé par une fonction de hachage des mots de passe (SHA-2).	Permet le stockage sécurisé des clés d'accès par une combinaison de longueur de clé (un nombre généré de manière aléatoire de 10^{31}) et d'un algorithme de hachage de mot de passe.
—	Clés d'accès S3 limitées dans le temps	Lorsque vous créez une clé d'accès S3 pour un utilisateur, les clients peuvent définir une date et une heure d'expiration sur la clé d'accès.	Permet aux administrateurs du grid de provisionner des clés d'accès S3 temporaires.
—	Plusieurs clés d'accès par compte d'utilisateur	StorageGRID permet de créer plusieurs clés d'accès et de les activer simultanément pour un compte utilisateur. Chaque action d'API étant consignée avec un compte utilisateur de locataire et une clé d'accès, la non-répudiation est préservée même si plusieurs clés sont actives.	Permet aux clients de faire pivoter les clés d'accès sans interruption et à chaque client d'avoir sa propre clé, décourageant ainsi le partage des clés entre les clients.

Fonction	Fonction	Impact	Conformité réglementaire
—	Règle d’accès IAM S3	StorageGRID prend en charge les règles IAM S3, ce qui permet aux administrateurs du grid de spécifier le contrôle d’accès granulaire par locataire, compartiment ou préfixe d’objet. StorageGRID prend également en charge les conditions et les variables des règles IAM, ce qui permet des règles de contrôle d’accès plus dynamiques.	Permet aux administrateurs de Grid de spécifier le contrôle d’accès par groupes d’utilisateurs pour l’ensemble du tenant ; permet également aux utilisateurs locataires de spécifier le contrôle d’accès pour leurs propres compartiments et objets.
—	API du service de jeton de sécurité S3 AssumeRole	StorageGRID prend en charge l’API S3 STS AssumeRole pour fournir des informations d’identification de sécurité temporaires (ID de clé d’accès, clé d’accès secrète, jeton de session) avec des autorisations réduites et une durée limitée. Les stratégies de session en ligne permettant de restreindre davantage les autorisations pendant la session sont prises en charge dans le cadre de l’API AssumeRole.	Permet aux administrateurs locataires de fournir un accès temporaire sécurisé aux données de l’objet.

Fonction	Fonction	Impact	Conformité réglementaire
—	Service de notification simple	StorageGRID prend en charge l'envoi de notifications lors de l'accès aux objets. Les types d'événements suivants sont pris en charge : • s3 : Objet créé : • s3:ObjetCréé:Mettre • s3 : Objet créé : Publication • s3:ObjetCréé:Copier • s3 : Objet créé : Téléchargement multi-parties complet • s3 : Objet supprimé : • s3:ObjectRemoved:Supprimer • s3 : Objet supprimé : Supprimer le marqueur créé • s3 : Restauration d'objet : Publication	Permet aux administrateurs locataires de surveiller l'accès aux objets
—	Chiffrement côté serveur avec clés gérées par StorageGRID (SSE)	StorageGRID prend en charge SSE, ce qui permet une protection mutualisée des données au repos avec des clés de chiffrement gérées par StorageGRID.	Permet aux locataires de chiffrer les objets. Une clé de chiffrement est requise pour écrire et récupérer ces objets.
Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)	Chiffrement côté serveur avec clés de chiffrement fournies par le client (SSE-C)	StorageGRID prend en charge SSE-C, ce qui permet une protection mutualisée des données au repos avec des clés de chiffrement gérées par le client. Bien que StorageGRID gère toutes les opérations de chiffrement et de déchiffrement d'objets, avec SSE-C, le client doit gérer les clés de cryptage lui-même.	Permet aux clients de chiffrer les objets avec des clés qu'ils contrôlent. Une clé de chiffrement est requise pour écrire et récupérer ces objets.

Sécurité des objets et des métadonnées

Explorez les fonctionnalités de sécurité des objets et des métadonnées de StorageGRID.

Fonction	Fonction	Impact	Conformité réglementaire
Advanced Encryption Standard (AES) - chiffrement d'objets côté serveur	StorageGRID assure le chiffrement des objets côté serveur basé sur AES 128 et AES 256. Les administrateurs du grid peuvent activer le chiffrement comme paramètre global par défaut. StorageGRID prend également en charge l'en-tête de chiffrement S3 x-amz côté serveur pour activer ou désactiver le chiffrement par objet. Lorsque cette option est activée, les objets sont chiffrés lorsqu'ils sont stockés ou en transit entre des nœuds de grid.	Stockage et transmission sécurisés d'objets, indépendamment du matériel de stockage sous-jacent.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)
Gestion intégrée des clés	Lorsque le chiffrement est activé, chaque objet est chiffré avec une clé symétrique unique générée de manière aléatoire, stockée dans StorageGRID sans accès externe.	Permet le chiffrement des objets sans gestion externe des clés.	
Disques de chiffrement conformes à la norme FIPS (Federal information Processing Standard) 140-2	Les appliances StorageGRID SG5812, SG5860, SG6160 et SGF6024 offrent la possibilité d'utiliser des disques de chiffrement conformes à la norme FIPS 140-2. Les clés de chiffrement des disques peuvent être gérées par un serveur KMIP externe.	Stockage sécurisé des données, métadonnées et objets du système. Le chiffrement logiciel des objets StorageGRID sécurise le stockage et la transmission des objets.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)
Cryptage conforme à la norme FIPS (Federal Information Processing Standard) 140-3 pour les nœuds	Les appliances StorageGRID SG5812, SG5860, SG6160, SGF6112, SG1100 et SG110 offrent l'option de chiffrement de nœud conforme à la norme FIPS 140-3. Les clés de chiffrement des nœuds sont gérées par un serveur KMIP externe.	Stockage sécurisé des données, métadonnées et objets du système. Le chiffrement logiciel des objets StorageGRID sécurise le stockage et la transmission des objets.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)

Fonction	Fonction	Impact	Conformité réglementaire
Analyse de l'intégrité en arrière-plan et auto-rétablissement	StorageGRID utilise un mécanisme d'interverrouillage de hachages, de checksums et de vérifications de la redondance cyclique (CRC) au niveau de l'objet et des sous-objets pour se protéger contre l'incohérence, la falsification ou la modification des données, aussi bien lorsque les objets sont en stockage qu'en transit. StorageGRID détecte automatiquement les objets corrompus et falsifiés et les remplace, tout en mettant en quarantaine les données modifiées et en alertant l'administrateur.	Permet aux administrateurs du grid de respecter les SLA, les réglementations et autres obligations en matière de durabilité des données. Aide les clients à détecter les ransomwares ou les virus qui tentent de chiffrer, d'altérer ou de modifier des données.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)
Placement et conservation des objets basés sur des règles	StorageGRID permet aux administrateurs du grid de configurer des règles ILM, qui spécifient la conservation, le placement, la protection, la transition et l'expiration des objets. Les administrateurs du grid peuvent configurer StorageGRID pour filtrer les objets en fonction de leurs métadonnées et appliquer des règles à différents niveaux de granularité, notamment à l'échelle du grid, du locataire, du compartiment, du préfixe de clé et des paires clé-valeur de métadonnées définies par l'utilisateur. StorageGRID permet de s'assurer que les objets sont stockés conformément aux règles ILM tout au long de leur cycle de vie, à moins qu'ils ne soient explicitement supprimés par le client.	Renforce le placement, la protection et la conservation des données. Aide les clients à respecter les SLA en matière de durabilité, de disponibilité et de performance.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)
Analyse des métadonnées en arrière-plan	StorageGRID analyse régulièrement les métadonnées d'objet en arrière-plan pour appliquer des modifications au placement ou à la protection des données d'objet, comme spécifié par la règle ILM.	Permet de détecter les objets corrompus.	

Fonction	Fonction	Impact	Conformité réglementaire
Cohérence ajustable	Les locataires peuvent sélectionner des niveaux de cohérence au niveau du compartiment pour s'assurer que les ressources, telles que la connectivité multisite, sont disponibles.	Offre la possibilité d'effectuer des écritures dans la grille uniquement lorsqu'un nombre requis de sites ou de ressources est disponible.	

Fonctions de sécurité de l'administration

Découvrez les fonctions de sécurité d'administration de StorageGRID.

Fonction	Fonction	Impact	Conformité réglementaire
Certificat de serveur (interface de gestion Grid)	Les administrateurs du grid peuvent configurer l'interface de gestion Grid pour utiliser un certificat de serveur signé par l'autorité de certification approuvée de leur organisation.	Permet l'utilisation de certificats numériques signés par leur autorité de certification standard et approuvée pour authentifier l'accès à l'interface utilisateur de gestion et à l'API entre un client de gestion et la grille.	—
Authentification utilisateur administrative	Les utilisateurs administratifs sont authentifiés à l'aide du nom d'utilisateur et du mot de passe. Les utilisateurs et groupes administratifs peuvent être locaux ou fédérés, importés depuis Active Directory ou LDAP du client. Les mots de passe des comptes locaux sont stockés dans un format protégé par bcrypt ; les mots de passe de ligne de commande sont stockés dans un format protégé par SHA-2.	Authentifie l'accès administratif à l'interface utilisateur de gestion et aux API.	—

Fonction	Fonction	Impact	Conformité réglementaire
Prise en charge SAML	StorageGRID prend en charge l'authentification unique (SSO) à l'aide de la norme SAML 2.0 (Security assertion Markup Language 2.0). Lorsque l'authentification SSO est activée, tous les utilisateurs doivent être authentifiés par un fournisseur d'identités externe avant d'accéder au Grid Manager, au tenant Manager, à l'API Grid Management ou à l'API de gestion des locataires. Les utilisateurs locaux ne peuvent pas se connecter à StorageGRID.	Niveaux de sécurité supplémentaires pour les administrateurs du grid et des locataires tels que SSO et l'authentification multifacteur (MFA)	NIST SP800-63
Contrôle granulaire des autorisations	Les administrateurs du grid peuvent attribuer des autorisations aux rôles et attribuer des rôles à des groupes d'utilisateurs administratifs, ce qui permet d'appliquer les tâches que les clients administratifs sont autorisés à effectuer à l'aide de l'interface utilisateur de gestion et des API.	Permet aux administrateurs de Grid de gérer le contrôle d'accès pour les utilisateurs et les groupes d'administration.	—

Fonction	Fonction	Impact	Conformité réglementaire
Journalisation des audits distribués	StorageGRID offre une infrastructure intégrée de journalisation des audits distribuée et évolutive pour des centaines de nœuds répartis sur un maximum de 16 sites. Les nœuds logiciels StorageGRID génèrent des messages d'audit, qui sont transmis via un système de relais d'audit redondant et finalement capturés dans un ou plusieurs référentiels de journaux d'audit. Les messages d'audit capturent les événements au niveau objet, tels que les opérations de l'API S3 initiées par le client, les événements de cycle de vie des objets par ILM, les vérifications de l'état des objets en arrière-plan et les modifications de configuration effectuées à partir de l'interface utilisateur de gestion ou des API. Les journaux d'audit peuvent être exportés par Syslog, ce qui permet aux messages d'audit d'être exploités par des outils tels que Splunk et ELK. Il existe quatre types de messages d'audit : • Messages d'audit système • Messages d'audit du stockage objet • Messages d'audit du protocole HTTP • Messages d'audit de gestion Les journaux d'audit peuvent être stockés dans un compartiment S3 pour une conservation à long terme et un accès aux applications.	Fournit aux administrateurs du grid un service d'audit évolutif et éprouvé qui leur permet d'exploiter les données d'audit pour divers objectifs. Tels que la résolution de problèmes, l'audit des performances des SLA, les opérations d'API d'accès aux données du client et les modifications de la configuration de la gestion.	—

Fonction	Fonction	Impact	Conformité réglementaire
Audit du système	Les messages d'audit du système capturent les événements liés au système, tels que l'état des nœuds de grid, la détection d'objets corrompus, les objets validés à tous les emplacements spécifiés conformément à la règle ILM et la progression des tâches de maintenance à l'échelle du système (tâches de grid).	Aide les clients à résoudre les problèmes liés aux systèmes et apporte une preuve que les objets sont stockés conformément à leur SLA. Les SLA sont implémentés par les règles ILM de StorageGRID et sont protégés contre l'intégrité.	—
Audit du stockage objet	Les messages d'audit du stockage objet capturent les transactions de l'API objet et les événements liés au cycle de vie. Ces événements incluent le stockage objet et la récupération, les transferts de nœuds grid à nœud grid et les vérifications.	Aide les clients à vérifier la progression des données dans le système et si les SLA, spécifiés dans la ILM de StorageGRID, sont livrés.	—
Audit du protocole HTTP	Les messages d'audit du protocole HTTP capturent les interactions du protocole HTTP liées aux applications clientes et aux nœuds StorageGRID. En outre, les clients peuvent capturer des en-têtes de requête HTTP spécifiques (tels que X-retransmis-for et les métadonnées utilisateur [x-amz-meta-*]) dans l'audit.	Aide les clients à auditer les opérations d'API d'accès aux données entre les clients et StorageGRID et à tracer une action sur un compte utilisateur individuel et une clé d'accès. Ils peuvent également connecter les métadonnées utilisateur à des fins d'audit et utiliser des outils de recherche de journaux, tels que Splunk ou ELK, pour rechercher des métadonnées objet.	—
Audit de gestion	Les messages d'audit de gestion consignent les demandes des utilisateurs administrateurs dans l'interface de gestion (Grid Management interface) ou les API. Chaque requête qui n'est pas une requête GET ou HEAD à l'API consigne une réponse avec le nom d'utilisateur, l'IP et le type de requête à l'API.	Aide les administrateurs Grid à établir un enregistrement des modifications de configuration système effectuées par l'utilisateur à partir de quelle adresse IP source et de quelle adresse IP de destination à quel moment.	—

Fonction	Fonction	Impact	Conformité réglementaire
Prise en charge de TLS 1.3 pour l'interface de gestion et l'accès aux API	TLS établit un protocole de poignée de main pour la communication entre un client admin et un nœud admin StorageGRID.	Permet à un client administratif et à StorageGRID de s'identifier et de s'authentifier mutuellement et de communiquer avec confidentialité et intégrité des données.	—
SNMPv3 pour surveillance StorageGRID	SNMPv3 fournit la sécurité en offrant à la fois une authentification forte et un cryptage des données pour la confidentialité. Avec v3, les unités de données de protocole sont chiffrées à l'aide de CBC-DES pour son protocole de chiffrement. L'authentification utilisateur de la personne qui a envoyé l'unité de données de protocole est fournie par le protocole d'authentification HMAC-SHA ou HMAC-MD5. SNMPv2 et v1 sont toujours pris en charge.	Permet aux administrateurs de la grille de surveiller le système StorageGRID en activant un agent SNMP sur le nœud d'administration.	—
Certificats client pour l'exportation des metrics Prometheus	Les administrateurs du grid peuvent télécharger ou générer des certificats clients qui peuvent être utilisés pour fournir un accès sécurisé et authentifié à la base de données StorageGRID Prometheus.	Les administrateurs du grid peuvent utiliser des certificats client pour surveiller StorageGRID en externe à l'aide d'applications telles que Grafana.	—

Fonctions de sécurité de la plate-forme

Découvrez les fonctionnalités de sécurité de la plate-forme dans StorageGRID.

Fonction	Fonction	Impact	Conformité réglementaire
Infrastructure de clé publique (PKI) interne, certificats de nœud et TLS	StorageGRID utilise une PKI interne et des certificats de nœud pour authentifier et crypter les communications internœuds. La communication internœud est sécurisée par TLS.	Permet de sécuriser le trafic système sur le LAN ou le WAN, en particulier dans un déploiement multisite.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)

Fonction	Fonction	Impact	Conformité réglementaire
Pare-feu de nœud	StorageGRID configure automatiquement les tables IP et les règles de pare-feu pour contrôler le trafic réseau entrant et sortant, ainsi que pour fermer les ports inutilisés.	Protection du système StorageGRID, des données et des métadonnées contre le trafic réseau non sollicité.	—
Durcicement du système d'exploitation	Le système d'exploitation de base des appliances physiques et des nœuds virtuels StorageGRID est renforcé ; les logiciels non liés sont supprimés.	Permet de minimiser les surfaces d'attaque potentielles.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)
Mises à jour périodiques de la plate-forme et des logiciels	StorageGRID fournit régulièrement des versions logicielles, notamment des systèmes d'exploitation, des binaires d'applications et des mises à jour logicielles.	Ils permettent de maintenir le système StorageGRID à jour avec les logiciels et les binaires d'applications les plus récents.	—
Connexion racine désactivée via SSH (Secure Shell)	La connexion root via SSH est désactivée sur tous les nœuds StorageGRID. L'accès SSH utilise l'authentification par certificat.	Aide les clients à se protéger contre les éventuels problèmes de piratage à distance des mots de passe de la connexion racine.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)
Synchronisation temporelle automatisée	StorageGRID synchronise automatiquement les horloges système de chaque nœud avec plusieurs serveurs NTP (External Time Network Time Protocol). Au moins quatre serveurs NTP de Stratum 3 ou version ultérieure sont requis.	Garantit la même référence de temps sur tous les nœuds.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)
Réseaux séparés pour le trafic client, administrateur et grid interne	Les nœuds logiciels et les appliances matérielles StorageGRID prennent en charge plusieurs interfaces réseau physiques et virtuelles, de sorte que les clients peuvent séparer le trafic client, d'administration et le trafic réseau interne sur différents réseaux.	Permettez aux administrateurs du grid de séparer le trafic réseau interne et externe et de fournir le trafic sur les réseaux avec différents SLA.	—
Plusieurs interfaces VLAN (Virtual LAN)	StorageGRID prend en charge la configuration des interfaces VLAN sur vos réseaux client et grid StorageGRID.	Permettez aux administrateurs de Grid de partitionner et d'isoler le trafic des applications pour plus de sécurité, de flexibilité et de performances.	

Fonction	Fonction	Impact	Conformité réglementaire
Réseau client non fiable	L'interface réseau client non fiable accepte les connexions entrantes uniquement sur les ports qui ont été explicitement configurés comme des noeuds finaux d'équilibrage de charge.	Garantit que les interfaces exposées à des réseaux non fiables sont sécurisées.	—
Pare-feu configurable	Gérez les ports ouverts et fermés pour les réseaux Admin, Grid et client.	Autoriser les administrateurs du grid à contrôler l'accès aux ports et à gérer l'accès aux périphériques approuvés aux ports.	
Comportement SSH amélioré	désactiver SSH par défaut avant l'installation. Dans l'état par défaut, l'accès SSH n'est activé que sur l'adresse des ports de gestion locaux. Les mots de passe des utilisateurs administrateur et root sont définis sur le numéro de série du contrôleur de calcul de l'appliance. La connexion n'est autorisée que sur la console série et la console graphique (BMC KVM). SSH sur n'importe quel port réseau est désactivé.	Améliore la protection de l'accès au réseau.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)
Chiffrement de nœud	Dans le cadre de la nouvelle fonction de chiffrement du serveur hôte KMS, un nouveau paramètre de chiffrement de nœud est ajouté au programme d'installation de l'appliance StorageGRID.	Ce paramètre doit être activé pendant la phase de configuration matérielle de l'installation de l'appliance.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)

Intégration au cloud

Découvrez comment StorageGRID s'intègre aux services cloud.

Fonction	Fonction	Impact
Analyse antivirus basée sur les notifications	Notifications d'événements de support des services de plateforme StorageGRID. Les notifications d'événements peuvent être utilisées avec des services de cloud computing externes pour déclencher des flux de travail d'analyse antivirus sur les données.	Permet aux administrateurs de locataires de déclencher l'analyse antivirus des données à l'aide de services de cloud computing externes.

Tr-4921 : défense contre les ransomware

Protégez les objets StorageGRID S3 contre les attaques par ransomware

Découvrez les attaques par ransomware et comment protéger vos données grâce aux bonnes pratiques de sécurité de StorageGRID.

Le nombre d'attaques par ransomware est en hausse Ce document fournit quelques recommandations sur la protection des données d'objet sur StorageGRID.

Les ransomware représentent aujourd'hui le danger omniprésent dans les data centers. Les ransomwares ont été conçus pour chiffrer les données et les rendre inutilisables par des utilisateurs et des applications qui en dépendent. La protection commence par les défenses habituelles : une mise en réseau renforcée et de solides pratiques de sécurité des utilisateurs. Nous devons ensuite appliquer les pratiques de sécurité de l'accès aux données.

Les ransomwares sont l'une des plus grandes menaces de sécurité. L'équipe NetApp StorageGRID travaille avec nos clients pour garder une longueur d'avance sur ces menaces. Le verrouillage d'objets et la gestion des versions vous permettent de vous protéger contre les modifications indésirables et de restaurer votre système suite à des attaques malveillantes. La sécurité des données est une entreprise multiniveaux, dans laquelle le stockage objet n'est qu'une partie de votre data Center.

Meilleures pratiques StorageGRID

Pour StorageGRID, les bonnes pratiques en matière de sécurité doivent inclure l'utilisation du protocole HTTPS avec des certificats signés pour la gestion et l'accès aux objets. Créez des comptes utilisateur dédiés aux applications et aux particuliers et n'utilisez pas les comptes root des locataires pour l'accès aux applications ou aux données utilisateur. En d'autres termes, suivez le principe du privilège minimum. Utilisez des groupes de sécurité avec des règles de gestion des identités et des accès (IAM) définies pour régir les droits d'utilisateur et les comptes d'accès spécifiques aux applications et aux utilisateurs. Une fois ces mesures mises en place, vous devez vous assurer que vos données sont protégées. Dans le cas de simple Storage Service (S3), lorsque les objets sont modifiés pour les chiffrer, il est remplacé par l'objet d'origine.

Méthodes de défense

Le mécanisme principal de protection contre les ransomwares dans l'API S3 consiste à mettre en œuvre le verrouillage objet. Toutes les applications ne sont pas compatibles avec le verrouillage d'objet. Il existe donc deux autres options pour protéger vos objets décrites dans ce rapport : la réplication vers un autre compartiment avec la gestion des versions activée et la gestion des versions avec les règles IAM.

Où trouver des informations complémentaires

Pour en savoir plus sur les informations données dans ce livre blanc, consultez ces documents et/ou sites web :

- Centre de documentation NetApp StorageGRIDhttps://docs.netapp.com/us-en/storagegrid/[]
- Accompagnement NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-enable/
- Documentation des produits NetApp https://www.netapp.com/support-and-training/documentation/

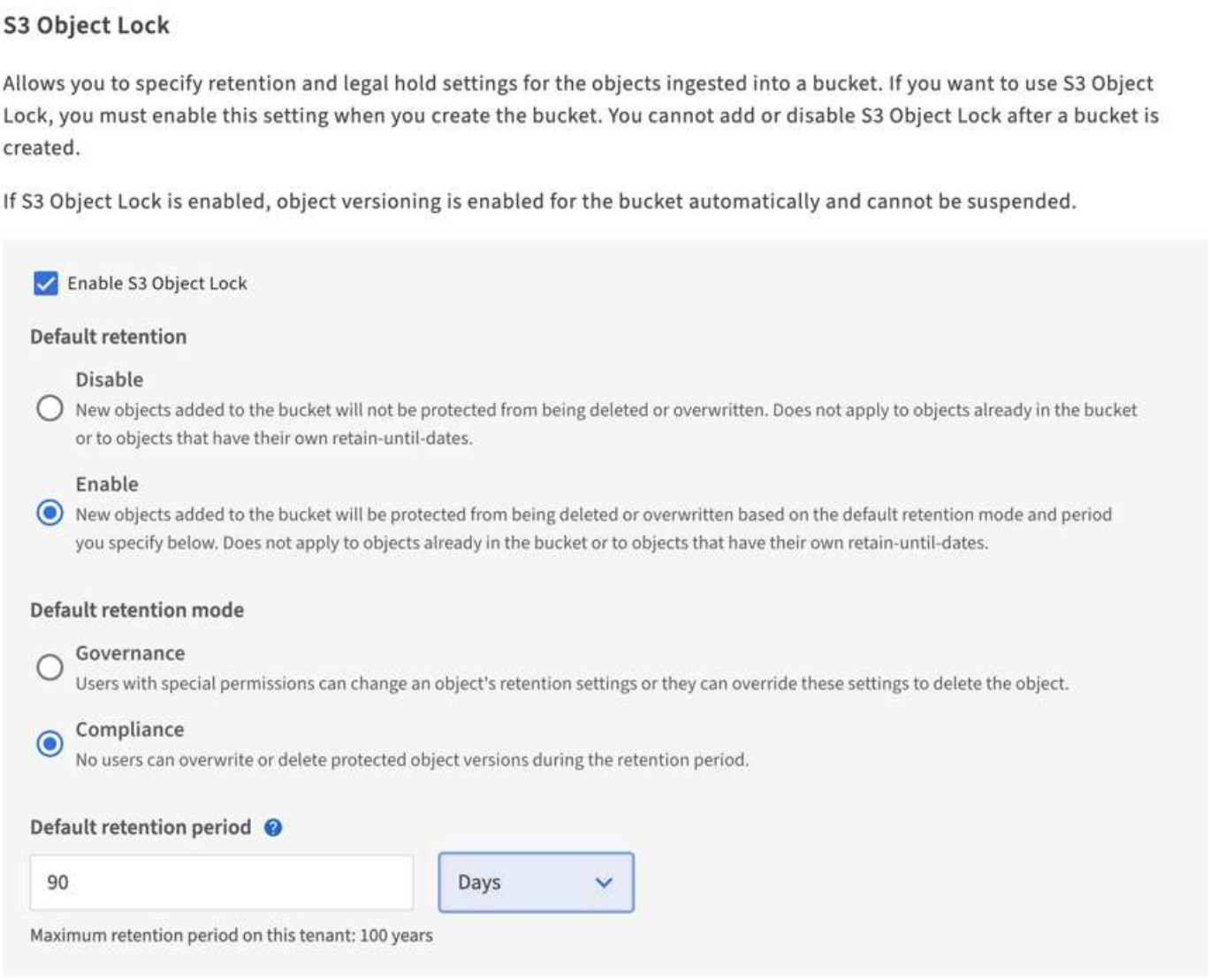
Protégez vos données contre les ransomwares à l'aide d'un verrouillage objet

Découvrez comment le verrouillage d'objets dans StorageGRID fournit un modèle

WORM pour empêcher la suppression ou le remplacement des données, et comment il répond aux exigences réglementaires.

Le verrouillage des objets fournit un modèle WORM qui empêche la suppression ou l'écrasement d'objets. L'implémentation du verrouillage objet par StorageGRID "Cohasset évalué" permet de respecter les exigences réglementaires et prend en charge la conservation à des fins juridiques, le mode de conformité et le mode de gouvernance pour la conservation des objets ainsi que les règles de conservation des compartiments par défaut. Vous devez activer le verrouillage d'objet dans le cadre de la création de compartiment et de la gestion des versions. Une version spécifique d'un objet est verrouillée, et si aucun ID de version n'est défini, la rétention est placée sur la version actuelle de l'objet. Si la conservation de la version actuelle est configurée et qu'une tentative de suppression, de modification ou d'écrasement de l'objet est effectuée, une nouvelle version est créée avec un marqueur de suppression ou la nouvelle révision de l'objet comme version actuelle, et la version verrouillée est conservée comme une version non actuelle. Pour les applications qui ne sont pas encore compatibles, vous pouvez toujours utiliser le verrouillage objet et une configuration de conservation par défaut placée sur le compartiment. Une fois la configuration définie, une conservation d'objet est appliquée à chaque nouvel objet placé dans le compartiment. Cela fonctionne tant que l'application est configurée pour ne pas supprimer ou écraser les objets avant que la durée de conservation ne soit écoulée.

Lors de la création d'un bucket dans l'interface utilisateur de gestion des locataires, vous pouvez activer le verrouillage des objets et configurer un mode de conservation par défaut et une période de conservation. Une fois configuré, cela définira une rétention de verrouillage d'objet minimale sur chaque objet ingéré dans ce bucket.



Voici quelques exemples d'utilisation de l'API de verrouillage d'objet :

La mise en attente légale du verrouillage d'objet est un état activé/désactivé simple appliqué à un objet.

```
aws s3api put-object-legal-hold --bucket mybucket --key myfile.txt --legal
-hold Status=ON --endpoint-url https://s3.company.com
```

La définition de l'état de mise en attente légale ne renvoie aucune valeur si elle a réussi, de sorte qu'elle peut être vérifiée à l'aide d'une opération GET.

```
aws s3api get-object-legal-hold --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
    "LegalHold": {
        "Status": "ON"
    }
}
```

Pour désactiver la mise en attente légale, appliquez le statut OFF.

```
aws s3api put-object-legal-hold --bucket mybucket --key myfile.txt --legal
-hold Status=OFF --endpoint-url https://s3.company.com
aws s3api get-object-legal-hold --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
    "LegalHold": {
        "Status": "OFF"
    }
}
```

La définition de la conservation d'objet s'effectue à l'aide d'un horodatage de conservation jusqu'à.

```
aws s3api put-object-retention --bucket mybucket --key myfile.txt
--retention '{"Mode":"COMPLIANCE", "RetainUntilDate": "2022-06-
10T16:00:00"}'  --endpoint-url https://s3.company.com
```

Encore une fois, il n'y a pas de valeur renvoyée en cas de réussite, vous pouvez donc vérifier l'état de conservation de la même manière avec un appel GET.

```
aws s3api get-object-retention --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
    "Retention": {
        "Mode": "COMPLIANCE",
        "RetainUntilDate": "2022-06-10T16:00:00+00:00"
    }
```

Le fait de conserver une conservation par défaut dans un compartiment activé pour le verrouillage d'objet applique une période de conservation en jours et en années.

```
aws s3api put-object-lock-configuration --bucket mybucket --object-lock
-configuration '{ "ObjectLockEnabled": "Enabled", "Rule": {
"DefaultRetention": { "Mode": "COMPLIANCE", "Days": 1 }}}' --endpoint-url
https://s3.company.com
```

Comme pour la plupart de ces opérations, aucune réponse n'est renvoyée en cas de succès. Par conséquent, nous pouvons effectuer une OPÉRATION GET pour que la configuration puisse être vérifiée.

```
aws s3api get-object-lock-configuration --bucket mybucket --endpoint-url
https://s3.company.com
{
```

```
    "ObjectLockConfiguration": {
        "ObjectLockEnabled": "Enabled",
        "Rule": {
            "DefaultRetention": {
                "Mode": "COMPLIANCE",
                "Days": 1
            }
        }
    }
}
```

Vous pouvez ensuite placer un objet dans le compartiment avec la configuration de conservation appliquée.

```
aws s3 cp myfile.txt s3://mybucket --endpoint-url https://s3.company.com
```

L'opération PUT renvoie une réponse.

```
upload: ./myfile.txt to s3://mybucket/myfile.txt
```

Sur l'objet de conservation, la durée de conservation définie dans le compartiment de l'exemple précédent est convertie en horodatage de conservation de l'objet.

```
aws s3api get-object-retention --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
    "Retention": {
        "Mode": "COMPLIANCE",
        "RetainUntilDate": "2022-03-02T15:22:47.202000+00:00"
    }
}
```

Protection contre les ransomwares à l'aide d'un compartiment répliqué avec gestion des versions

Découvrez comment répliquer des objets vers un compartiment secondaire à l'aide de StorageGRID CloudMirror.

Les applications et les charges de travail ne seront pas toutes compatibles avec le verrouillage en mode objet. Une autre option consiste à répliquer les objets vers un compartiment secondaire dans la même grille (de préférence un locataire différent avec accès limité) ou tout autre terminal S3 avec le service de plateforme StorageGRID, CloudMirror.

StorageGRID CloudMirror est un composant de StorageGRID qui peut être configuré pour répliquer les objets d'un compartiment vers une destination définie lors de leur ingestion dans le compartiment source et ne réplique pas les suppressions. Comme CloudMirror est un composant intégré de StorageGRID, il ne peut pas

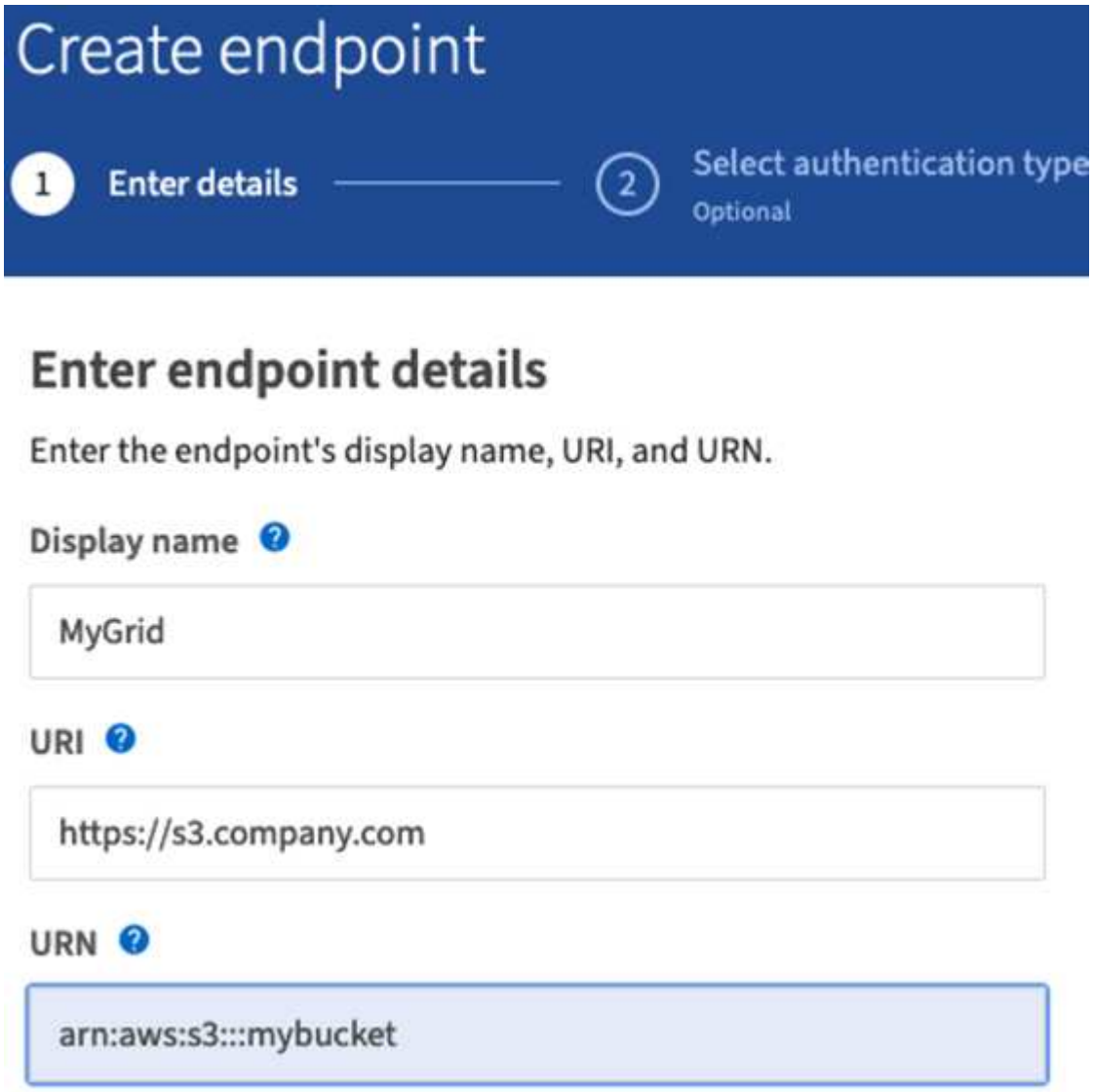
être désactivé ou manipulé par une attaque basée sur l'API S3. Vous pouvez configurer ce compartiment répliqué avec la gestion des versions activée. Dans ce scénario, vous avez besoin d'un nettoyage automatisé des anciennes versions du compartiment répliqué qui peuvent être jetées en toute sécurité. Pour cela, vous pouvez utiliser le moteur de règles ILM de StorageGRID. Créez des règles pour gérer le placement des objets en fonction d'une période non actuelle pendant plusieurs jours, suffisamment pour avoir identifié et récupéré une attaque.

L'un des inconvénients de cette approche est qu'elle consomme plus de stockage en conservant une seconde copie complète du compartiment et plusieurs versions des objets pendant un certain temps. En outre, les objets qui ont été supprimés intentionnellement du compartiment principal doivent être supprimés manuellement du compartiment répliqué. Il existe d'autres options de réplication en dehors du produit, telles que NetApp CloudSync, qui peuvent répliquer les suppressions pour une solution similaire. Un autre inconvénient est que la gestion des versions du compartiment secondaire est activée et que le verrouillage d'objet n'est pas activé, c'est qu'il existe un certain nombre de comptes privilégiés qui peuvent être utilisés pour causer des dommages à l'emplacement secondaire. L'avantage est qu'il doit s'agir d'un compte unique pour ce terminal ou ce compartiment locataire, et le compromis n'inclut probablement pas l'accès aux comptes sur l'emplacement principal, et inversement.

Une fois les compartiments source et destination créés et la destination configurée avec la gestion des versions, vous pouvez configurer et activer la réplication comme suit :

Étapes

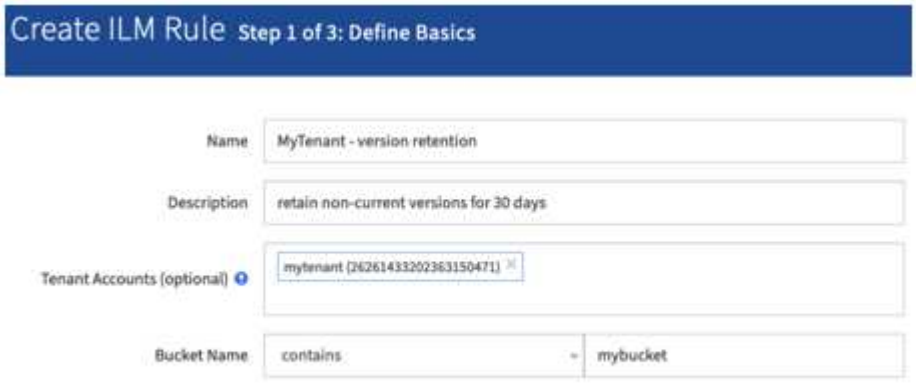
1. Pour configurer CloudMirror, créez un terminal de services de plateforme pour la destination S3.

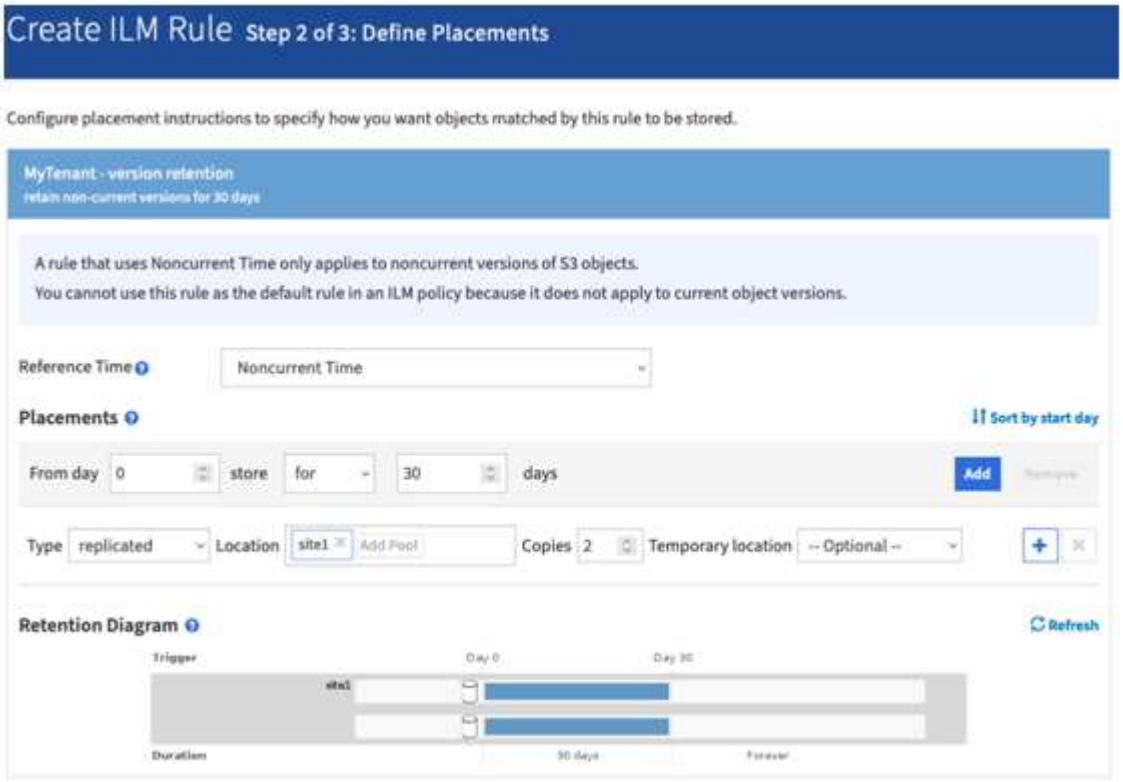


2. Sur le compartiment source, configurez la réplication pour utiliser le terminal configuré.

```
<ReplicationConfiguration>
    <Role></Role>
    <Rule>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
            <Bucket>arn:aws:s3:::mybucket</Bucket>
            <StorageClass>STANDARD</StorageClass>
        </Destination>
    </Rule>
</ReplicationConfiguration>
```

3. Créez des règles ILM pour gérer le placement du stockage et la gestion de la durée du stockage des versions. Dans cet exemple, les versions non actuelles des objets à stocker sont configurées.





Il y a deux copies sur le site 1 pendant 30 jours. Vous configurez également les règles de la version actuelle des objets en fonction de l'utilisation de l'heure d'ingestion comme heure de référence dans la règle ILM pour correspondre à la durée de stockage du compartiment source. Le placement de stockage des versions d'objets peut être codé par effacement ou répliqué.

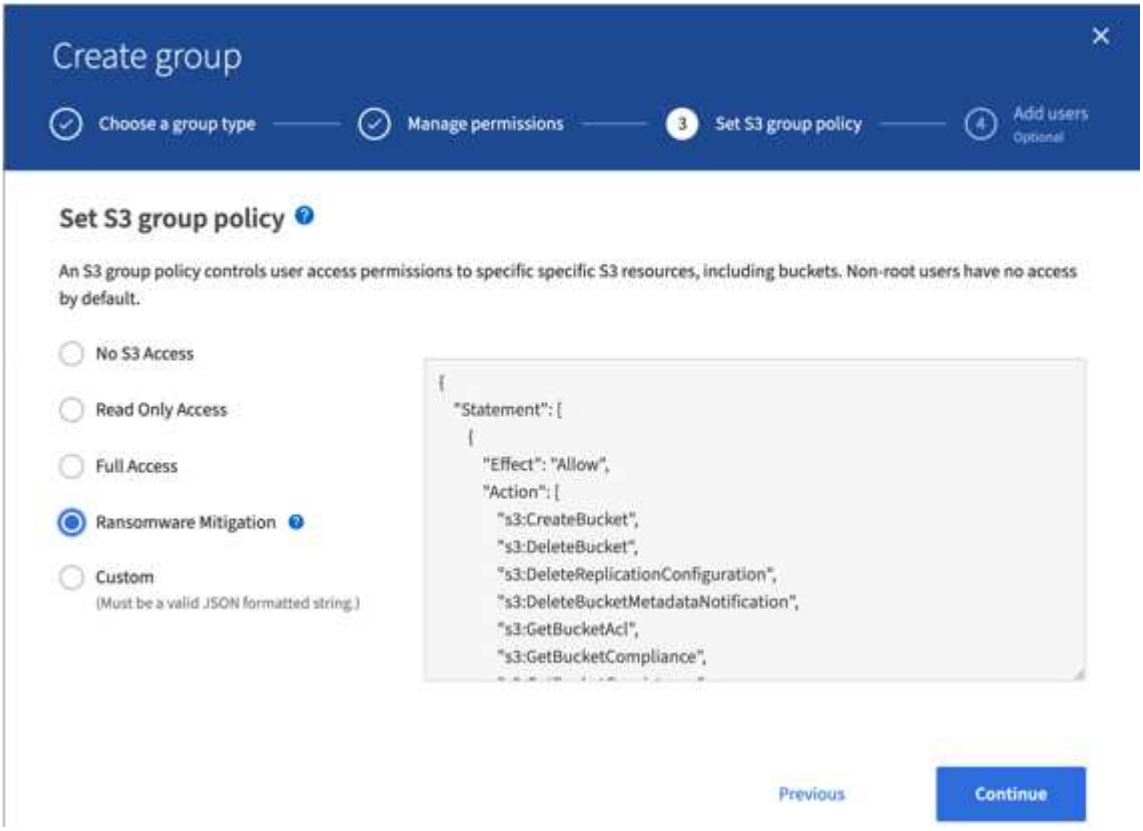
Défense anti-ransomware à l'aide du contrôle des versions avec une politique IAM de protection

Découvrez comment protéger vos données en activant la gestion des versions dans le compartiment et en implémentant les règles IAM sur les groupes de sécurité des utilisateurs dans StorageGRID.

Une méthode pour protéger vos données sans verrouillage objet ou réplication consiste à activer la gestion des versions sur le compartiment et à mettre en œuvre des règles IAM sur les groupes de sécurité utilisateur afin de limiter la capacité des utilisateurs à gérer des versions des objets. En cas d'attaque, de nouvelles

versions incorrectes des données sont créées en tant que version actuelle, et la version la plus récente non-actuelle est la sécurité des données. Les comptes compromis pour accéder aux données n'ont pas accès à supprimer ni à modifier la version non actuelle qui les protège pour des opérations de restauration ultérieures. Comme dans le scénario précédent, les règles ILM gèrent la conservation des versions non actuelles avec la durée de votre choix. L'inconvénient est qu'il existe toujours la possibilité de comptes privilégiés pour une attaque de mauvais acteurs, mais tous les comptes de service d'application et les utilisateurs doivent être configurés avec un accès plus restrictif. La stratégie de groupe restrictif doit explicitement autoriser chaque action que vous souhaitez que les utilisateurs ou l'application soient capables et refuser explicitement toute action dont vous ne voulez pas qu'ils soient capables. NetApp ne recommande pas l'utilisation d'une autorisation générique car une nouvelle action pourrait être introduite à l'avenir et vous voudrez contrôler si elle est autorisée ou refusée. Pour cette solution, la liste de refus doit inclure DeleteObjectVersion, PutBucketPolicy, DeleteBuckePolicy, PutLifecycleConfiguration et PutBucketVersioning afin de protéger la configuration de gestion des versions du compartiment et de l'objet des modifications utilisateur ou programmatiques.

Dans StorageGRID, l'option de stratégie de groupe S3 « Atténuation des ransomwares » facilite la mise en œuvre de cette solution. Lors de la création d'un groupe d'utilisateurs dans le locataire, après avoir sélectionné les autorisations du groupe, vous pouvez voir cette politique facultative.



Voici le contenu de la stratégie de groupe qui inclut la plupart des opérations disponibles explicitement autorisées et le minimum requis refusé.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
```

```
                "s3:DeleteBucket",
                "s3:DeleteReplicationConfiguration",
"s3:DeleteBucketMetadataNotification",
                "s3:GetBucketAcl",
                "s3:GetBucketCompliance",
                "s3:GetBucketConsistency",
                "s3:GetBucketLastAccessTime",
                "s3:GetBucketLocation",
                "s3:GetBucketNotification"
"s3:GetBucketObjectLockConfiguration",
                "s3:GetBucketPolicy",
                "s3:GetBucketMetadataNotification",
                "s3:GetReplicationConfiguration",
                "s3:GetBucketCORS",
                "s3:GetBucketVersioning",
                "s3:GetBucketTagging",
                "s3:GetEncryptionConfiguration",
                "s3:GetLifecycleConfiguration",
                "s3:ListBucket",
                "s3:ListBucketVersions",
                "s3:ListAllMyBuckets",
                "s3:ListBucketMultipartUploads",
                "s3:PutBucketConsistency",
                "s3:PutBucketLastAccessTime",
                "s3:PutBucketNotification",
"s3:PutBucketObjectLockConfiguration",
                "s3:PutReplicationConfiguration",
                "s3:PutBucketCORS",
                "s3:PutBucketMetadataNotification",
                "s3:PutBucketTagging",
                "s3:PutEncryptionConfiguration",
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:DeleteObjectTagging",
                "s3:DeleteObjectVersionTagging",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectLegalHold",
                "s3:GetObjectRetention",
                "s3:GetObjectTagging",
                "s3:GetObjectVersion",
                "s3:GetObjectVersionAcl",
                "s3:GetObjectVersionTagging",
                "s3:ListMultipartUploadParts",
                "s3:PutObject",
                "s3:PutObjectAcl",
```

```
                "s3:PutObjectLegalHold",
                "s3:PutObjectRetention",
                "s3:PutObjectTagging",
                "s3:PutObjectVersionTagging",
                "s3:RestoreObject",
                "s3:ValidateObject",
                "s3:PutBucketCompliance",
                "s3:PutObjectVersionAcl"
            ],
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "s3:DeleteObjectVersion",
                "s3:DeleteBucketPolicy",
                "s3:PutBucketPolicy",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketVersioning"
            ],
            "Resource": "arn:aws:s3:::*"
        }
    ]
}
```

Enquête et correction des ransomwares

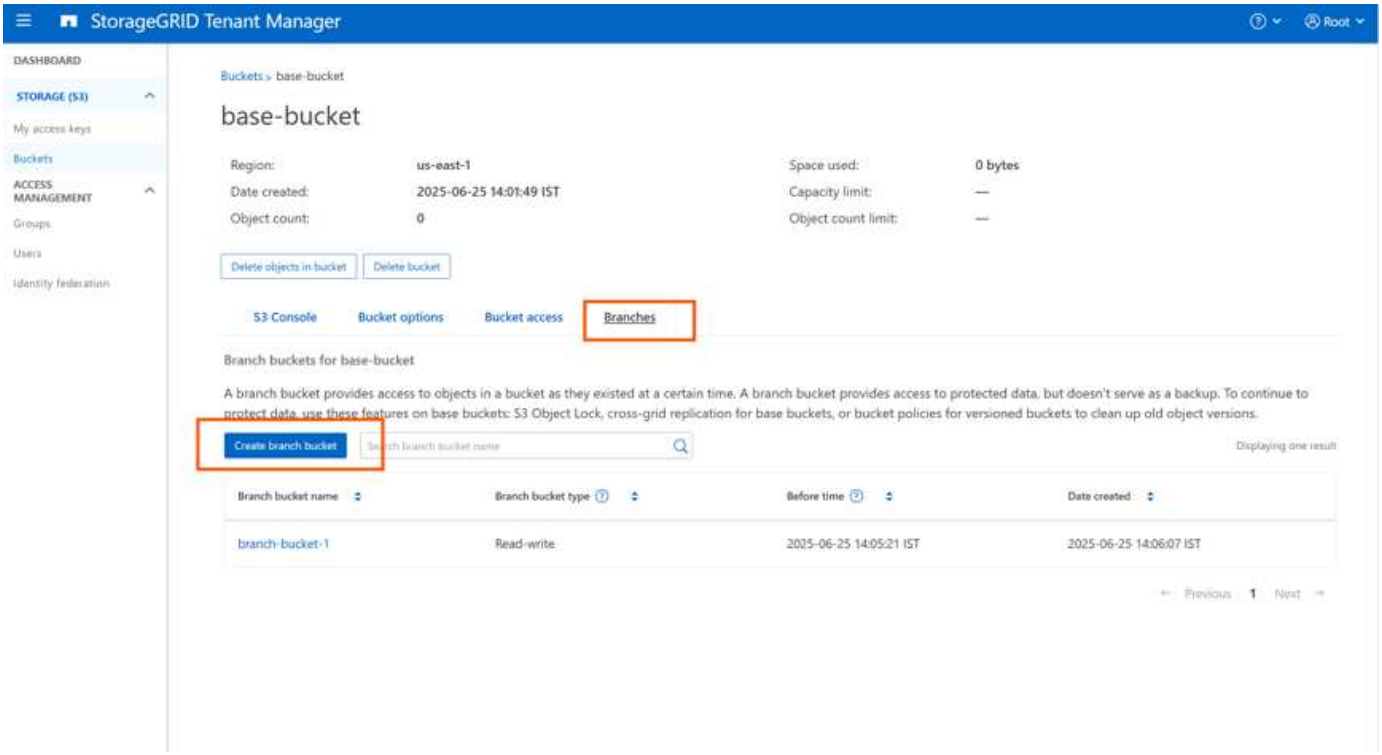
Découvrez comment enquêter et corriger les buckets après une éventuelle attaque de ransomware avec StorageGRID.

Dans StorageGRID 12.0, la nouvelle fonctionnalité de compartiment de branche a été ajoutée pour étendre l'utilité du contrôle de version pour la défense contre les ransomwares. Un bucket de branche fournit un accès aux objets d'un bucket tels qu'ils existaient à un certain moment, à condition qu'ils existent toujours dans le bucket. Les buckets de branches ne peuvent être créés que pour les buckets de base compatibles avec le contrôle de version.

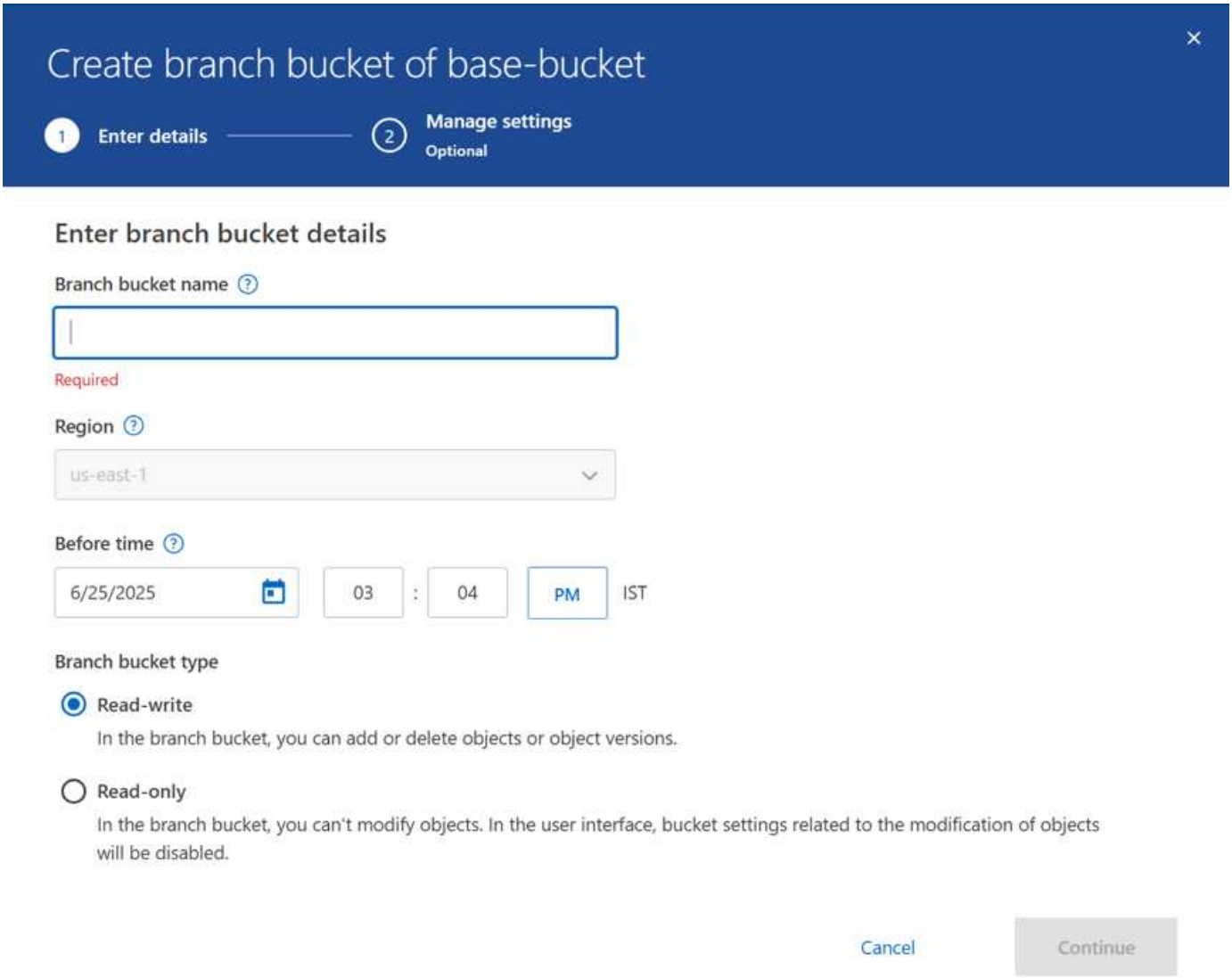
Cela signifie que si vous suspectez qu'une attaque de ransomware a eu lieu, vous pouvez créer un bucket de branche en lecture/écriture ou en lecture seule contenant tous les objets et versions qui existaient avant l'heure de l'attaque initiale. Vous pouvez utiliser ce bucket de branche pour comparer le contenu du bucket de base afin de déterminer quels objets ont changé et si le changement faisait partie de l'attaque ou non. Vous pouvez également utiliser un bucket de branche pour poursuivre les opérations client à l'aide de la branche propre tout en enquêtant sur l'attaque.

Création d'un bucket de branches

- Accédez à la page des détails du bucket de base et à l'onglet Branches pour créer un bucket de branche.



- Une fois le bouton Créer un bucket de branche cliqué, une fenêtre contextuelle s'ouvre avec les détails préremplis de la région associée au bucket de base.
- indiquez le nom du bucket de branche, avant l'heure, et sélectionnez le type de bucket de branche à créer.



Tr-4765 : StorageGRID du moniteur

Introduction à la surveillance StorageGRID

Découvrez comment contrôler votre système StorageGRID à l'aide d'applications externes telles que Splunk.

La surveillance efficace du stockage objet NetApp StorageGRID permet aux administrateurs de répondre rapidement aux problèmes urgents et d'ajouter de manière proactive des ressources pour gérer la croissance des workloads. Ce rapport fournit des conseils généraux sur la façon de surveiller les mesures clés et d'exploiter les applications de surveillance externes. Il est destiné à compléter le guide de surveillance et de dépannage existant.

Un déploiement NetApp StorageGRID se compose généralement de plusieurs sites et de nombreux nœuds qui créent un système de stockage objet distribué et tolérant aux pannes. Dans un système de stockage distribué et résilient tel que StorageGRID, il est normal que des conditions d'erreur existent alors que la grille continue de fonctionner normalement. En tant qu'administrateur, le défi consiste à comprendre le seuil auquel les conditions d'erreur (telles que les nœuds en panne) constituent un problème qui doit être immédiatement résolu par rapport aux informations à analyser. En analysant les données d'StorageGRID, vous pouvez

analyser votre charge de travail et prendre des décisions avisées, notamment concernant l'ajout de ressources.

StorageGRID fournit une excellente documentation qui analyse le sujet de la surveillance. Ce rapport part du principe que vous connaissez StorageGRID et que vous avez consulté la documentation correspondante. Au lieu de répéter ces informations, nous nous référons à la documentation produit tout au long de ce guide. La documentation des produits StorageGRID est disponible en ligne et au format PDF.

L'objectif de ce document est de compléter la documentation produit et de découvrir comment contrôler votre système StorageGRID à l'aide d'applications externes, telles que Splunk.

Sources de données

Pour réussir la surveillance de NetApp StorageGRID, il est important de savoir où collecter des données sur l'état et les opérations de votre système StorageGRID.

- **Interface utilisateur Web et tableau de bord.** Le gestionnaire de grille StorageGRID présente une vue de haut niveau des informations que vous, en tant qu'administrateur, devez voir dans une présentation logique. En tant qu'administrateur, vous pouvez également approfondir les informations de niveau de service pour le dépannage et la collecte des journaux.
- **Journaux d'audit.** StorageGRID conserve des journaux d'audit granulaires des actions des locataires telles que LA COMMANDE PUT, GET et DELETE. Vous pouvez également suivre le cycle de vie d'un objet de l'ingestion à l'application des règles de gestion des données.
- **API métriques.** Les API de l'interface utilisateur sont sous-jacentes à l'interface GMI de StorageGRID. Cette approche vous permet d'extraire des données à l'aide d'outils externes de surveillance et d'analyse.

Où trouver des informations complémentaires

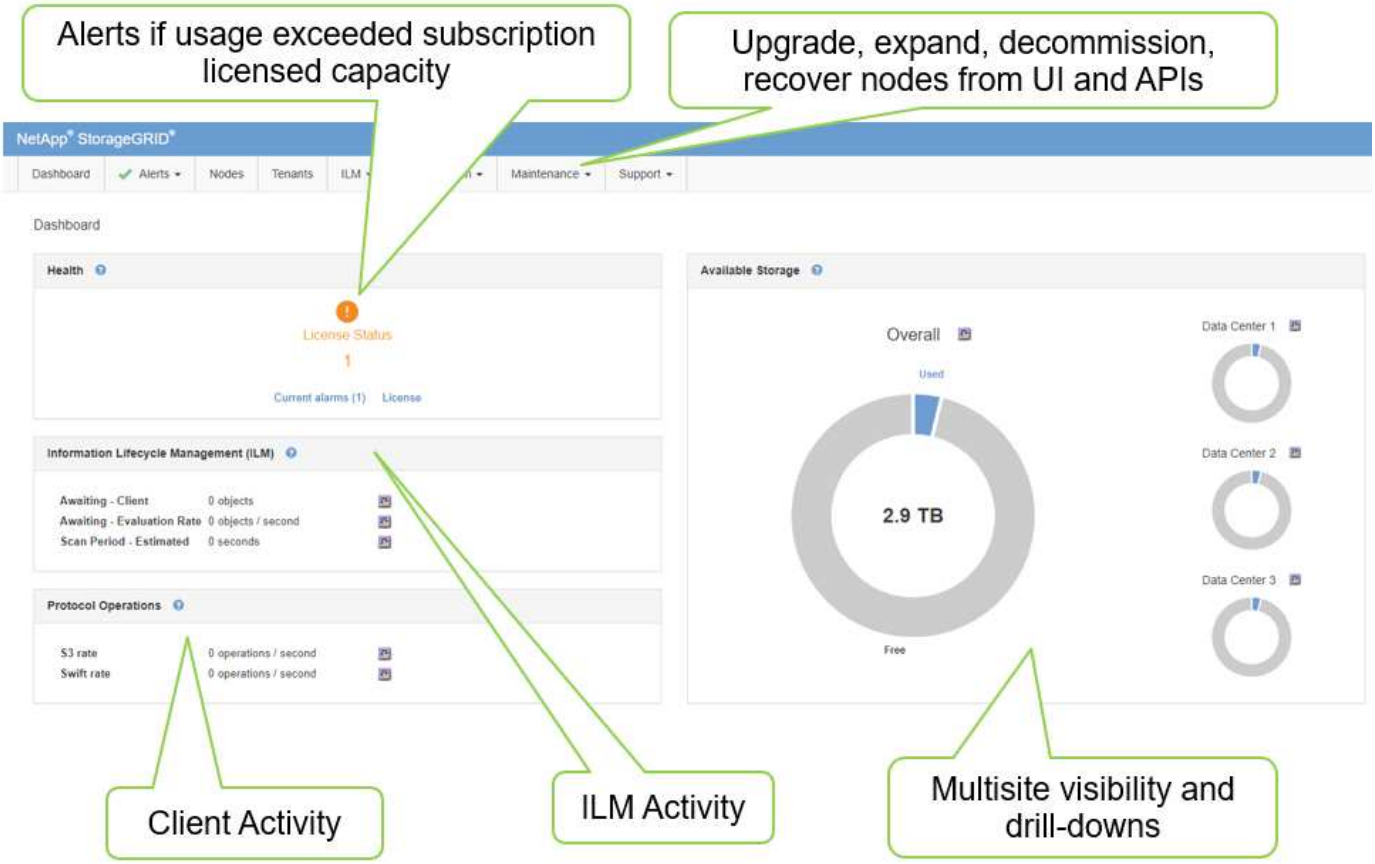
Pour en savoir plus sur les informations données dans ce livre blanc, consultez ces documents et/ou sites web :

- Centre de documentation NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-118/
- Accompagnement NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-enable/
- Documentation des produits NetApp https://www.netapp.com/support-and-training/documentation/
- NetApp StorageGRID application pour Splunk https://splunkbase.splunk.com/app/3898/#/details

Utilisez le tableau de bord GMI pour surveiller StorageGRID

Le tableau de bord de l'interface de gestion Grid (GMI) de StorageGRID offre une vue centralisée de l'infrastructure StorageGRID. Vous pouvez ainsi surveiller l'état, les performances et la capacité de l'ensemble du grid.

Utilisez le tableau de bord GMI pour examiner chaque composant central de la grille.



Informations à surveiller régulièrement

Une version précédente de ce rapport technique énuméré les mesures à vérifier périodiquement par rapport aux tendances. Cette information est maintenant incluse dans le "Guide de surveillance et de dépannage".

Surveiller le stockage

Dans une version précédente de ce rapport technique, nous liseous où surveiller les mesures importantes, telles que l'espace de stockage objet, l'espace de métadonnées, les ressources réseau, etc. Cette information est maintenant incluse dans le "Guide de surveillance et de dépannage".

Utilisez les alertes pour surveiller StorageGRID

Découvrez comment utiliser le système d'alertes de StorageGRID pour surveiller les problèmes, gérer les alertes personnalisées et étendre les notifications d'alertes via SNMP ou par e-mail.

Les alertes fournissent des informations critiques qui vous permettent de surveiller les divers événements et conditions de votre système StorageGRID.

Le système d'alertes est conçu pour être le principal outil de surveillance des problèmes susceptibles de survenir dans votre système StorageGRID. Le système d'alertes se concentre sur les problèmes exploitables du système et propose une interface simple d'utilisation.

Nous fournissons un ensemble de règles d'alerte par défaut qui visent à faciliter la surveillance et le dépannage de votre système. Vous pouvez davantage gérer les alertes en créant des alertes personnalisées, en modifiant ou en désactivant les alertes par défaut et en désactivant les notifications d'alerte.

Les alertes sont également extensibles via SNMP ou la notification par e-mail.

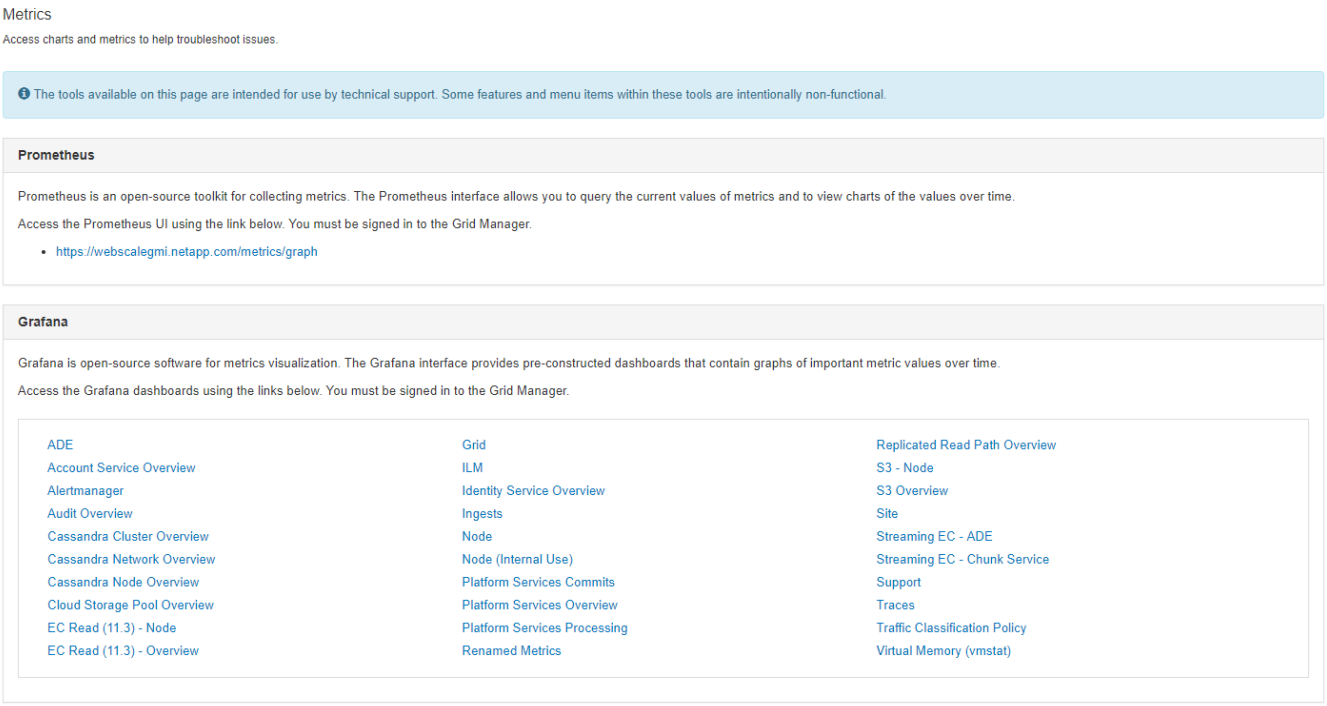
Pour plus d'informations sur les alertes, reportez-vous à la "documentation produit" page disponible en ligne et au format PDF.

Surveillance avancée dans StorageGRID

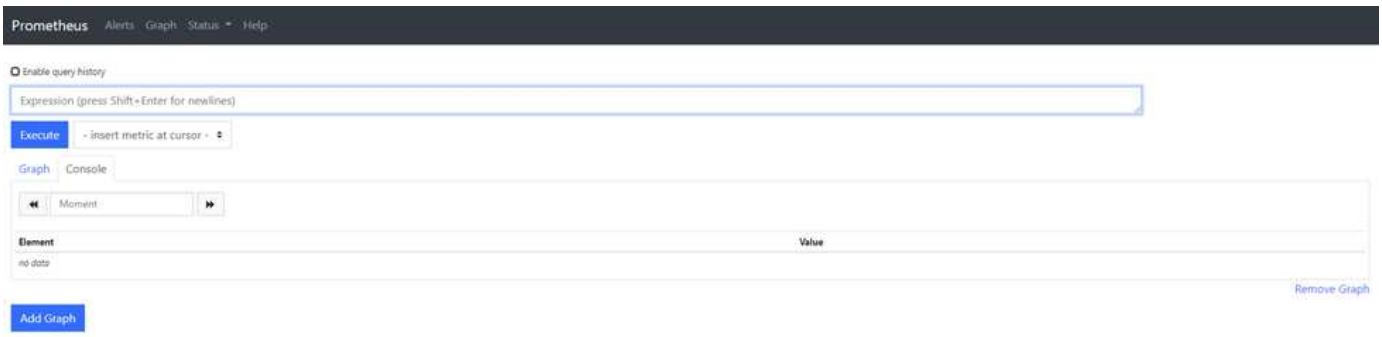
Découvrez comment accéder à des metrics et les exporter pour résoudre vos problèmes.

Affichage des API de metrics via une requête Prometheus

Prometheus est un logiciel open source qui collecte des metrics. Pour accéder au Prometheus intégré de StorageGRID via l'interface GMI, accédez au **support › Metrics**.



Vous pouvez également accéder directement au lien.



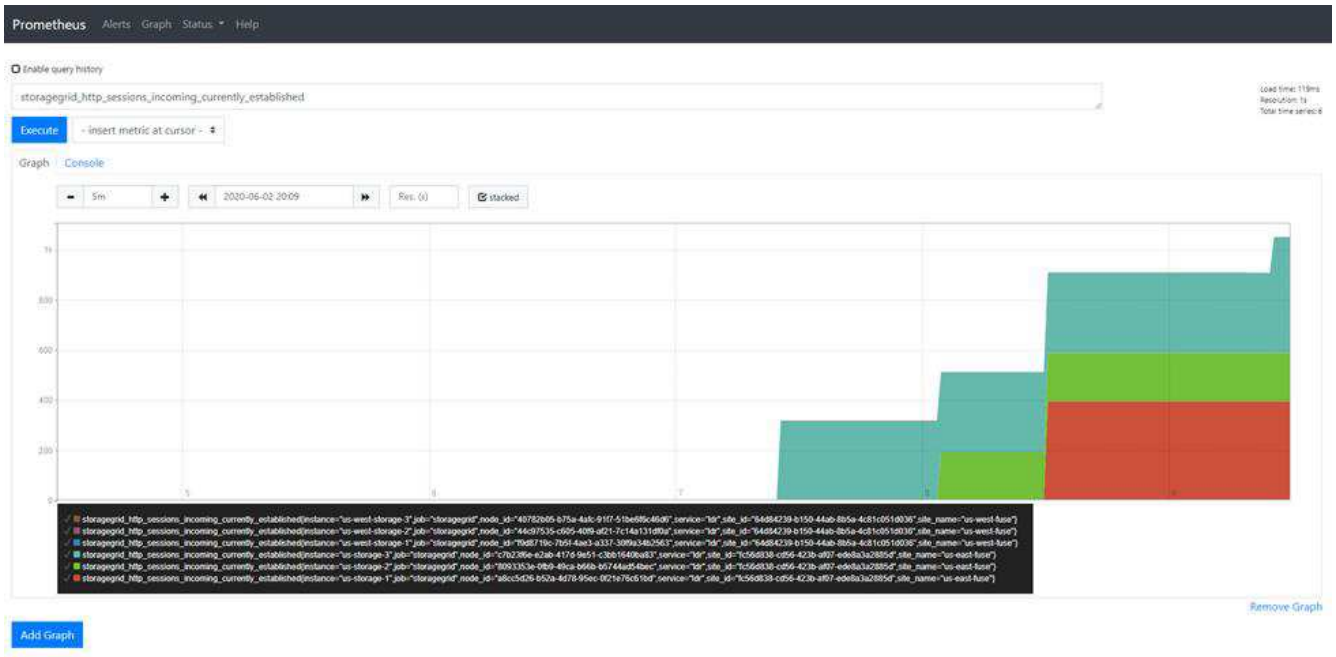
Avec cette vue, vous pouvez accéder à l'interface Prometheus. Ensuite, vous pouvez effectuer des recherches

parmi les mesures disponibles et même tester des requêtes.

Pour effectuer une requête URL Prometheus, procédez comme suit :

Étapes

1. Commencez à taper dans la zone de texte de la requête. Au fur et à mesure que vous tapez, les indicateurs sont répertoriés. À nos fins, seuls les metrics commençant par StorageGRID et Node sont importants.
2. Pour afficher le nombre de sessions HTTP pour chaque nœud, tapez `storagegrid_http` et sélectionnez `storagegrid_http_sessions_incoming_currently_established`. Cliquez sur Exécuter et affichez les informations au format graphique ou console.



Les requêtes et les graphiques que vous créez via cette URL ne persistent pas. Les requêtes complexes consomment des ressources sur le nœud d'administration. NetApp vous recommande d'utiliser cette vue pour explorer les metrics disponibles.

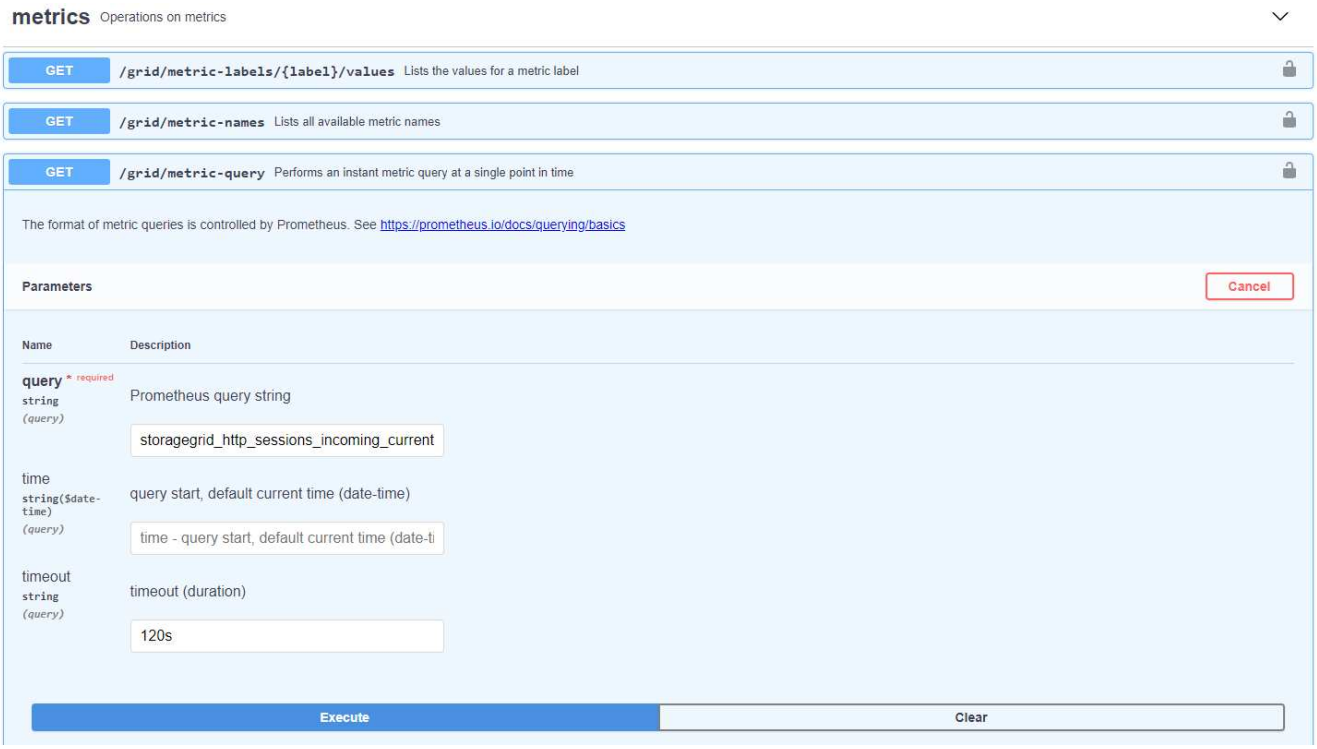
Il n'est pas recommandé de s'interfacer directement avec notre instance Prometheus, car cela nécessite l'ouverture de ports supplémentaires. L'accès aux metrics via notre API est la méthode recommandée et sécurisée.

Exportez les metrics via l'API

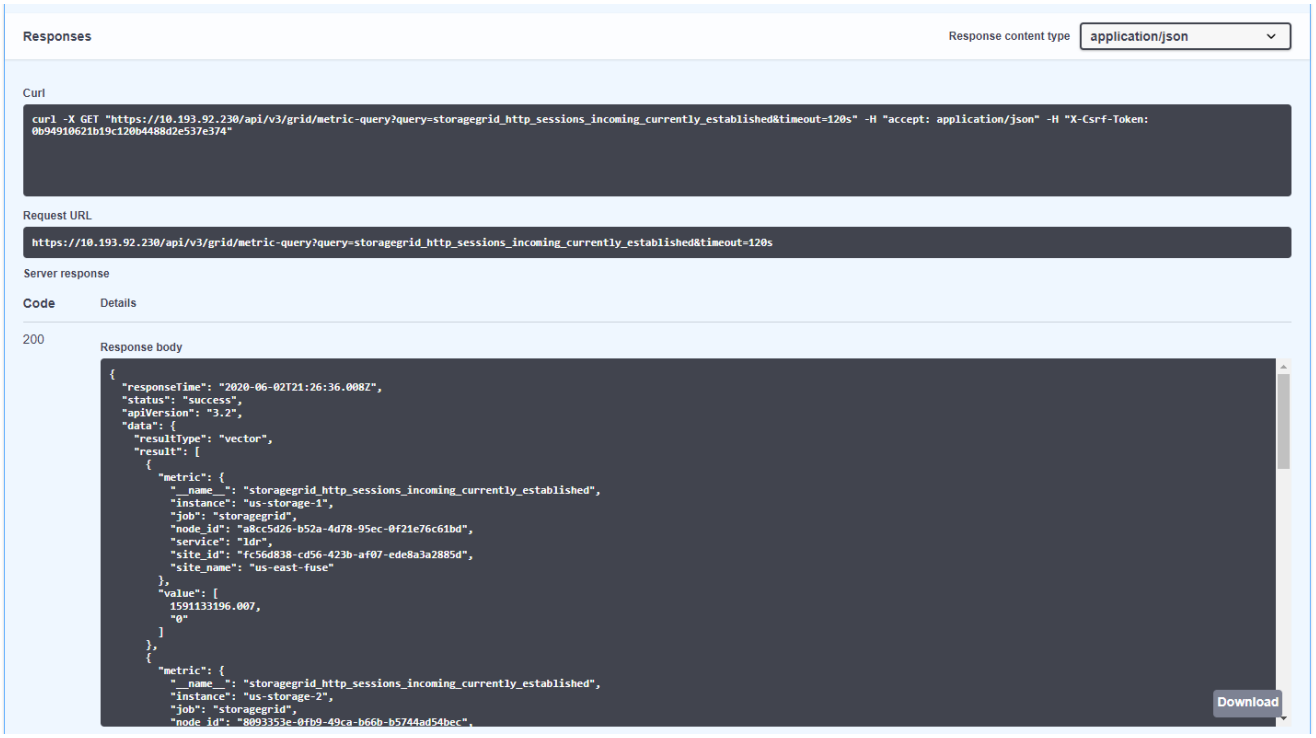
Vous pouvez également accéder aux mêmes données via l'API de gestion StorageGRID.

Pour exporter des metrics via l'API, effectuez la procédure suivante :

1. Dans l'interface GMI, sélectionnez **aide › Documentation API**.
2. Faites défiler jusqu'à Metrics et sélectionnez GET /grid/Metric-query.



La réponse inclut les mêmes informations que celles que vous pouvez obtenir via une requête URL Prometheus. Vous pouvez à nouveau voir le nombre de sessions HTTP actuellement établies sur chaque nœud de stockage. Vous pouvez également télécharger la réponse au format JSON pour plus de lisibilité. La figure suivante présente des exemples de réponses à des requêtes Prometheus.



L’avantage de l’utilisation de l’API est qu’elle vous permet d’effectuer des requêtes authentifiées

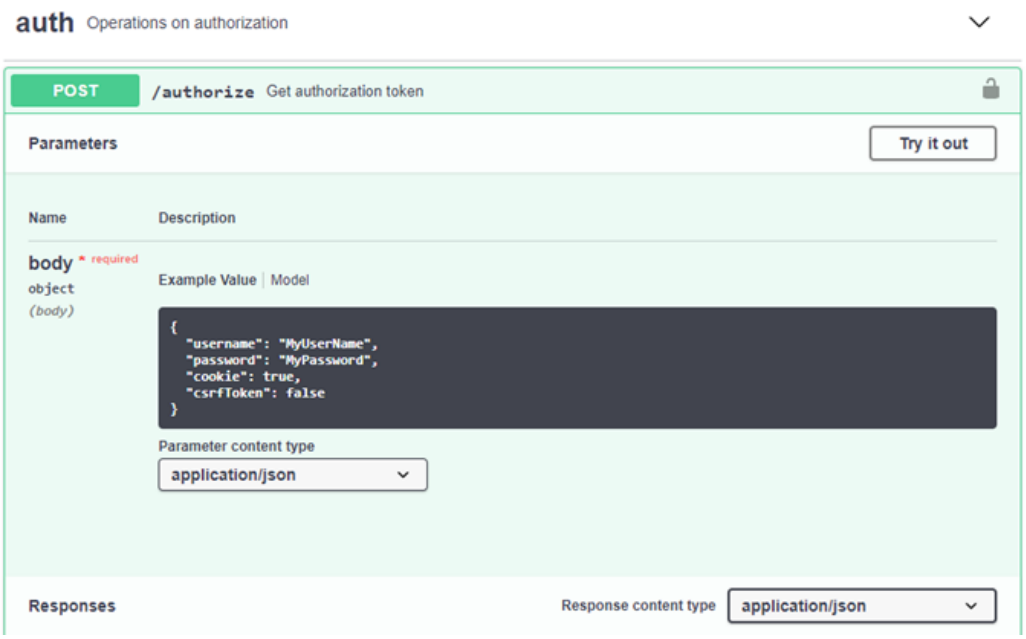
Accédez aux metrics à l'aide de CURL dans StorageGRID

Découvrez comment accéder aux metrics via l'interface de ligne de commandes en utilisant curl.

Pour effectuer cette opération, vous devez d'abord obtenir un jeton d'autorisation. Pour demander un jeton, procédez comme suit :

Étapes

1. Dans l'interface GMI, sélectionnez **aide › Documentation API**.
2. Faites défiler jusqu'à Auth pour rechercher des opérations sur l'autorisation. La capture d'écran suivante montre les paramètres de la méthode POST.



3. Cliquez sur essayer et modifiez le corps avec votre nom d'utilisateur et votre mot de passe GMI.
4. Cliquez sur Exécuter.
5. Copiez la commande curl fournie dans la section curl et collez-la dans une fenêtre de terminal. La commande se présente comme suit :

```
curl -X POST "https:// <Primary_Admin_IP>/api/v3/authorize" -H "accept:
application/json" -H "Content-Type: application/json" -H "X-Csrf-Token:
dc30b080e1ca9bc05ddb81104381d8c8" -d "{ \"username\": \"MyUsername\",
\"password\": \"MyPassword\", \"cookie\": true, \"csrfToken\": false}"
-k
```

> Si votre mot de passe GMI contient des caractères spéciaux, n'oubliez pas d'utiliser \ pour échapper à des caractères spéciaux. Par exemple, remplacez ! avec \!

6. Après avoir exécuté la commande curl précédente, le résultat vous donne un jeton d'autorisation comme dans l'exemple suivant :

```
{"responseTime":"2020-06-
03T00:12:17.031Z","status":"success","apiVersion":"3.2","data":"8a1e528d
-18a7-4283-9a5e-b2e6d731e0b2"}
```

Vous pouvez désormais utiliser la chaîne du jeton d'autorisation pour accéder aux métriques via cURL. La procédure d'accès aux métriques est similaire aux étapes de la section "Surveillance avancée dans StorageGRID". Cependant, à des fins de démonstration, nous montrons un exemple avec GET /grid/metric-labels/{label}/values sélectionné dans la catégorie Metrics.

7. Par exemple, la commande curl suivante avec le jeton d'autorisation précédent répertorie les noms de sites dans StorageGRID.

```
curl -X GET "https://10.193.92.230/api/v3/grid/metric-
labels/site_name/values" -H "accept: application/json" -H
"Authorization: Bearer 8a1e528d-18a7-4283-9a5e-b2e6d731e0b2"
```

La commande CURL génère la sortie suivante :

```
{"responseTime":"2020-06-
03T00:17:00.844Z","status":"success","apiVersion":"3.2","data":["us-
east-fuse","us-west-fuse"]}
```

Affichez les metrics à l'aide du tableau de bord Grafana dans StorageGRID

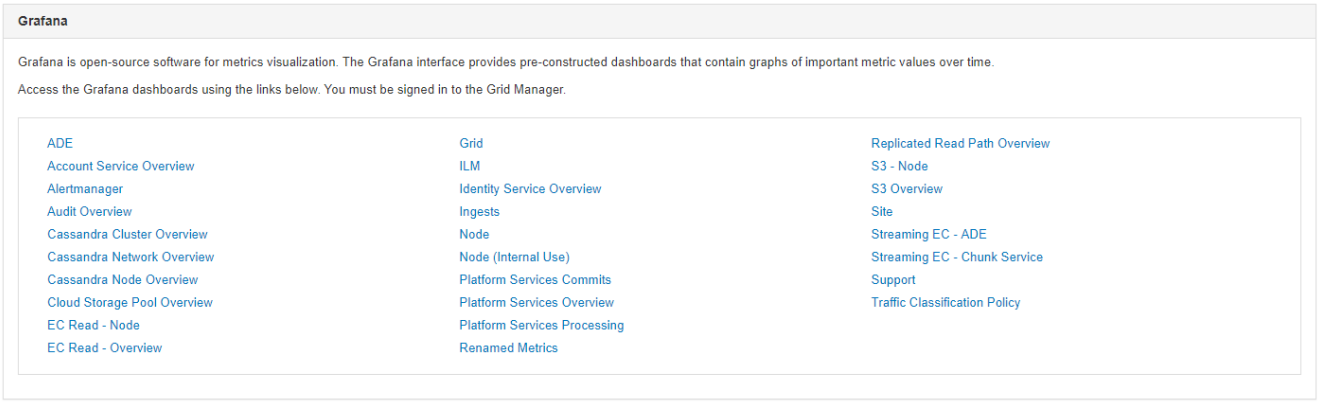
Découvrez comment utiliser l'interface Grafana pour visualiser et surveiller vos données StorageGRID.

Grafana est un logiciel open source pour la visualisation des mesures. Par défaut, nous disposons de tableaux de bord préconstruits qui fournissent des informations utiles et puissantes sur votre système StorageGRID.

Ces tableaux de bord préconstruits sont non seulement utiles pour la surveillance, mais aussi pour le dépannage d'un problème. Certains sont destinés à être utilisés par le support technique. Par exemple, pour afficher les mesures d'un nœud de stockage, procédez comme suit.

Étapes

1. Dans l'interface GMI, **support › Metrics**.
2. Dans la section Grafana, sélectionnez le tableau de bord Node.



3. Dans Grafana, définissez les hôtes sur le nœud sur lequel vous souhaitez afficher les mesures. Dans ce cas, un nœud de stockage est sélectionné. Plus d'informations sont fournies que les captures d'écran suivantes.

Utilisez les stratégies de classification du trafic dans StorageGRID

Découvrez comment configurer et configurer des règles de classification du trafic pour gérer et optimiser le trafic réseau dans StorageGRID.

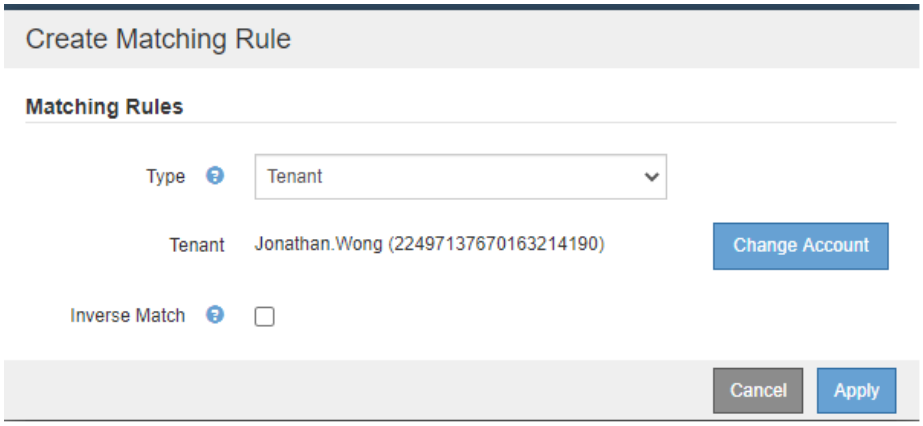
Les règles de classification du trafic fournissent une méthode de surveillance et/ou de limitation du trafic basée sur un locataire, un compartiments, des sous-réseaux IP ou des terminaux d'équilibrage de charge spécifiques. La connectivité réseau et la bande passante sont des mesures particulièrement importantes pour StorageGRID.

Pour configurer une stratégie de classification de trafic, procédez comme suit :

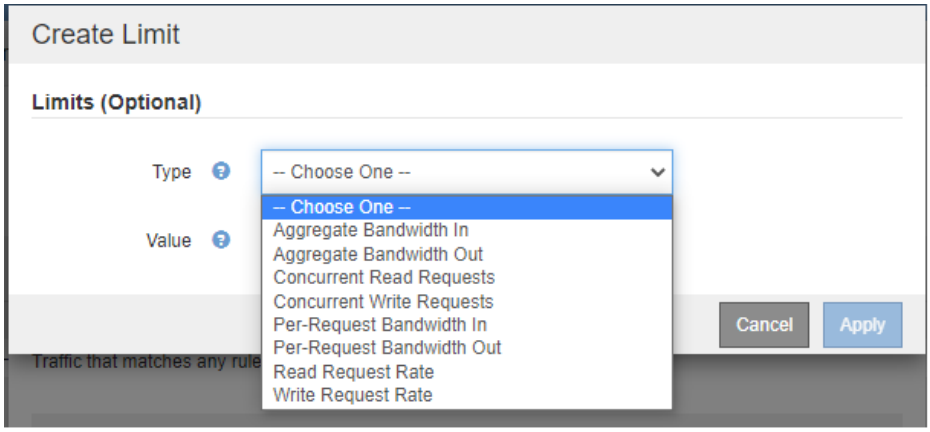
Étapes

1. Dans l'interface GMI, accédez au **Configuration › Paramètres système › Classification du trafic**.
2. Cliquez sur Créer +

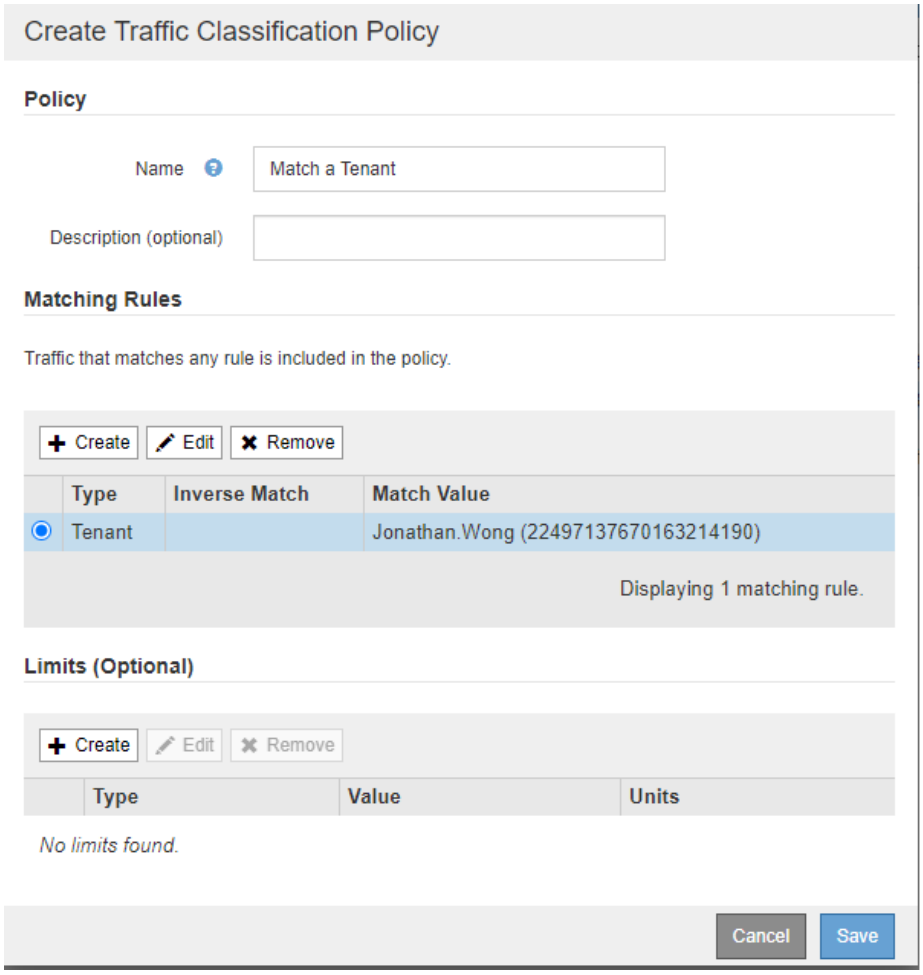
3. Entrez un nom et une description pour votre police.
4. Créez une règle correspondante.



5. Définissez une limite (facultatif).



6. Enregistrez votre police



Pour afficher les mesures associées à votre stratégie de classification de trafic, sélectionnez votre stratégie et cliquez sur métriques. Un tableau de bord Grafana est généré et affiche des informations telles que le trafic des demandes Load Balancer et la durée moyenne des demandes.

Utilisez les journaux d'audit pour surveiller StorageGRID

Découvrez comment utiliser le journal d'audit StorageGRID pour obtenir des informations détaillées sur les activités des locataires et du grid et comment exploiter des outils tels que Splunk pour l'analyse des journaux.

Le journal des audits StorageGRID vous permet de collecter des informations détaillées sur les activités du locataire et du grid. Le journal des audits peut être exposé à des fins d'analytique via le protocole NFS. Pour obtenir des instructions détaillées sur l'exportation du journal d'audit, reportez-vous au Guide de l'administrateur.

Une fois l'audit exporté, vous pouvez utiliser des outils d'analyse des journaux tels que Splunk ou Logstash + Elasticsearch pour comprendre l'activité des locataires ou créer des rapports détaillés de facturation et de facturation interne.

Des informations détaillées sur les messages d'audit sont disponibles dans la documentation StorageGRID. Voir "Messages d'audit".

Utilisez l'application StorageGRID pour Splunk

En savoir plus sur l'application NetApp StorageGRID pour Splunk qui permet de surveiller et d'analyser votre environnement StorageGRID au sein de la plateforme Splunk.

Splunk est une plateforme logicielle qui importe et indexe les données machine pour offrir de puissantes fonctionnalités de recherche et d'analyse. L'application NetApp StorageGRID est un complément pour Splunk qui importe et enrichit les données à partir de StorageGRID.

Vous trouverez des instructions sur l'installation, la mise à niveau et la configuration du module complémentaire StorageGRID à l'adresse suivante : https://splunkbase.splunk.com/app/3895/#/details

Tr-4882 : installation d'une grille métallique StorageGRID

Introduction à l'installation de StorageGRID

Découvrez comment installer StorageGRID sur des hôtes bare Metal.

Le TR-4882 fournit un ensemble d'instructions pratiques et détaillées qui produit une installation de travail de NetApp StorageGRID. L'installation peut se faire soit sur des serveurs bare Metal, soit sur des machines virtuelles exécutées sur Red Hat Enterprise Linux (RHEL). L'approche consiste à effectuer une installation « optiniée » de six services conteneurisés StorageGRID sur trois machines physiques (ou virtuelles) dans une disposition et une configuration de stockage suggérées. Certains clients peuvent comprendre plus facilement le processus de déploiement en suivant l'exemple de déploiement présenté dans ce rapport technique.

Pour une compréhension plus approfondie de StorageGRID et du processus d'installation, consultez [StorageGRID d'installation, de https://docs.netapp.com/us-en/storagegrid-118/landing-install-upgrade/index.html mise à niveau et de correctif] dans la documentation du produit.

Avant de commencer votre déploiement, examinons les exigences en matière de calcul, de stockage et de réseau pour le logiciel NetApp StorageGRID. StorageGRID s'exécute comme un service conteneurisé au sein de Podman ou Docker. Dans ce modèle, certaines exigences concernent le système d'exploitation hôte (le système qui héberge Docker, lequel exécute le logiciel StorageGRID). D'autres ressources sont allouées directement aux conteneurs Docker exécutés sur chaque hôte. Dans ce déploiement, afin d'optimiser

l'utilisation du matériel, nous déployons deux services par hôte physique. Pour plus d'informations, veuillez consulter la section suivante "Conditions préalables à l'installation de StorageGRID".

Les étapes décrites dans ce rapport technique permettent d'effectuer une installation StorageGRID fonctionnelle sur six hôtes bare Metal. Vous disposez désormais d'une grille et d'un réseau client qui fonctionnent, ce qui est utile dans la plupart des scénarios de test.

Où trouver des informations complémentaires

Pour en savoir plus sur les informations données dans ce rapport technique, consultez les ressources de documentation suivantes :

- Centre de documentation NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-118/
- Accompagnement NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-enable/
- Documentation des produits NetApp https://www.netapp.com/support-and-training/documentation/

Conditions préalables à l'installation de StorageGRID

Découvrez les besoins en ressources de calcul, de stockage, de réseau, docker et de nœuds pour déployer StorageGRID.

Exigences de calcul

Le tableau ci-dessous répertorie les ressources minimales requises pour chaque type de nœud StorageGRID. Il s'agit des ressources minimales requises pour les nœuds StorageGRID.

Type de nœud	Cœurs de processeurs	RAM
Admin	8	24 GO
Stockage	8	24 GO
Passerelle	8	24 GO

En outre, chaque hôte Docker physique doit disposer d'un minimum de 16 Go de RAM pour fonctionner correctement. Ainsi, par exemple, pour héberger deux des services décrits dans le tableau ensemble sur un hôte Docker physique, effectuez le calcul suivant :

24 + 24 + 16 = 64 Go de RAM et 8 + 8 = 16 cœurs

Comme nombre de serveurs modernes dépassent ces exigences, nous combinons six services (conteneurs StorageGRID) en trois serveurs physiques.

Configuration réseau requise

Les trois types de trafic StorageGRID sont les suivants :

- **Trafic de grille (requis).** Trafic StorageGRID interne qui circule entre tous les nœuds de la grille.
- **Trafic Admin (facultatif).** Trafic utilisé pour l'administration et la maintenance du système.
- **Trafic client (facultatif).** Le trafic qui circule entre les applications client externes et la grille, y compris toutes les demandes de stockage objet des clients S3 et Swift.

Vous pouvez configurer jusqu'à trois réseaux à utiliser avec le système StorageGRID. Chaque type de réseau

doit se trouver sur un sous-réseau distinct sans chevauchement. Si tous les nœuds se trouvent sur le même sous-réseau, aucune adresse de passerelle n'est requise.

Pour cette évaluation, nous allons déployer sur deux réseaux, qui contiennent la grille et le trafic client. Il est possible d'ajouter un réseau d'administration plus tard pour servir cette fonction supplémentaire.

Il est très important de mapper les réseaux de manière cohérente aux interfaces sur tous les hôtes. Par exemple, s'il existe deux interfaces sur chaque nœud, sen192 et en224, elles doivent toutes être mappées sur le même réseau ou VLAN sur tous les hôtes. Dans cette installation, le programme d'installation les mappe dans les conteneurs Docker comme eth0@if2 et eth2@if3 (car le bouclage est if1 à l'intérieur du conteneur). Il est donc très important d'avoir un modèle cohérent.

Remarque sur la mise en réseau Docker

StorageGRID utilise la mise en réseau différemment de certaines implémentations de conteneurs Docker. Il n'utilise pas la mise en réseau fournie par Docker (ou Kubernetes ou Swarm). StorageGRID génère alors le conteneur sous la forme --net=none, de sorte que Docker ne fait rien pour le mettre en réseau. Une fois le conteneur généré par le service StorageGRID, un nouveau périphérique macvlan est créé à partir de l'interface définie dans le fichier de configuration du nœud. Ce périphérique a une nouvelle adresse MAC et agit comme un périphérique réseau distinct qui peut recevoir des paquets de l'interface physique. Le périphérique macvlan est alors déplacé dans l'espace de noms du conteneur et renommé eth0, eth1 ou eth2 à l'intérieur du conteneur. À ce stade, le périphérique réseau n'est plus visible dans le système d'exploitation hôte. Dans notre exemple, le dispositif réseau Grid est eth0 à l'intérieur des conteneurs Docker et le réseau client est eth2. Si nous disposions d'un réseau d'administration, le dispositif serait eth1 dans le conteneur.

> La nouvelle adresse MAC du périphérique réseau de conteneur peut nécessiter l'activation du mode promiscuous dans certains environnements réseau et virtuels. Ce mode permet au périphérique physique de recevoir et d'envoyer des paquets pour les adresses MAC qui diffèrent de l'adresse MAC physique connue. si vous exécutez VMware vSphere, vous devez accepter le mode promiscuité, les modifications d'adresse MAC et les transmissions forgées dans les groupes de ports qui serviront le trafic StorageGRID lors de l'exécution de RHEL. Ubuntu ou Debian fonctionne sans ces changements dans la plupart des circonstances.

Conditions de stockage

Les nœuds nécessitent chacun des périphériques de disque SAN ou locaux de la taille indiquée dans le tableau suivant.

> Les chiffres du tableau concernent chaque type de service StorageGRID, et non l'ensemble de la grille ni chaque hôte physique. En fonction des choix de déploiement, nous calculerons les chiffres pour chaque hôte physique dans "Configuration et configuration requise de l'hôte physique", plus loin dans ce document. Les chemins ou systèmes de fichiers marqués d'un astérisque seront créés dans le conteneur StorageGRID lui-même par le programme d'installation. Aucune configuration manuelle ni création de système de fichiers n'est requise de la part de l'administrateur, mais les hôtes doivent disposer de périphériques de stockage par blocs pour répondre à ces exigences. En d'autres termes, le périphérique de stockage par blocs doit apparaître à l'aide de la commande `lsblk` mais ne doit pas être formaté ni monté dans le système d'exploitation hôte.

Type de nœud	Objectif de LUN	Nombre de LUN	Taille minimale de la LUN	Système de fichiers manuel requis	Entrée de configuration de nœud suggérée
Tout	Espace système du nœud d'administration `/var/local` (SSD utile ici)	Un pour chaque nœud d'administration	90 GO	Non	`BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/ADM-VAR-LOCAL`
Tous les nœuds	Pool de stockage Docker au `/var/lib/docker for container pool`	Un pour chaque hôte (physique ou machine virtuelle)	100 Go par conteneur	Oui – etx4	Na : formatez et montez en tant que système de fichiers hôte (non mappé dans le conteneur)
Admin	Journaux d'audit de nœud d'administration (données système dans le conteneur d'administration) `/var/local/audit/export`	Un pour chaque nœud d'administration	200 GO	Non	`BLOCK_DEVICE_AUDIT_LOGS =/dev/mapper/ADM-OS`
Admin	Tables de nœuds d'administration (données système dans le conteneur d'administration) `/var/local/mysql_ibdata`	Un pour chaque nœud d'administration	200 GO	Non	`BLOCK_DEVICE_TABLES = /dev/mapper/ADM-MySQL`
Nœuds de stockage	Stockage objet (dispositifs en mode bloc `/var/local/rangedb0`) (SSD utile ici) `/var/local/rangedb1` `/var/local/rangedb2`	Trois pour chaque conteneur de stockage	4,000 GO	Non	`BLOCK_DEVICE_RANGEDB_000 = /dev/mapper/SN-Db00` `BLOCK_DEVICE_RANGEDB_001 = /dev/mapper/SN-Db01` `BLOCK_DEVICE_RANGEDB_002 = /dev/mapper/SN-Db02`

Dans cet exemple, les tailles de disque indiquées dans le tableau suivant sont nécessaires par type de conteneur. Les exigences par hôte physique sont décrites "Configuration et configuration requise de l'hôte physique" plus loin dans ce document.

Tailles de disques par type de conteneur

Conteneur d'administration

Nom	Taille (Gio)
Docker-Store	100 (par conteneur)
ADM-OS	90
SMA-Vérification	200
ADM-MySQL	200

Conteneur de stockage

Nom	Taille (Gio)
Docker-Store	100 (par conteneur)
SN-OS	90
Rangedb-0	4096
Rangedb-1	4096
Rangedb-2	4096

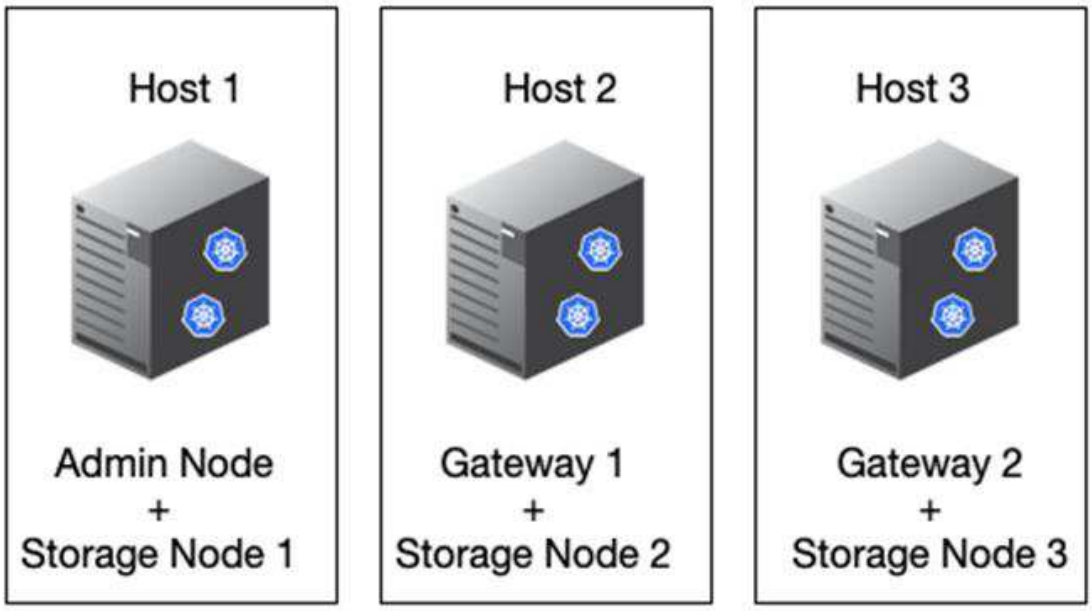
Conteneur de passerelle

Nom	Taille (Gio)
Docker-Store	100 (par conteneur)
/var/local	90

Configuration et configuration requise de l’hôte physique

En combinant les exigences de calcul et de réseau indiquées dans le tableau ci-dessus, vous pouvez obtenir un ensemble de matériel de base requis pour cette installation de trois serveurs physiques (ou virtuels) avec 16 cœurs, 64 Go de RAM et deux interfaces réseau. Si un débit plus élevé est souhaité, il est possible de lier deux interfaces ou plus sur la grille ou le réseau client et d’utiliser une interface marquée VLAN telle que bond0.520 dans le fichier de configuration du nœud. Si vous attendez des charges de travail plus intenses, il vaut mieux augmenter la mémoire pour l’hôte et les conteneurs.

Comme illustré dans la figure ci-dessous, ces serveurs hébergent six conteneurs Docker, deux par hôte. La RAM est calculée en fournissant 24 Go par conteneur et 16 Go pour le système d’exploitation hôte lui-même.



La mémoire RAM totale requise par hôte physique (ou machine virtuelle) est de 24 x 2 + 16 = 64 Go. Les tableaux suivants répertorient le stockage sur disque requis pour les hôtes 1, 2 et 3.

Hôte 1	**Taille (Gio)**
Docker Store	`/var/lib/docker` (Système de fichiers)
200 (100 x 2)	**Conteneur Admin**
`BLOCK_DEVICE_VAR_LOCAL`	90
`BLOCK_DEVICE_AUDIT_LOGS`	200
`BLOCK_DEVICE_TABLES`	200
Conteneur de stockage	SN-OS `/var/local` (périphérique)
90	Rangedb-0 (périphérique)
4096	Rangedb-1 (périphérique)
4096	Rangedb-2 (dispositif)

Hôte 2	**Taille (Gio)**
Docker Store	`/var/lib/docker` (Partagé)
200 (100 x 2)	**Conteneur passerelle**
GW-OS `*/var/local`	100
Conteneur de stockage	`*/var/local`
100	Rangedb-0

Hôte 2	Taille (Gio)
4096	Rangedb-1
4096	Rangedb-2

Hôte 3	Taille (Gio)
Docker Store	`/var/lib/docker` (Partagé)
200 (100 x 2)	**Conteneur passerelle**
*/var/local	100
Conteneur de stockage	*/var/local
100	Rangedb-0
4096	Rangedb-1
4096	Rangedb-2

Le Docker Store a été calculé en autorisant 100 Go par /var/local (par conteneur) x deux conteneurs = 200 Go.

Préparation des nœuds

Pour préparer l'installation initiale de StorageGRID, installez d'abord RHEL version 9.2 et activez SSH. Configurez les interfaces réseau, le protocole NTP (Network Time Protocol), le DNS et le nom d'hôte conformément aux bonnes pratiques. Vous avez besoin d'au moins une interface réseau activée sur le réseau en grille et une autre pour le réseau client. Si vous utilisez une interface marquée VLAN, configurez-la comme indiqué dans les exemples ci-dessous. Sinon, une simple configuration d'interface réseau standard suffit.

Si vous devez utiliser une balise VLAN sur l'interface réseau de la grille, votre configuration doit avoir deux fichiers `/etc/sysconfig/network-scripts/` au format suivant :

```
# cat /etc/sysconfig/network-scripts/ifcfg-enp67s0
# This is the parent physical device
TYPE=Ethernet
BOOTPROTO=none
DEVICE=enp67s0
ONBOOT=yes
# cat /etc/sysconfig/network-scripts/ifcfg-enp67s0.520
# The actual device that will be used by the storage node file
DEVICE=enp67s0.520
BOOTPROTO=none
NAME=enp67s0.520
IPADDR=10.10.200.31
PREFIX=24
VLAN=yes
ONBOOT=yes
```

Cet exemple suppose que votre périphérique réseau physique pour le réseau de grille est enp67s0. Il pourrait également être un dispositif lié tel que bond0. Que vous utilisiez la liaison ou une interface réseau standard,

vous devez utiliser l'interface marquée VLAN dans votre fichier de configuration de nœud si votre port réseau n'a pas de VLAN par défaut ou si le VLAN par défaut n'est pas associé au réseau de grille. Le conteneur StorageGRID lui-même ne débalise pas les trames Ethernet, il doit donc être géré par le système d'exploitation parent.

Configuration du stockage en option avec iSCSI

Si vous n'utilisez pas de stockage iSCSI, vous devez vous assurer que host1, host2 et host3 disposent de périphériques de blocs d'une taille suffisante pour répondre à leurs besoins. Voir "Tailles de disques par type de conteneur" pour les exigences de stockage de host1, host2 et host3.

Pour configurer le stockage avec iSCSI, procédez comme suit :

Étapes

1. Si vous utilisez un stockage iSCSI externe tel que le logiciel de gestion des données NetApp E-Series ou NetApp ONTAP®, installez les packages suivants :

```
sudo yum install iscsi-initiator-utils
sudo yum install device-mapper-multipath
```

2. Recherchez l'ID d'initiateur sur chaque hôte.

```
# cat /etc/iscsi/initiatorname.iscsi
InitiatorName=iqn.2006-04.com.example.node1
```

3. En utilisant le nom de l'initiateur de l'étape 2, mappez les LUN de votre périphérique de stockage (du nombre et de la taille indiqués dans le tableau "Conditions de stockage") à chaque nœud de stockage.
4. Identifiez les LUN créées avec et connectez-vous à ces LUN `iscsiadm` .

```
# iscsiadm -m discovery -t st -p target-ip-address
# iscsiadm -m node -T iqn.2006-04.com.example:3260 -l
Logging in to [iface: default, target: iqn.2006-04.com.example:3260,
portal: 10.64.24.179,3260] (multiple)
Login to [iface: default, target: iqn.2006-04.com.example:3260, portal:
10.64.24.179,3260] successful.
```

> Pour plus de détails, consultez le "Création d'un initiateur iSCSI" portail des clients Red Hat.

5. Pour afficher les chemins d'accès multiples et les WWID de LUN associés, exécutez la commande suivante :

```
# multipath -ll
```

Si vous n'utilisez pas iSCSI avec des périphériques à chemins d'accès multiples, montez simplement votre périphérique à l'aide d'un nom de chemin unique qui persistera à modifier et à redémarrer le périphérique.

```
/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:1:0
```

L'utilisation de `/dev/sdx` noms de périphériques peut entraîner des problèmes ultérieurement si des périphériques sont supprimés ou ajoutés. si vous utilisez des périphériques multivoies, modifiez le `/etc/multipath.conf` fichier pour utiliser les alias comme suit.

Ces périphériques peuvent être présents ou non sur tous les nœuds, selon la disposition.

```
multipaths {
multipath {
wwid 36d039ea00005f06a000003c45fa8f3dc
alias Docker-Store
}
multipath {
wwid 36d039ea00006891b000004025fa8f597
alias Adm-Audit
}
multipath {
wwid 36d039ea00005f06a000003c65fa8f3f0
alias Adm-MySQL
}
multipath {
wwid 36d039ea00006891b000004015fa8f58c
alias Adm-OS
}
multipath {
wwid 36d039ea00005f06a000003c55fa8f3e4
alias SN-OS
}
multipath {
wwid 36d039ea00006891b000004035fa8f5a2
alias SN-Db00
}
multipath {
wwid 36d039ea00005f06a000003c75fa8f3fc
alias SN-Db01
}
multipath {
    wwid 36d039ea00006891b000004045fa8f5af
alias SN-Db02
}
multipath {
wwid 36d039ea00005f06a000003c85fa8f40a
```

```
alias GW-OS
}
}
```

Avant d'installer Docker sur votre système d'exploitation hôte, formatez et montez le support de LUN ou de disque `/var/lib/docker`. Les autres LUN sont définies dans le fichier de configuration du nœud et utilisées directement par les conteneurs StorageGRID. C'est-à-dire qu'ils n'apparaissent pas dans le système d'exploitation hôte ; ils apparaissent dans les conteneurs eux-mêmes et ces systèmes de fichiers sont gérés par le programme d'installation.

Si vous utilisez une LUN avec support iSCSI, placez un élément similaire à la ligne suivante dans votre fichier fstab. Comme indiqué, les autres LUN n'ont pas besoin d'être montées dans le système d'exploitation hôte, mais doivent apparaître comme périphériques de bloc disponibles.

```
/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:1:0 /var/lib/docker ext4
defaults 0 0
```

Préparation de l'installation de Docker

Pour préparer l'installation de Docker, procédez comme suit :

Étapes

1. Créez un système de fichiers sur le volume de stockage Docker sur les trois hôtes.

   ```
   # sudo mkfs.ext4 /dev/sd?
   ```

   Si vous utilisez des périphériques iSCSI avec chemins d'accès multiples, utilisez `/dev/mapper/Docker-Store`.

2. Créer le point de montage du volume de stockage Docker :

   ```
   # sudo mkdir -p /var/lib/docker
   ```

3. Ajoutez une entrée similaire pour docker-Storage-volume-device à `/etc/fstab`.

   ```
   /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:1:0 /var/lib/docker ext4
   defaults 0 0
   ```

   L'option suivante `_netdev` est recommandée uniquement si vous utilisez un périphérique iSCSI. Si vous utilisez un périphérique de bloc local `_netdev` n'est pas nécessaire et `defaults` est recommandé.

   ```
   /dev/mapper/Docker-Store /var/lib/docker ext4 _netdev 0 0
   ```

4. Montez le nouveau système de fichiers et affichez l'utilisation du disque.

```
# sudo mount /var/lib/docker
[root@host1]# df -h | grep docker
/dev/sdb 200G 33M 200G 1% /var/lib/docker
```

5. Désactivez l'échange et désactivez-le pour des raisons de performances.

```
$ sudo swapoff --all
```

6. Pour conserver les paramètres, supprimez toutes les entrées de swap de /etc/fstab telles que :

```
/dev/mapper/rhel-swap swap defaults 0 0
```

> Si vous ne désactivez pas ces fichiers, les performances peuvent être considérablement réduites.

7. Effectuez un redémarrage test de votre nœud pour vous assurer que le `/var/lib/docker` volume est persistant et que tous les périphériques de disque sont retournés.

Installez Docker pour StorageGRID

Découvrez comment installer Docker pour StorageGRID.

Pour installer Docker, procédez comme suit :

Étapes

1. Configurez yum repo pour Docker.

```
sudo yum install -y yum-utils
sudo yum-config-manager --add-repo \
https://download.docker.com/linux/rhel/docker-ce.repo
```

2. Installez les packages nécessaires.

```
sudo yum install docker-ce docker-ce-cli containerd.io
```

3. Démarrez Docker.

```
sudo systemctl start docker
```

4. Tester Docker.

```
sudo docker run hello-world
```

5. Assurez-vous que Docker s'exécute au démarrage du système.

```
sudo systemctl enable docker
```

Préparez les fichiers de configuration des nœuds pour StorageGRID

Découvrez comment préparer les fichiers de configuration des nœuds pour StorageGRID.

À un niveau élevé, le processus de configuration des nœuds comprend les étapes suivantes :

Étapes

1. Créez le `/etc/storagegrid/nodes` répertoire sur tous les hôtes.

```
sudo [root@host1 ~]# mkdir -p /etc/storagegrid/nodes
```

2. Créez les fichiers nécessaires par hôte physique pour correspondre à la disposition du type de conteneur/nœud. Dans cet exemple, nous avons créé deux fichiers par hôte physique sur chaque machine hôte.

> ⓘ Le nom du fichier définit le nom réel du nœud pour l'installation. Par exemple, `dc1-adm1.conf` devient un nœud nommé `dc1-adm1`.

— Host1 :
```
dc1-adm1.conf
dc1-sn1.conf
```

— Host2 :
```
dc1-gw1.conf
dc1-sn2.conf
```

— Host3 :
```
dc1-gw2.conf
dc1-sn3.conf
```

Préparation des fichiers de configuration du nœud

Les exemples suivants utilisent le `/dev/disk/by-path` format. Vous pouvez vérifier les chemins d'accès corrects en exécutant les commandes suivantes :

```
[root@host1 ~]# lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
sda 8:0 0 90G 0 disk
```

```
├─sda1 8:1 0 1G 0 part /boot
└─sda2 8:2 0 89G 0 part
├─rhel-root 253:0 0 50G 0 lvm /
├─rhel-swap 253:1 0 9G 0 lvm
└─rhel-home 253:2 0 30G 0 lvm /home
sdb 8:16 0 200G 0 disk /var/lib/docker
sdc 8:32 0 90G 0 disk
sdd 8:48 0 200G 0 disk
sde 8:64 0 200G 0 disk
sdf 8:80 0 4T 0 disk
sdg 8:96 0 4T 0 disk
sdh 8:112 0 4T 0 disk
sdi 8:128 0 90G 0 disk
sr0 11:0 1 1024M 0 rom
```

Et ces commandes :

```
[root@host1 ~]# ls -l /dev/disk/by-path/
total 0
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:02:01.0-ata-1.0 ->
../../sr0
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:0:0 ->
../../sda
lrwxrwxrwx 1 root root 10 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:0:0-part1
-> ../../sda1
lrwxrwxrwx 1 root root 10 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:0:0-part2
-> ../../sda2
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:1:0 ->
../../sdb
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:2:0 ->
../../sdc
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:3:0 ->
../../sdd
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:4:0 ->
../../sde
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:5:0 ->
../../sdf
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:6:0 ->
../../sdg
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:8:0 ->
../../sdh
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:9:0 ->
../../sdi
```

Exemple pour le nœud d'administration principal

Exemple de nom de fichier :

```
/etc/storagegrid/nodes/dc1-adm1.conf
```

Exemple de contenu de fichier :

> Les chemins de disque peuvent suivre les exemples ci-dessous ou utiliser `/dev/mapper/alias` la dénomination de style. N'utilisez pas de noms de périphériques de blocage tels que `/dev/sdb` , car ils peuvent changer au redémarrage et causer des dommages importants à votre grille.

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Primary
MAXIMUM_RAM = 24g
BLOCK_DEVICE_VAR_LOCAL = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:2:0
BLOCK_DEVICE_AUDIT_LOGS = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:3:0
BLOCK_DEVICE_TABLES = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:4:0
GRID_NETWORK_TARGET = ens192
CLIENT_NETWORK_TARGET = ens224
GRID_NETWORK_IP = 10.193.204.43
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.193.204.1
CLIENT_NETWORK_CONFIG = STATIC
CLIENT_NETWORK_IP = 10.193.205.43
CLIENT_NETWORK_MASK = 255.255.255.0
CLIENT_NETWORK_GATEWAY = 10.193.205.1
```

Exemple de nœud de stockage

Exemple de nom de fichier :

```
/etc/storagegrid/nodes/dc1-sn1.conf
```

Exemple de contenu de fichier :

```
NODE_TYPE = VM_Storage_Node
MAXIMUM_RAM = 24g
ADMIN_IP = 10.193.174.43
BLOCK_DEVICE_VAR_LOCAL = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:9:0
BLOCK_DEVICE_RANGEDB_00 = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:5:0
BLOCK_DEVICE_RANGEDB_01 = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:6:0
BLOCK_DEVICE_RANGEDB_02 = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:8:0
```

```
GRID_NETWORK_TARGET = ens192
CLIENT_NETWORK_TARGET = ens224
GRID_NETWORK_IP = 10.193.204.44
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.193.204.1
```

Exemple de nœud de passerelle

Exemple de nom de fichier :

```
/etc/storagegrid/nodes/dc1-gw1.conf
```

Exemple de contenu de fichier :

```
NODE_TYPE = VM_API_Gateway
MAXIMUM_RAM = 24g
ADMIN_IP = 10.193.204.43
BLOCK_DEVICE_VAR_LOCAL = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:1:0
GRID_NETWORK_TARGET = ens192
CLIENT_NETWORK_TARGET = ens224
GRID_NETWORK_IP = 10.193.204.47
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.193.204.1
CLIENT_NETWORK_IP = 10.193.205.47
CLIENT_NETWORK_MASK = 255.255.255.0
CLIENT_NETWORK_GATEWAY = 10.193.205.1
```

Installez les dépendances et les packages StorageGRID

Découvrez comment installer les packages et les dépendances StorageGRID.

Pour installer les dépendances et les packages StorageGRID, exécutez les commandes suivantes :

```
[root@host1 rpms]# yum install -y python-netaddr
[root@host1 rpms]# rpm -ivh StorageGRID-Webscale-Images-*.rpm
[root@host1 rpms]# rpm -ivh StorageGRID-Webscale-Service-*.rpm
```

Validez les fichiers de configuration StorageGRID

Découvrez comment valider le contenu des fichiers de configuration pour StorageGRID.

Après avoir créé les fichiers de configuration dans `/etc/storagegrid/nodes` pour chacun de vos nœuds StorageGRID, vous devez valider le contenu de ces fichiers.

Pour valider le contenu des fichiers de configuration, exécutez la commande suivante sur chaque hôte :

```
sudo storagegrid node validate all
```

Si les fichiers sont corrects, le résultat indique RÉUSSI pour chaque fichier de configuration :

```
Checking for misnamed node configuration files… PASSED
Checking configuration file for node dc1-adm1… PASSED
Checking configuration file for node dc1-gw1… PASSED
Checking configuration file for node dc1-sn1… PASSED
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes… PASSED
```

Si les fichiers de configuration sont incorrects, les problèmes sont affichés comme AVERTISSEMENT et ERREUR. Si des erreurs de configuration sont détectées, vous devez les corriger avant de poursuivre l'installation.

```
Checking for misnamed node configuration files…
  WARNING: ignoring /etc/storagegrid/nodes/dc1-adm1
  WARNING: ignoring /etc/storagegrid/nodes/dc1-sn2.conf.keep
  WARNING: ignoring /etc/storagegrid/nodes/my-file.txt
Checking configuration file for node dc1-adm1…
  ERROR: NODE_TYPE = VM_Foo_Node
         VM_Foo_Node is not a valid node type.  See *.conf.sample
  ERROR: ADMIN_ROLE = Foo
         Foo is not a valid admin role.  See *.conf.sample
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-gw1-var-local
         /dev/mapper/sgws-gw1-var-local is not a valid block device
Checking configuration file for node dc1-gw1…
  ERROR: GRID_NETWORK_TARGET = bond0.1001
         bond0.1001 is not a valid interface.  See `ip link show`
  ERROR: GRID_NETWORK_IP = 10.1.3
         10.1.3 is not a valid IPv4 address
  ERROR: GRID_NETWORK_MASK = 255.248.255.0
         255.248.255.0 is not a valid IPv4 subnet mask
Checking configuration file for node dc1-sn1…
  ERROR: GRID_NETWORK_GATEWAY = 10.2.0.1
         10.2.0.1 is not on the local subnet
  ERROR: ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0foo
         Could not parse subnet list
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes…
  ERROR: GRID_NETWORK_IP = 10.1.0.4
         dc1-sn2 and dc1-sn3 have the same GRID_NETWORK_IP
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn2-var-local
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_VAR_LOCAL
  ERROR: BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn2-rangedb-0
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_RANGEDB_00
```

Démarrez le service d'hôte StorageGRID

Découvrez comment démarrer le service hôte StorageGRID.

Pour démarrer les nœuds StorageGRID et vous assurer qu'ils redémarrent après un redémarrage de l'hôte, vous devez activer et démarrer le service hôte StorageGRID.

Pour démarrer le service hôte StorageGRID, procédez comme suit.

Étapes

1. Exécutez les commandes suivantes sur chaque hôte :

```
sudo systemctl enable storagegrid
sudo systemctl start storagegrid
```

Le processus de démarrage peut prendre un certain temps lors de l'exécution initiale.

2. Exécutez la commande suivante pour vérifier que le déploiement se déroule :

```
sudo storagegrid node status node-name
```

3. Pour tout nœud qui renvoie un état de `Not-Running` ou `Stopped`, exécutez la commande suivante :

```
sudo storagegrid node start node-name
```

Par exemple, dans le résultat suivant, vous démarriez le `dc1-adm1` nœud :

```
[user@host1]# sudo storagegrid node status
Name Config-State Run-State
dc1-adm1 Configured Not-Running
dc1-sn1 Configured Running
```

4. Si vous avez précédemment activé et démarré le service hôte StorageGRID (ou si vous n'êtes pas sûr que le service a été activé et démarré), exécutez également la commande suivante :

```
sudo systemctl reload-or-restart storagegrid
```

Configurez le gestionnaire de grille dans StorageGRID

Découvrez comment configurer le Gestionnaire de grille dans StorageGRID sur le nœud d'administration principal.

Terminez l'installation en configurant le système StorageGRID à partir de l'interface utilisateur du Gestionnaire de grille sur le nœud d'administration principal.

Étapes générales

La configuration de la grille et la fin de l'installation impliquent les tâches suivantes :

Étapes

1. Accédez à Grid Manager
2. "Spécifier les informations de licence StorageGRID"
3. "Ajouter des sites à StorageGRID"
4. "Spécifiez les sous-réseaux de réseau de grille"
5. "Approuver les nœuds de la grille en attente"
6. "Spécifiez les informations du serveur NTP"
7. "Spécifiez les informations relatives au serveur système du nom de domaine"

8. "Spécifiez les mots de passe système StorageGRID"
9. "Vérifiez votre configuration et terminez l'installation"

Accédez à Grid Manager

Utilisez le Gestionnaire de grille pour définir toutes les informations requises pour configurer votre système StorageGRID.

Avant de commencer, le nœud d'administration principal doit être déployé et avoir terminé la séquence de démarrage initiale.

Pour utiliser Grid Manager pour définir des informations, procédez comme suit.

Étapes

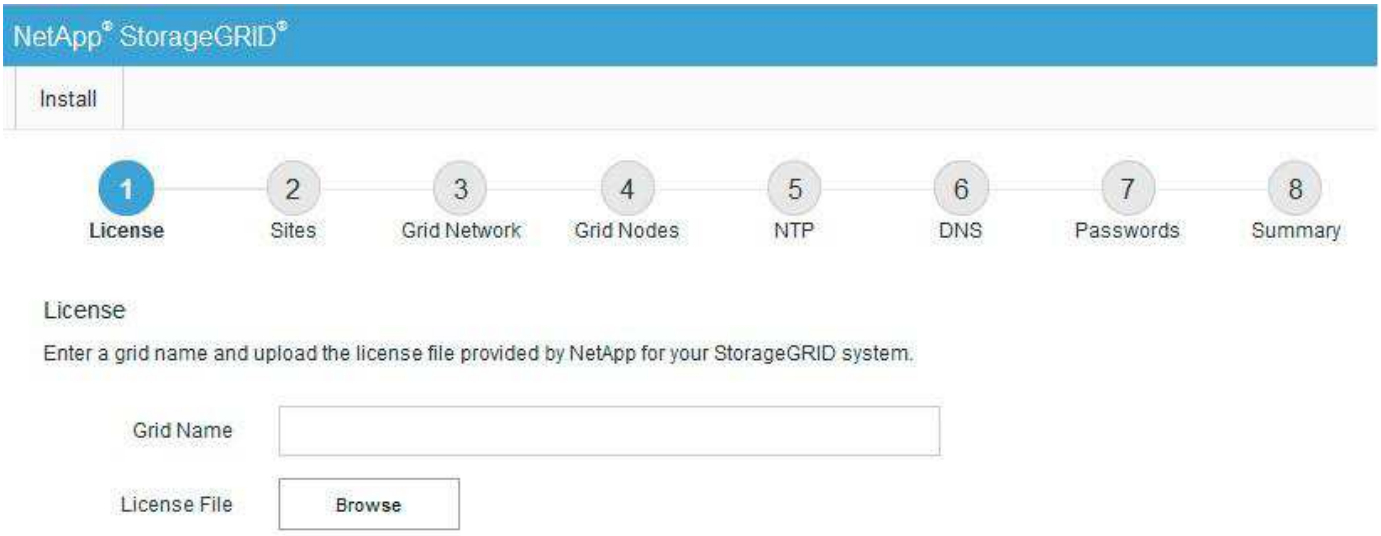
1. Accédez à Grid Manager à l'adresse suivante :

   ```
   https://primary_admin_node_grid_ip
   ```

   Vous pouvez également accéder à Grid Manager sur le port 8443.

   ```
   https://primary_admin_node_ip:8443
   ```

2. Cliquez sur installer un système StorageGRID. La page utilisée pour configurer une grille StorageGRID s'affiche.



Ajoutez les détails de la licence StorageGRID

Découvrez comment télécharger le fichier de licence StorageGRID.

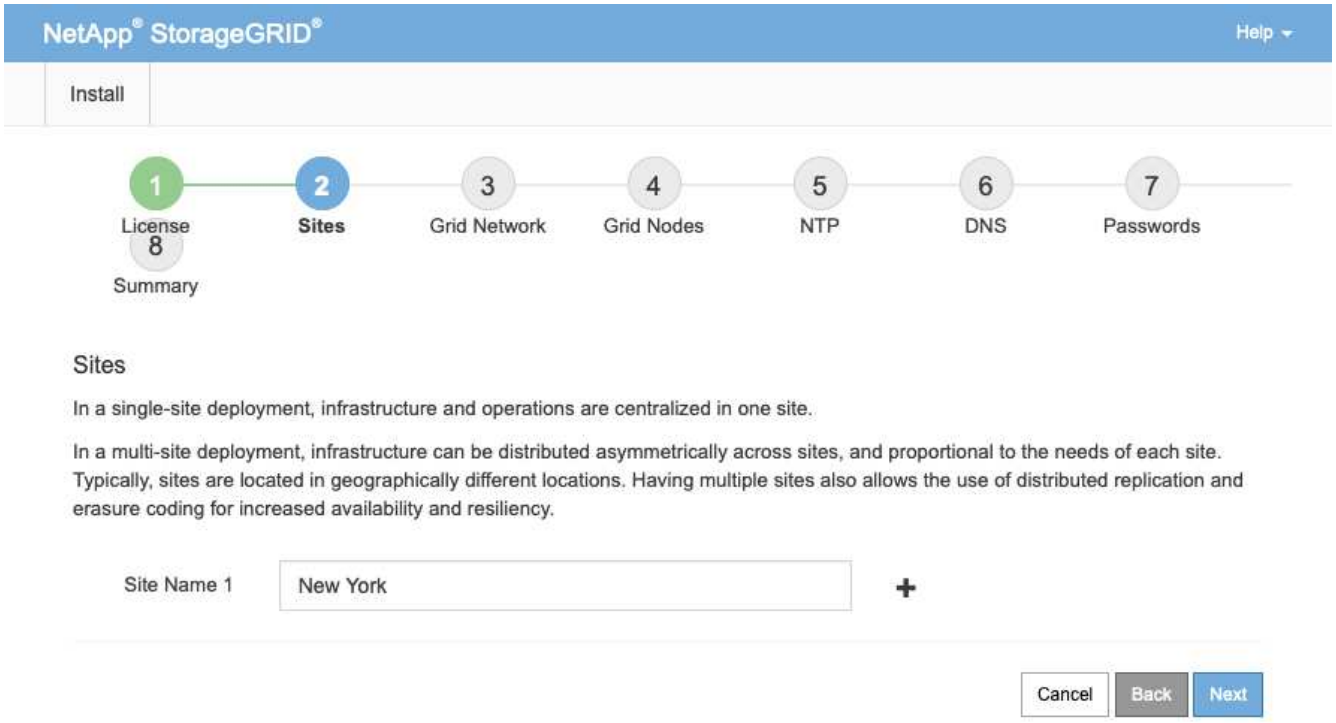
Vous devez indiquer le nom de votre système StorageGRID et télécharger le fichier de licence fourni par NetApp.

Pour spécifier les informations de licence StorageGRID, procédez comme suit :

Étapes

1. Sur la page Licence, dans le champ Nom de la grille, entrez un nom pour votre système StorageGRID. Après l'installation, le nom s'affiche en tant que premier niveau dans l'arborescence de la topologie de la grille.
2. Cliquez sur Parcourir, localisez le fichier de licence NetApp (`NLF-unique-id.txt`), puis cliquez sur Ouvrir. Le fichier de licence est validé et le numéro de série et la capacité de stockage sous licence s'affichent.

   L'archive d'installation de StorageGRID inclut une licence gratuite qui ne fournit aucun droit d'assistance pour le produit. Vous pouvez effectuer une mise à jour vers une licence offrant une assistance après l'installation.



3. Cliquez sur Suivant.

Ajouter des sites à StorageGRID

Découvrez comment ajouter des sites à StorageGRID afin d'améliorer la fiabilité et la capacité de stockage.

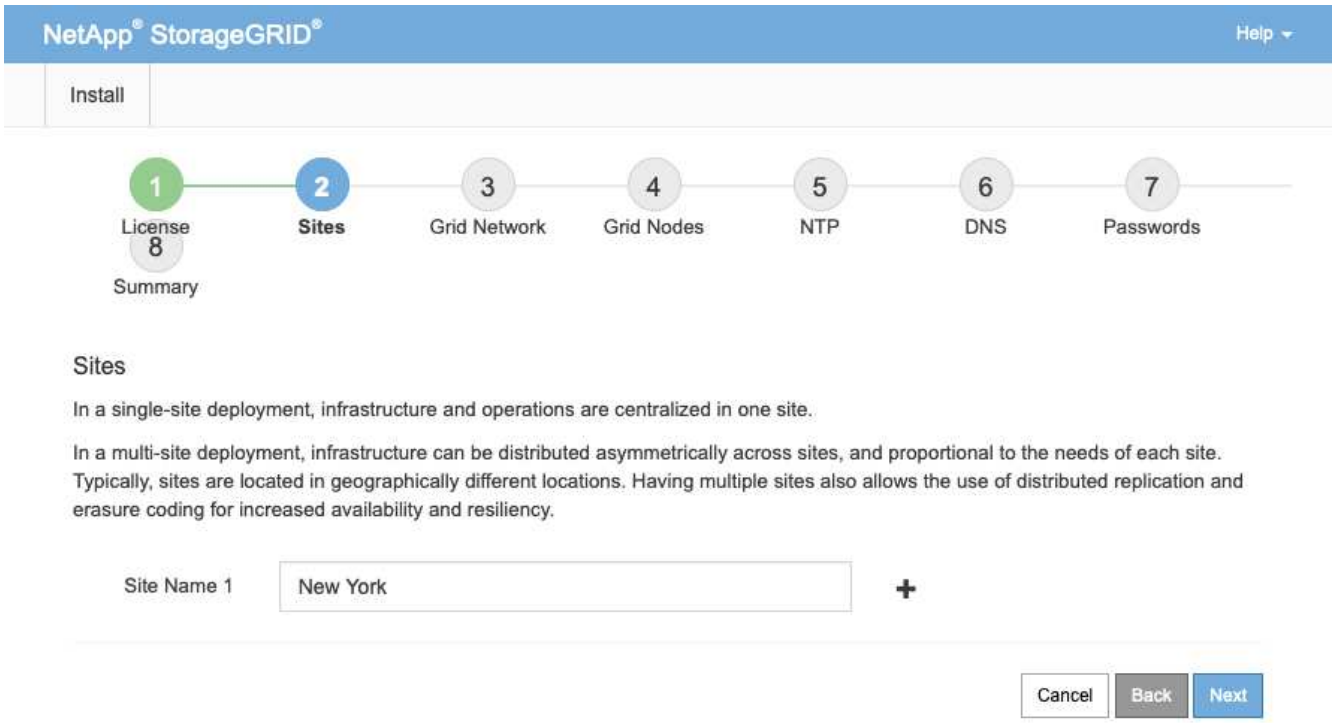
Lorsque vous installez StorageGRID, vous devez créer au moins un site. Vous pouvez créer des sites supplémentaires pour augmenter la fiabilité et la capacité de stockage de votre système StorageGRID.

Pour ajouter des sites, procédez comme suit :

Étapes

1. Sur la page sites, entrez le nom du site.
2. Pour ajouter des sites supplémentaires, cliquez sur le signe plus en regard de la dernière entrée de site et

entrez le nom dans la zone de texte Nouveau nom de site. Ajoutez autant de sites supplémentaires que nécessaire pour votre topologie de grille. Vous pouvez ajouter jusqu'à 16 sites.



3. Cliquez sur Suivant.

Spécifiez les sous-réseaux de réseau de grille pour StorageGRID

Découvrez comment configurer les sous-réseaux réseau de la grille pour StorageGRID.

Vous devez spécifier les sous-réseaux utilisés sur le réseau de la grille.

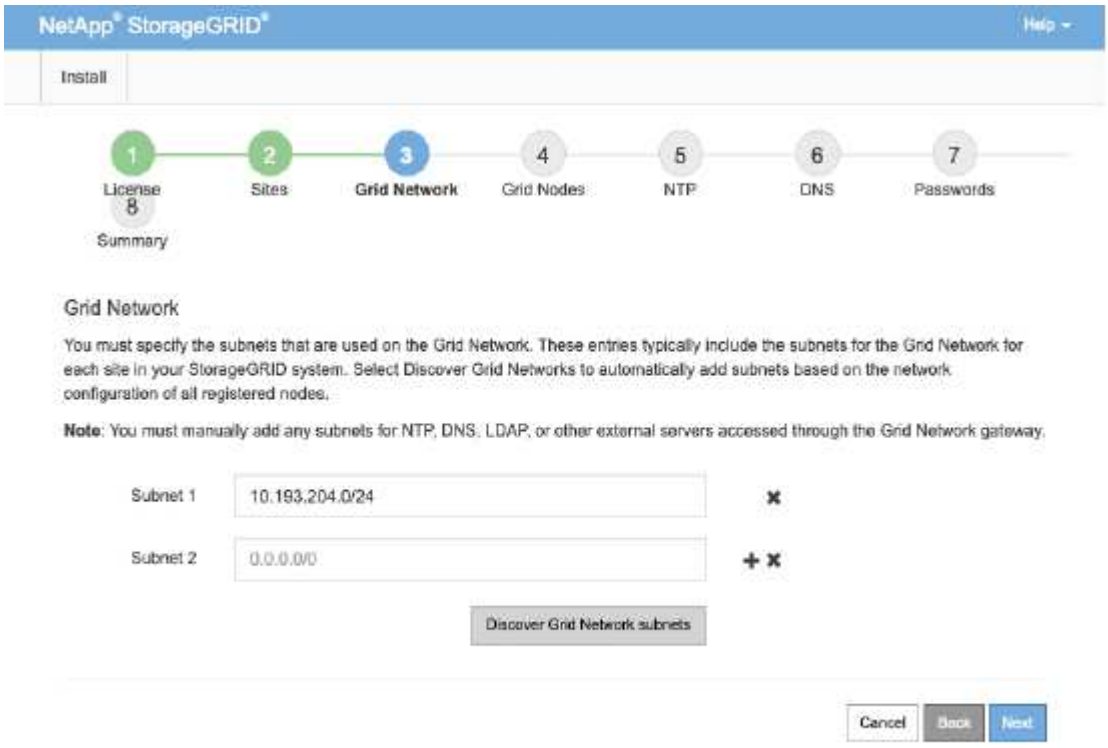
Les entrées de sous-réseau incluent les sous-réseaux du réseau de grille pour chaque site de votre système StorageGRID, en plus des sous-réseaux qui doivent être accessibles via le réseau de grille (par exemple, les sous-réseaux hébergeant vos serveurs NTP).

Si vous avez plusieurs sous-réseaux de grille, la passerelle de réseau de grille est requise. Tous les sous-réseaux de la grille spécifiés doivent être accessibles via cette passerelle.

Pour spécifier des sous-réseaux de réseau de grille, procédez comme suit :

Étapes

1. Dans la zone de texte sous-réseau 1, spécifiez l'adresse réseau CIDR d'au moins un réseau de grille.
2. Cliquez sur le signe plus à côté de la dernière entrée pour ajouter une entrée réseau supplémentaire. Si vous avez déjà déployé au moins un nœud, cliquez sur détecter les sous-réseaux de réseaux de grille pour remplir automatiquement la liste de sous-réseaux de réseau de grille avec les sous-réseaux signalés par les nœuds de grille qui ont été enregistrés avec Grid Manager.



3. Cliquez sur Suivant.

Approuver les nœuds grid pour StorageGRID

Découvrez comment vérifier et approuver tous les nœuds de grille en attente qui rejoignent le système StorageGRID.

Vous devez approuver chaque nœud de grille avant de rejoindre le système StorageGRID.

Avant de commencer, tous les nœuds de grid des appliances virtuelles et StorageGRID doivent être déployés.

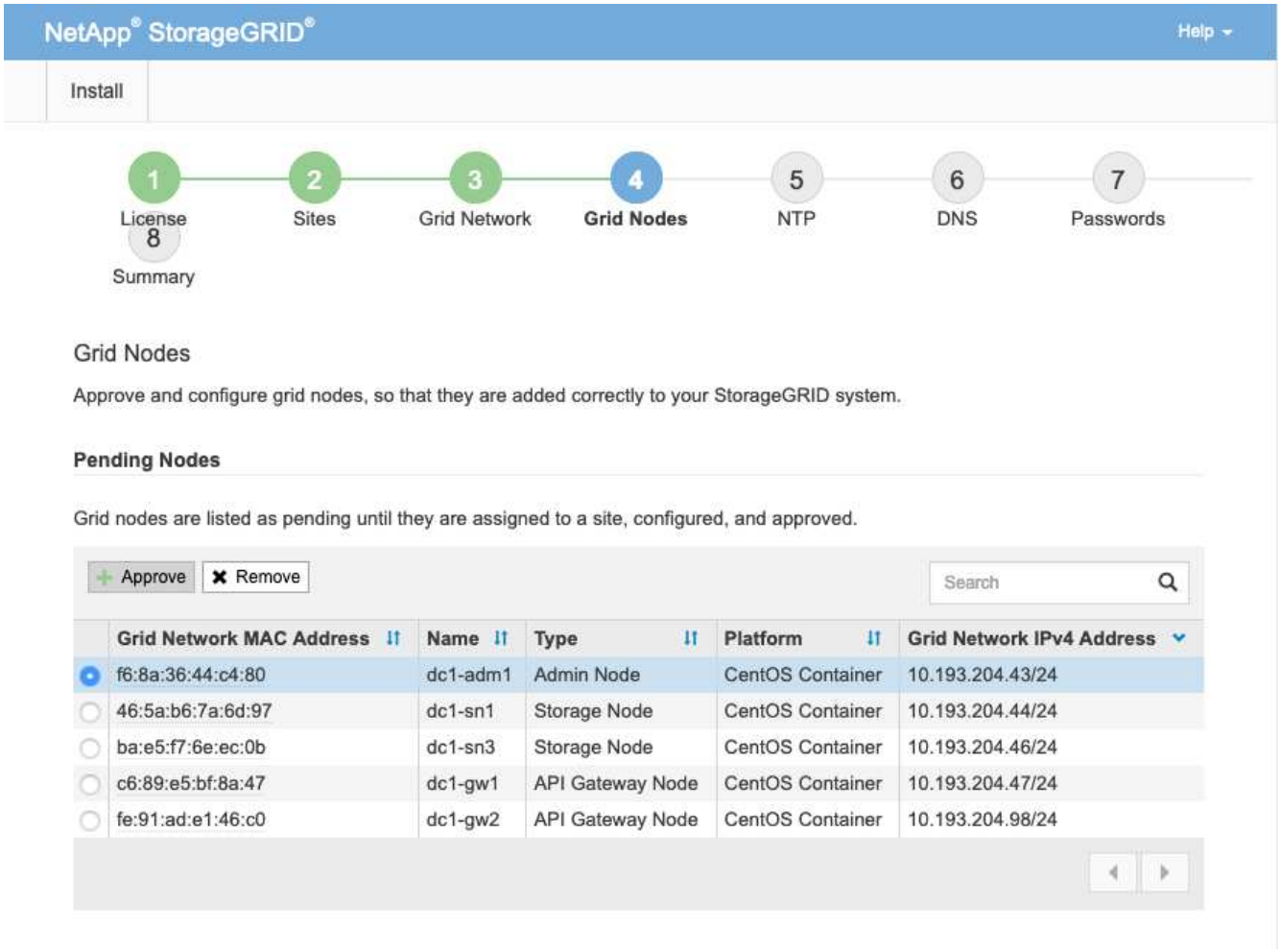
Pour approuver des nœuds de grille en attente, procédez comme suit :

Étapes

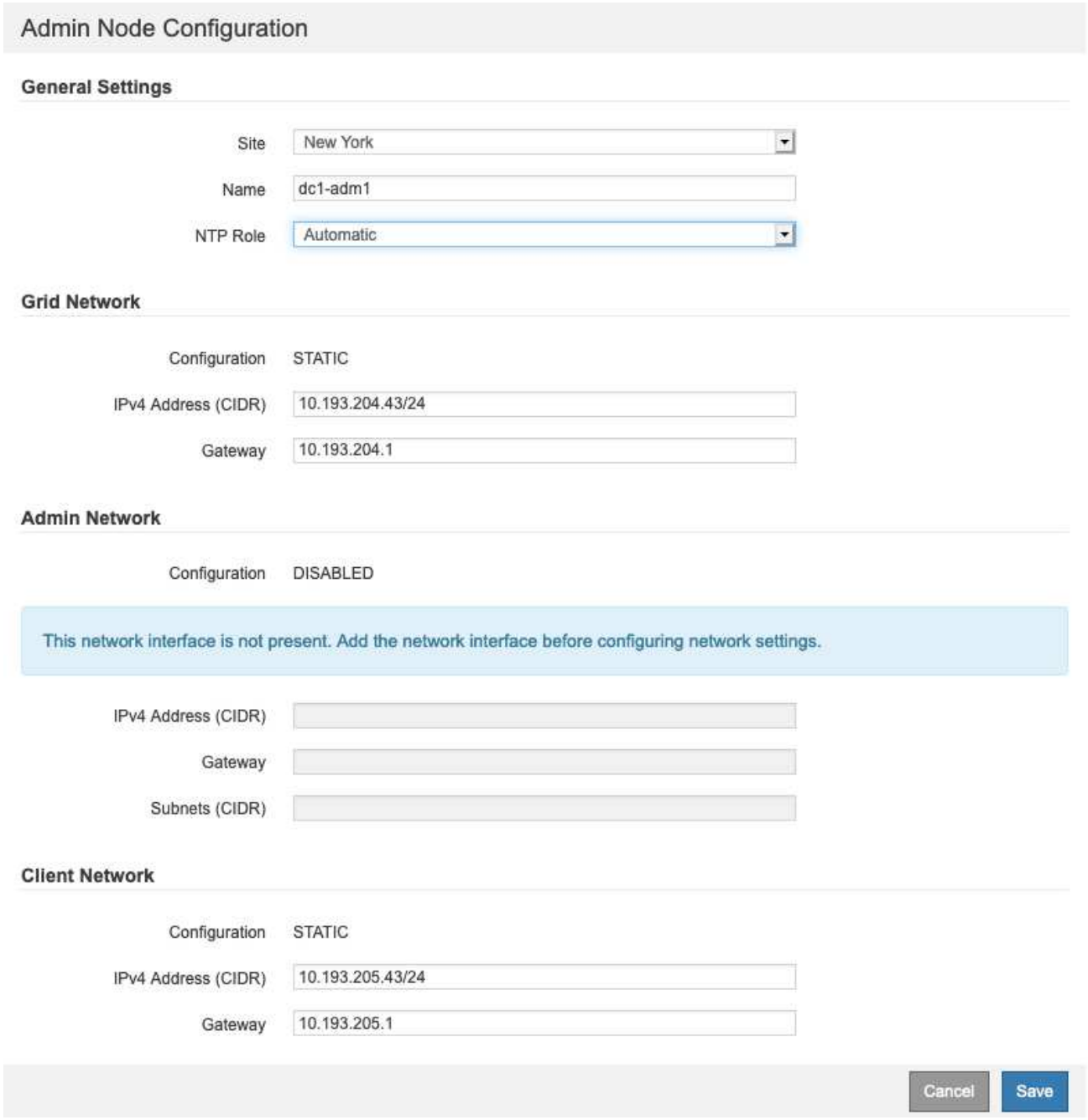
1. Consultez la liste nœuds en attente et vérifiez qu'elle affiche tous les nœuds de grille que vous avez déployés.

   Si un nœud de grid n'est pas inclus, vérifiez qu'il a été déployé correctement.

2. Cliquez sur le bouton radio en regard d'un nœud en attente que vous souhaitez approuver.



3. Cliquez sur approuver.
4. Dans Paramètres généraux, modifiez les paramètres des propriétés suivantes, si nécessaire.



— **site** : le nom système du site pour ce noeud de grille.

— **Nom** : le nom d'hôte qui sera affecté au nœud, et le nom qui sera affiché dans Grid Manager. Le nom par défaut est celui que vous avez spécifié lors du déploiement du nœud, mais vous pouvez le modifier en fonction de vos besoins.

— **NTP role** : le rôle NTP du nœud de grille. Les options sont automatique, principal et client. La sélection de l'option automatique affecte le rôle principal aux nœuds d'administration, aux nœuds de stockage avec des services ADC (administrative Domain Controller), aux nœuds de passerelle et à tous les nœuds de grille qui ont des adresses IP non statiques. Le rôle client est attribué à tous les autres nœuds de la grille.

Assurez-vous qu'au moins deux nœuds de chaque site peuvent accéder à au moins quatre sources NTP externes. Si un seul nœud d'un site peut atteindre les sources NTP, des problèmes de synchronisation surviennent en cas de panne de ce nœud. En outre, la désignation de deux nœuds par site en tant que sources NTP principales assure une

synchronisation précise si un site est isolé du reste de la grille.

— **Service ADC (noeuds de stockage uniquement)** : sélectionnez automatique pour permettre au système de déterminer si le noeud nécessite le service ADC. Le service ADC conserve le suivi de l'emplacement et de la disponibilité des services de réseau. Au moins trois nœuds de stockage sur chaque site doivent inclure le service ADC. Vous ne pouvez pas ajouter le service ADC à un nœud après son déploiement.

5. Dans réseau Grid, modifiez les paramètres des propriétés suivantes si nécessaire :

— **adresse IPv4 (CIDR)** : adresse réseau CIDR de l'interface réseau de la grille (eth0 à l'intérieur du conteneur). Par exemple `192.168.1.234/24`, .

— **passerelle** : la passerelle réseau de la grille. Par exemple `192.168.0.1`, .

S'il existe plusieurs sous-réseaux de grille, la passerelle est requise.

Si vous avez sélectionné DHCP pour la configuration réseau de la grille et que vous modifiez la valeur ici, la nouvelle valeur est configurée comme une adresse statique sur le nœud. Assurez-vous que l'adresse IP résultante ne se trouve pas dans un pool d'adresses DHCP.

6. Pour configurer le réseau d'administration pour le nœud de grille, ajoutez ou mettez à jour les paramètres de la section réseau d'administration si nécessaire.

Entrez les sous-réseaux de destination des routes de cette interface dans la zone de texte Subnet (CIDR). S'il existe plusieurs sous-réseaux d'administration, la passerelle d'administration est requise.

Si vous avez sélectionné DHCP pour la configuration réseau d'administration et que vous modifiez la valeur ici, la nouvelle valeur est configurée comme une adresse statique sur le nœud. Assurez-vous que l'adresse IP résultante ne se trouve pas dans un pool d'adresses DHCP.

Appareils : pour une appliance StorageGRID, si le réseau d'administration n'a pas été configuré lors de l'installation initiale à l'aide du programme d'installation de l'appliance StorageGRID, il ne peut pas être configuré dans cette boîte de dialogue Gestionnaire de grille. Au lieu de cela, vous devez procéder comme suit :

a. Redémarrez l'appliance : dans le programme d'installation de l'appliance, sélectionnez **Avancé › redémarrer**. Le redémarrage peut prendre plusieurs minutes.
b. Sélectionnez **configurer la mise en réseau › Configuration de la liaison** et activez les réseaux appropriés.
c. Sélectionnez **configurer la mise en réseau › Configuration IP** et configurez les réseaux activés.
d. Revenez à la page d'accueil et cliquez sur Démarrer l'installation.
e. Dans Grid Manager : si le nœud est répertorié dans le tableau nœuds approuvés, réinitialisez-le.
f. Supprimez le nœud du tableau nœuds en attente.
g. Attendez que le nœud réapparaisse dans la liste nœuds en attente.
h. Confirmez que vous pouvez configurer les réseaux appropriés. Elles doivent déjà contenir les informations que vous avez fournies sur la page de configuration IP. Pour plus d'informations, reportez-

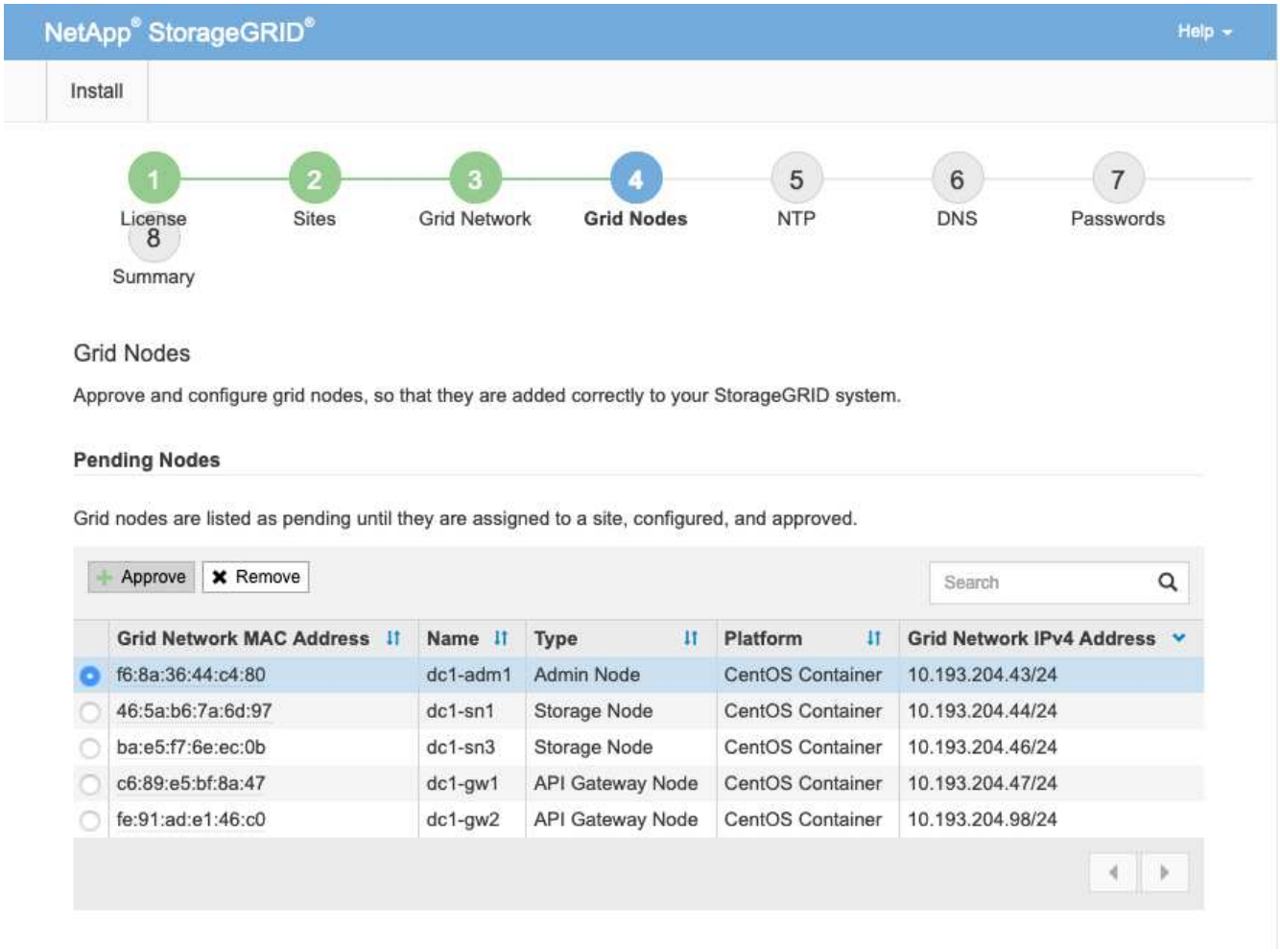
vous aux instructions d'installation et d'entretien de votre modèle d'appareil.

7. Si vous souhaitez configurer le réseau client pour le nœud de grille, ajoutez ou mettez à jour les paramètres dans la section réseau client si nécessaire. Si le réseau client est configuré, la passerelle est requise et devient la passerelle par défaut du noeud après l'installation.

   Appareils : pour une appliance StorageGRID, si le réseau client n'a pas été configuré lors de l'installation initiale à l'aide du programme d'installation de l'appliance StorageGRID, il ne peut pas être configuré dans cette boîte de dialogue Gestionnaire de grille. Au lieu de cela, vous devez procéder comme suit :

   a. Redémarrez l'appliance : dans le programme d'installation de l'appliance, sélectionnez **Avancé › redémarrer**. Le redémarrage peut prendre plusieurs minutes.
   b. Sélectionnez **configurer la mise en réseau › Configuration de la liaison** et activez les réseaux appropriés.
   c. Sélectionnez **configurer la mise en réseau › Configuration IP** et configurez les réseaux activés.
   d. Revenez à la page d'accueil et cliquez sur Démarrer l'installation.
   e. Dans Grid Manager : si le nœud est répertorié dans le tableau nœuds approuvés, réinitialisez-le.
   f. Supprimez le nœud du tableau nœuds en attente.
   g. Attendez que le nœud réapparaisse dans la liste nœuds en attente.
   h. Confirmez que vous pouvez configurer les réseaux appropriés. Elles doivent déjà contenir les informations que vous avez fournies sur la page de configuration IP. Pour plus d'informations, reportez-vous aux instructions d'installation et de maintenance de votre appareil.

8. Cliquez sur Enregistrer. L'entrée de nœud de la grille passe à la liste nœuds approuvés.



9. Répétez les étapes 1 à 1-8 pour chaque nœud de grille en attente que vous souhaitez approuver.

   Vous devez approuver tous les nœuds que vous souhaitez dans la grille. Cependant, vous pouvez revenir à cette page à tout moment avant de cliquer sur installer sur la page Résumé. Pour modifier les propriétés d'un nœud de grille approuvé, cliquez sur son bouton radio, puis cliquez sur Modifier.

10. Lorsque vous avez fini d'approuver les nœuds de la grille, cliquez sur Suivant.

Spécifiez les détails du serveur NTP pour StorageGRID

Découvrez comment spécifier les informations de configuration NTP de votre système StorageGRID afin que les opérations effectuées sur des serveurs distincts puissent être synchronisées.

Pour éviter les problèmes de décalage horaire, vous devez spécifier quatre références de serveur NTP externe de Stratum 3 ou supérieur.

> 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. Sur les versions antérieures de Windows, le service horaire n'est pas suffisamment précis et n'est pas pris en charge par Microsoft pour une utilisation dans des environnements exigeants tels que StorageGRID.

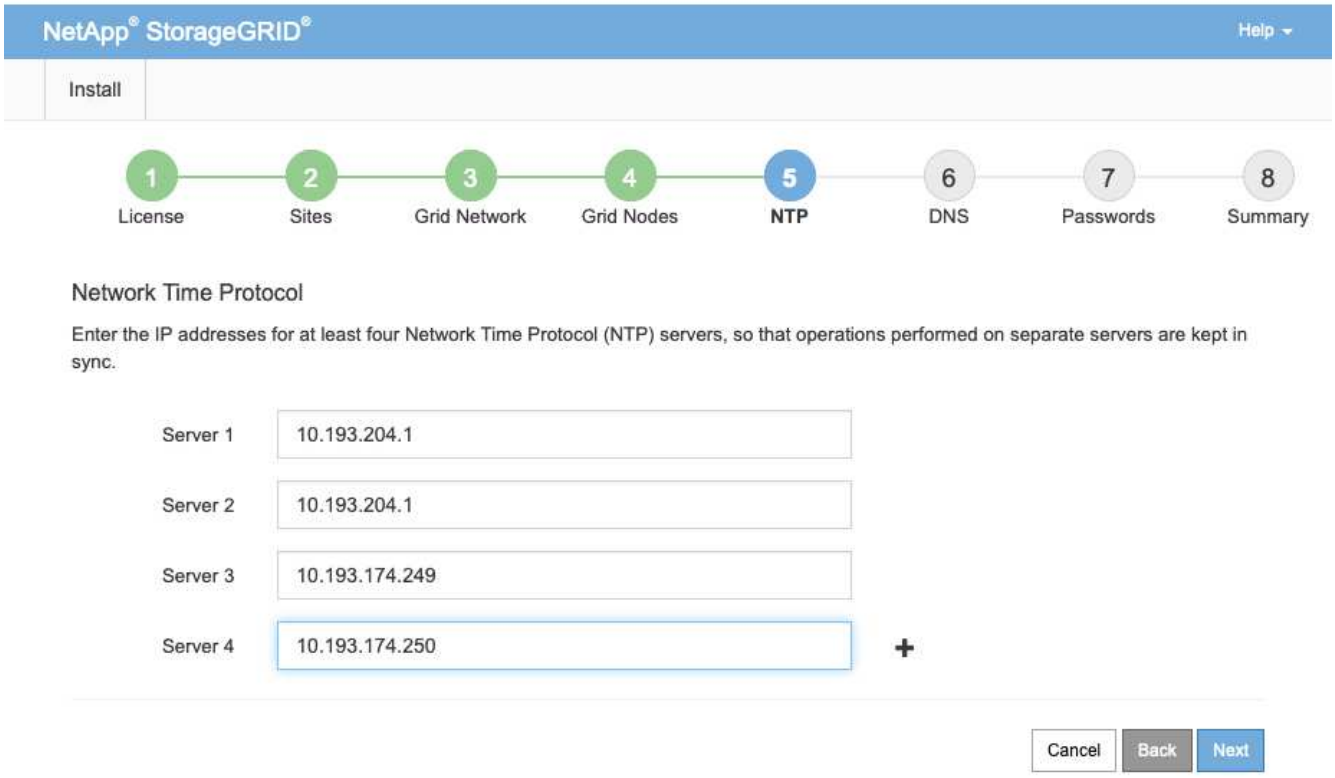
Les serveurs NTP externes sont utilisés par les nœuds auxquels vous avez précédemment attribué les rôles NTP principaux.

> Le réseau client n'est pas activé suffisamment tôt dans le processus d'installation pour être la seule source de serveurs NTP. Assurez-vous qu'au moins un serveur NTP peut être atteint sur le réseau de grille ou le réseau d'administration.

Pour spécifier les informations du serveur NTP, procédez comme suit :

Étapes

1. Dans les zones de texte serveur 1 à serveur 4, spécifiez les adresses IP d'au moins quatre serveurs NTP.
2. Si nécessaire, cliquez sur le signe plus en regard de la dernière entrée pour ajouter d'autres entrées de serveur.



3. Cliquez sur Suivant.

Spécifiez les détails du serveur DNS pour StorageGRID

Découvrez comment configurer le serveur DNS pour StorageGRID.

Vous devez spécifier les informations DNS de votre système StorageGRID pour pouvoir accéder aux serveurs externes en utilisant des noms d'hôte au lieu d'adresses IP.

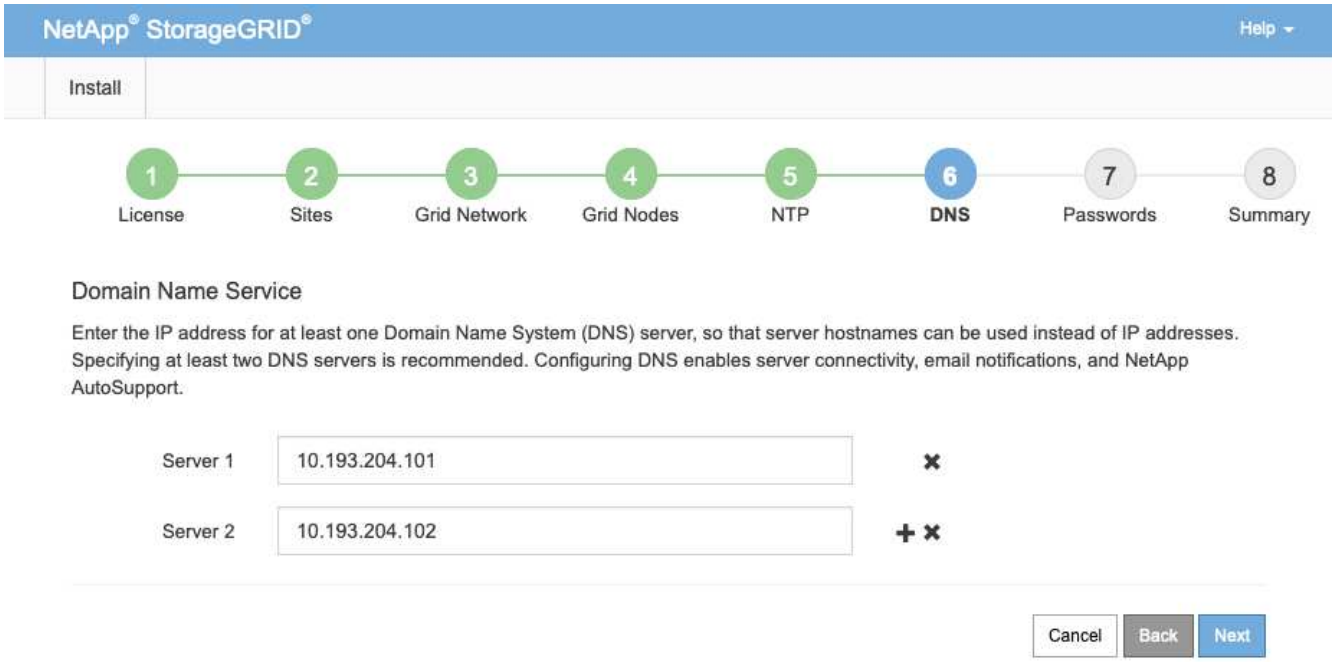
La spécification des informations du serveur DNS vous permet d'utiliser des noms d'hôte de nom de domaine complet (FQDN) plutôt que des adresses IP pour les notifications par e-mail et les messages NetApp AutoSupport®. NetApp recommande de spécifier au moins deux serveurs DNS.

Vous devez sélectionner des serveurs DNS auxquels chaque site peut accéder localement en cas d'isatterissage du réseau.

Pour spécifier des informations sur le serveur DNS, procédez comme suit :

Étapes

1. Dans la zone de texte serveur 1, spécifiez l'adresse IP d'un serveur DNS.
2. Si nécessaire, cliquez sur le signe plus en regard de la dernière entrée pour ajouter d'autres serveurs.



3. Cliquez sur Suivant.

Spécifiez les mots de passe système pour StorageGRID

Découvrez comment sécuriser votre système StorageGRID en définissant la phrase de passe de provisioning et le mot de passe utilisateur root de gestion de grille.

Pour saisir les mots de passe à utiliser pour sécuriser votre système StorageGRID, procédez comme suit :

Étapes

1. Dans Provisioning Passphrase (phrase de passe de provisionnement), saisissez la phrase de passe de provisionnement qui sera requise pour modifier la topologie de la grille de votre système StorageGRID. Vous devez enregistrer ce mot de passe en lieu sûr.
2. Dans confirmer la phrase de passe de provisionnement, saisissez à nouveau la phrase de passe de provisionnement.
3. Dans le champ Grid Management Root User Password, entrez le mot de passe à utiliser pour accéder à Grid Manager en tant qu'utilisateur root.
4. Dans confirmer le mot de passe de l'utilisateur racine, entrez à nouveau le mot de passe du gestionnaire de grille.

5. Si vous installez une grille à des fins de démonstration de faisabilité ou de démonstration, désélectionnez l'option Créer des mots de passe de ligne de commande aléatoires.

   Pour les déploiements en production, des mots de passe aléatoires doivent toujours être utilisés pour des raisons de sécurité. Désélectionnez l'option Créer des mots de passe de ligne de commande aléatoires uniquement pour les grilles de démonstration si vous souhaitez utiliser des mots de passe par défaut pour accéder aux nœuds de grille à partir de la ligne de commande à l'aide du compte root ou admin.

   > Lorsque vous cliquez sur installer dans la page Résumé , vous êtes invité à télécharger le fichier du progiciel de récupération (`sgws-recovery-packageid-revision.zip`. Vous devez télécharger ce fichier pour terminer l'installation. Les mots de passe permettant d'accéder au système sont stockés dans le `Passwords.txt` fichier, contenu dans le fichier du progiciel de récupération.

6. Cliquez sur Suivant.

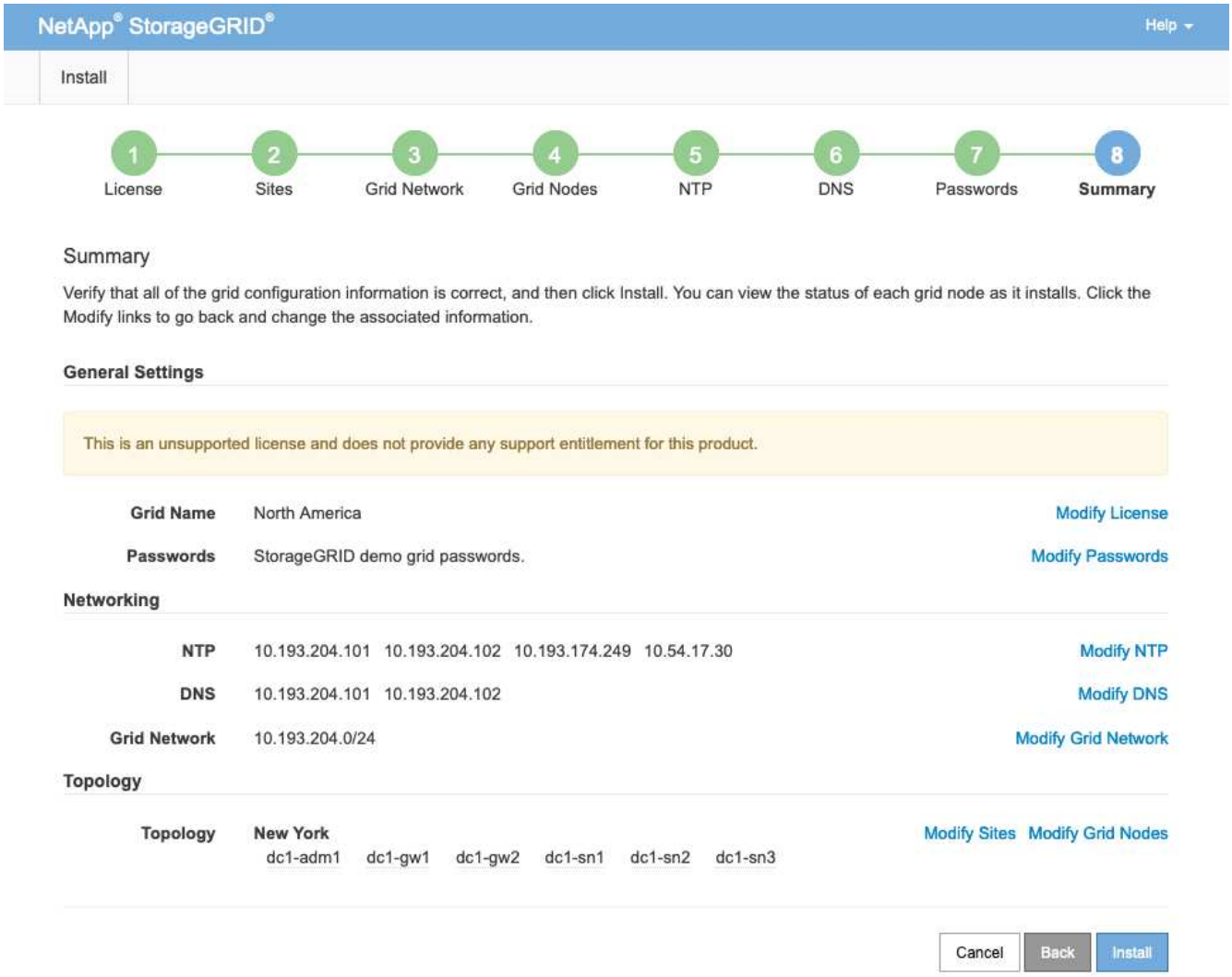
Vérifiez la configuration et terminez l'installation de StorageGRID

Découvrez comment valider les informations de configuration du grid et terminer le processus d'installation de StorageGRID.

Pour vous assurer que l'installation se termine correctement, lisez attentivement les informations de configuration que vous avez saisies. Effectuez la procédure suivante.

Étapes

1. Afficher la page Résumé.



2. Vérifiez que toutes les informations de configuration de la grille sont correctes. Utilisez les liens Modifier de la page Résumé pour revenir en arrière et corriger les erreurs.
3. Cliquez sur installation.

> Si un nœud est configuré pour utiliser le réseau client, la passerelle par défaut de ce nœud passe du réseau grid au réseau client lorsque vous cliquez sur installer. En cas de perte de connectivité, assurez-vous que vous accédez au nœud d'administration principal via un sous-réseau accessible. Pour plus d'informations, reportez-vous à la section « installation et provisionnement réseau ».

4. Cliquez sur Télécharger le pack de récupération.

   Lorsque l'installation progresse jusqu'au point où la topologie de la grille est définie, vous êtes invité à télécharger le fichier du progiciel de récupération (`.zip`) et à confirmer que vous pouvez accéder au contenu de ce fichier. Vous devez télécharger le fichier du package de récupération pour pouvoir récupérer le système StorageGRID en cas de défaillance d'un ou plusieurs nœuds de grille.

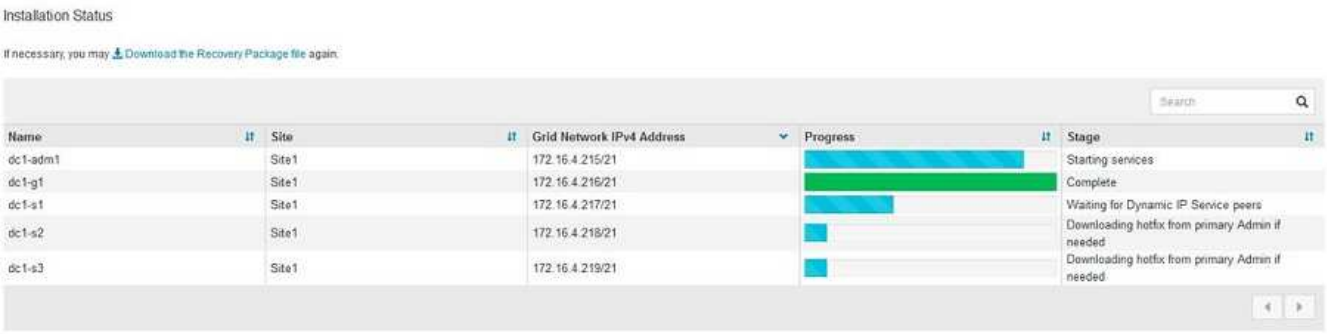
   Vérifiez que vous pouvez extraire le contenu du `.zip` fichier, puis l'enregistrer dans deux emplacements sécurisés et séparés.

> Le fichier du progiciel de récupération doit être sécurisé car il contient des clés de cryptage

et des mots de passe qui peuvent être utilisés pour obtenir des données du système StorageGRID.

5. Sélectionnez l'option J'ai téléchargé et vérifié le fichier de package de récupération, puis cliquez sur Suivant.

Si l'installation est toujours en cours, la page État de l'installation s'ouvre. Cette page indique la progression de l'installation pour chaque nœud de la grille.



Lorsque l'étape complète est atteinte pour tous les nœuds de grille, la page de connexion de Grid Manager s'ouvre.

6. Connectez-vous à Grid Manager en tant qu'utilisateur root avec le mot de passe que vous avez spécifié lors de l'installation.

Mettez à niveau les nœuds bare-Metal dans StorageGRID

En savoir plus sur le processus de mise à niveau des nœuds bare-Metal dans StorageGRID.

Le processus de mise à niveau des nœuds bare-Metal est différent de celui des appliances et des nœuds VMware. Avant d'effectuer une mise à niveau d'un nœud bare-Metal, vous devez d'abord mettre à niveau les fichiers RPM sur tous les hôtes avant d'exécuter la mise à niveau via l'interface graphique.

```
[root@host1 rpms]# rpm -Uvh StorageGRID-Webscale-Images-*.rpm
[root@host1 rpms]# rpm -Uvh StorageGRID-Webscale-Service-*.rpm
```

Vous pouvez maintenant procéder à la mise à niveau du logiciel via l'interface graphique.

Tr-4907 : configurer StorageGRID avec veritas Enterprise Vault

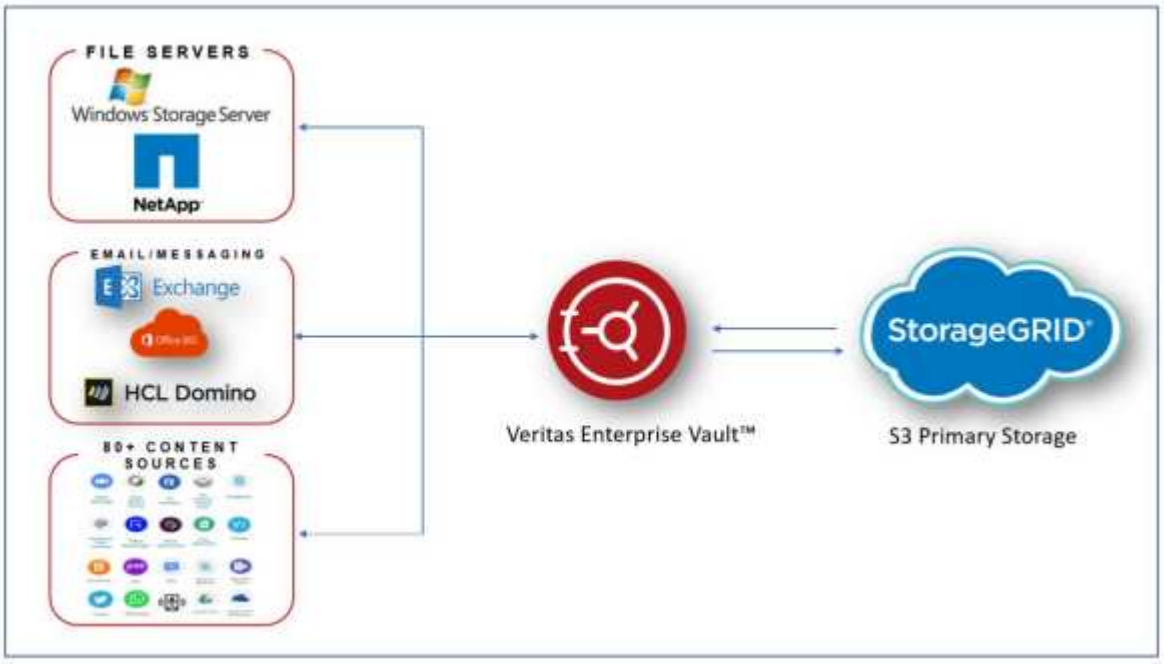
Introduction à la configuration de StorageGRID pour le basculement de site

Découvrez comment veritas Enterprise Vault utilise StorageGRID comme cible de stockage primaire pour la reprise après incident.

Ce guide de configuration fournit les étapes de configuration de NetApp® StorageGRID® en tant que cible de stockage principale avec veritas Enterprise Vault. Elle décrit également comment configurer StorageGRID pour un basculement de site dans un scénario de reprise d'activité.

Architecture de référence

StorageGRID fournit une cible de sauvegarde dans le cloud sur site compatible avec S3 pour veritas Enterprise Vault. La figure suivante illustre l'architecture de veritas Enterprise Vault et StorageGRID.



Où trouver des informations complémentaires

Pour en savoir plus sur les informations données dans ce livre blanc, consultez ces documents et/ou sites web :

- Centre de documentation NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-118/
- Accompagnement NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-enable/

- Documentation des produits NetApp https://www.netapp.com/support-and-training/documentation/

Configurer StorageGRID et veritas Enterprise Vault

Découvrez comment implémenter des configurations de base pour StorageGRID 11.5 ou version ultérieure et veritas Enterprise Vault 14.1 ou version ultérieure.

Ce guide de configuration est basé sur StorageGRID 11.5 et Enterprise Vault 14.1. Pour le stockage en mode WORM (Write Once, Read Many) avec le verrouillage des objets S3, StorageGRID 11.6 et Enterprise Vault 14.2.2 ont été utilisés. Pour plus d'informations sur ces instructions, rendez-vous sur la "Documentation StorageGRID" page ou contactez un expert StorageGRID.

Conditions requises pour configurer StorageGRID et veritas Enterprise Vault

- Avant de configurer StorageGRID avec veritas Enterprise Vault, vérifiez les conditions préalables suivantes :

> Pour le stockage WORM (verrouillage objet), StorageGRID 11.6 ou version supérieure est requis.

- veritas Enterprise Vault 14.1 ou version ultérieure est installé.

> Pour le stockage WORM (Object Lock), Enterprise Vault version 14.2.2 ou supérieure est requis.

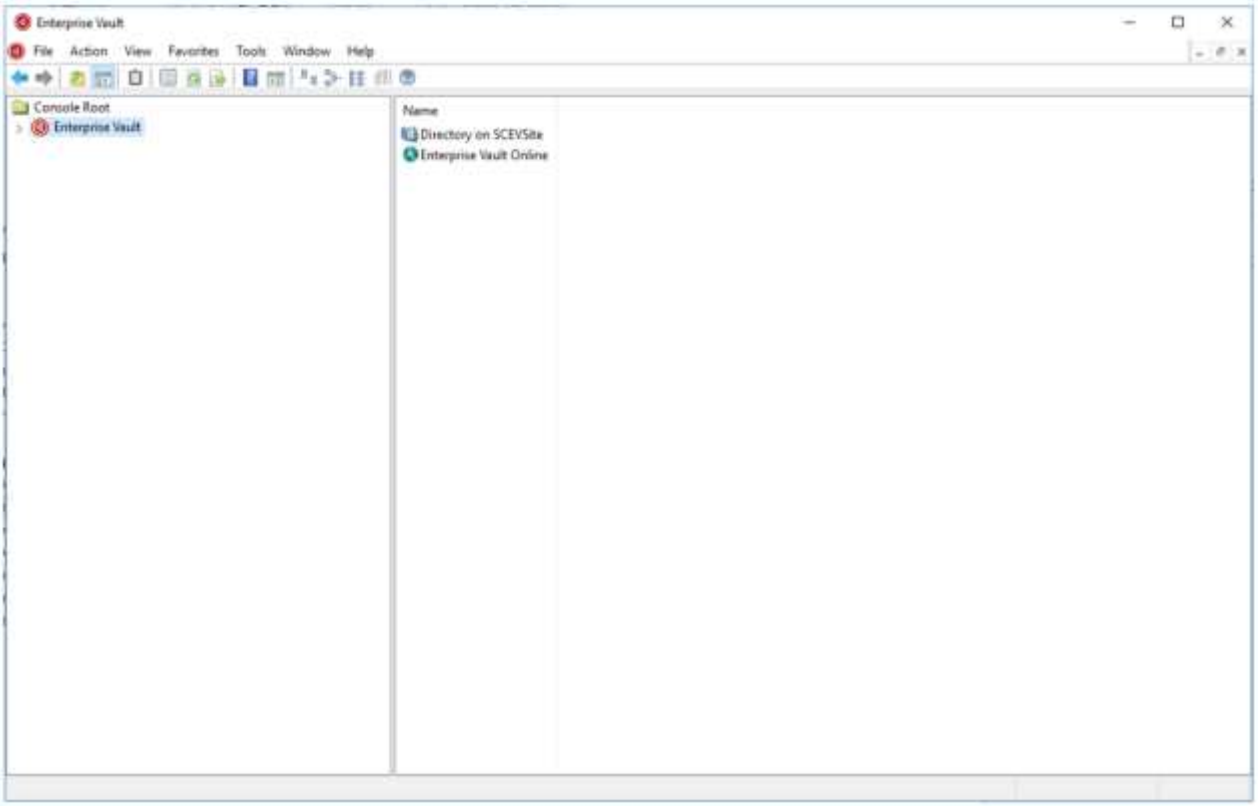
- Des groupes de magasins de coffre-fort et un magasin de coffre-fort ont été créés. Pour plus d'informations, reportez-vous au Guide d'administration de veritas Enterprise Vault.
- Un locataire StorageGRID, une clé d'accès, une clé secrète et un compartiment ont été créés.
- Un noeud final de l'équilibreur de charge StorageGRID a été créé (HTTP ou HTTPS).
- Si vous utilisez un certificat auto-signé, ajoutez le certificat d'autorité de certification auto-signé de StorageGRID aux serveurs Enterprise Vault. Pour plus d'informations, consultez ce "Article de la base de connaissances veritas".
- Mettez à jour et appliquez le dernier fichier de configuration Enterprise Vault pour activer les solutions de stockage prises en charge, telles que NetApp StorageGRID. Pour plus d'informations, consultez ce document "Article de la base de connaissances veritas".

Configurez StorageGRID avec veritas Enterprise Vault

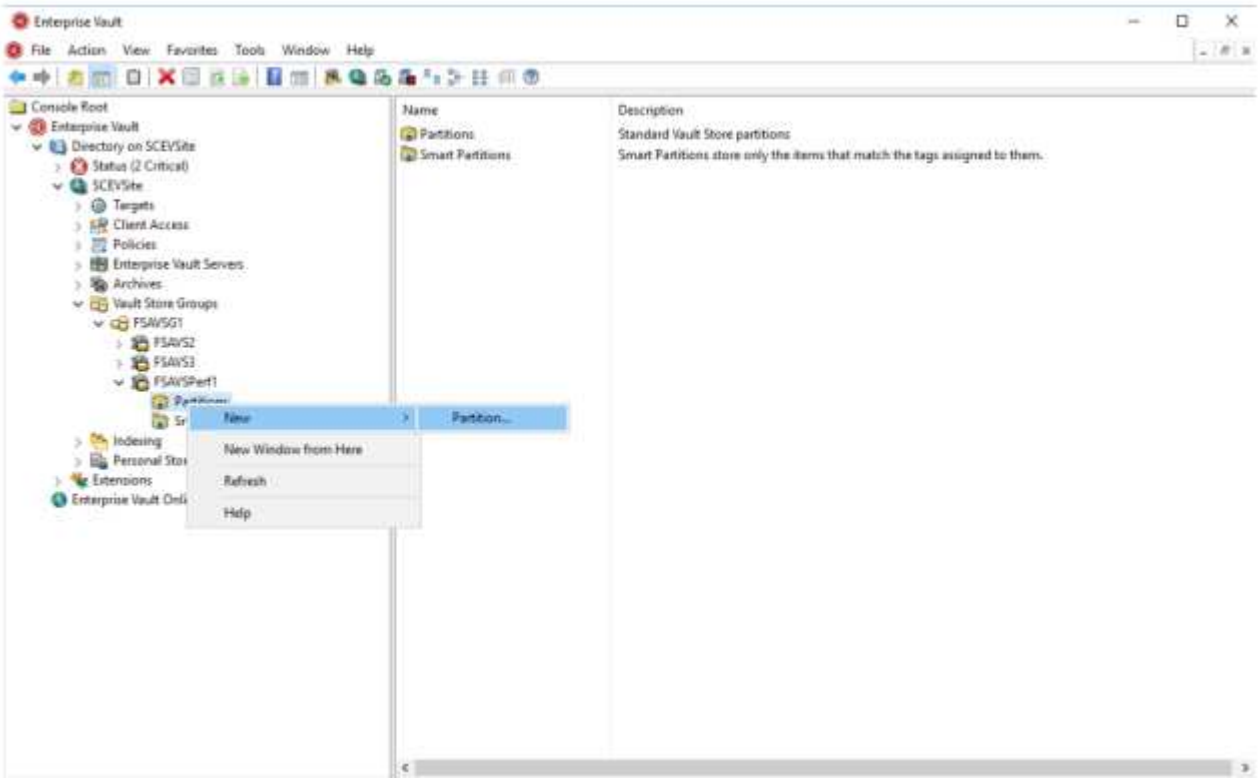
Pour configurer StorageGRID avec veritas Enterprise Vault, procédez comme suit :

Étapes

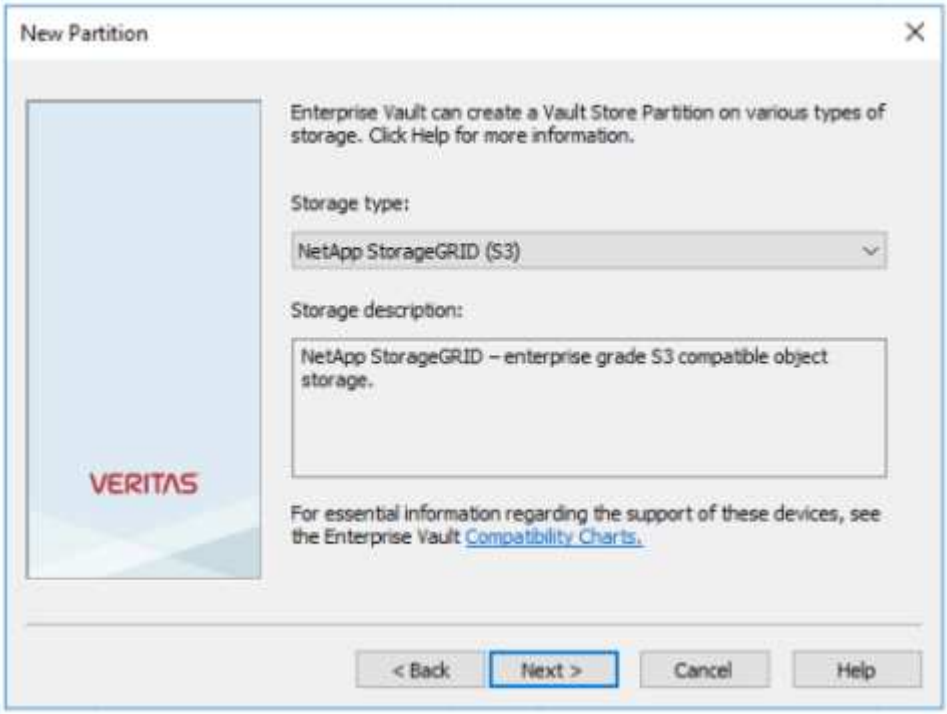
1. Lancez la console Enterprise Vault Administration.



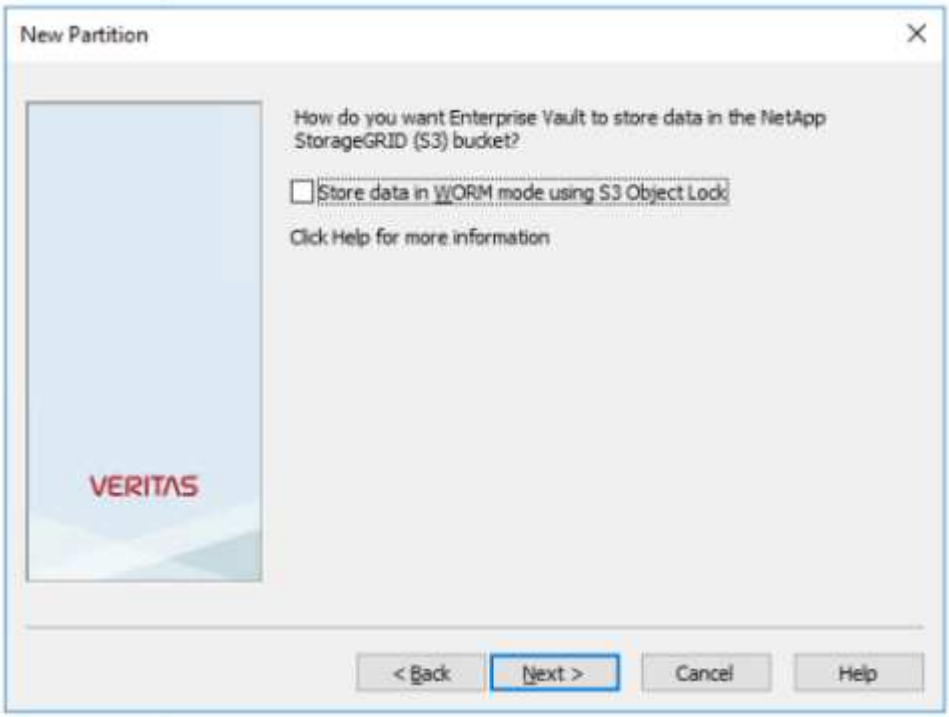
2. Créez une nouvelle partition de magasin de coffre-fort dans le magasin de coffre-fort approprié. Développez le dossier groupes du magasin Vault, puis le magasin de coffre-fort approprié. Cliquez avec le bouton droit de la souris sur partition et sélectionnez **New › partition**.



3. Suivez l’assistant de création de nouvelle partition. Dans le menu déroulant Type de stockage, sélectionnez NetApp StorageGRID (S3). Cliquez sur Suivant.

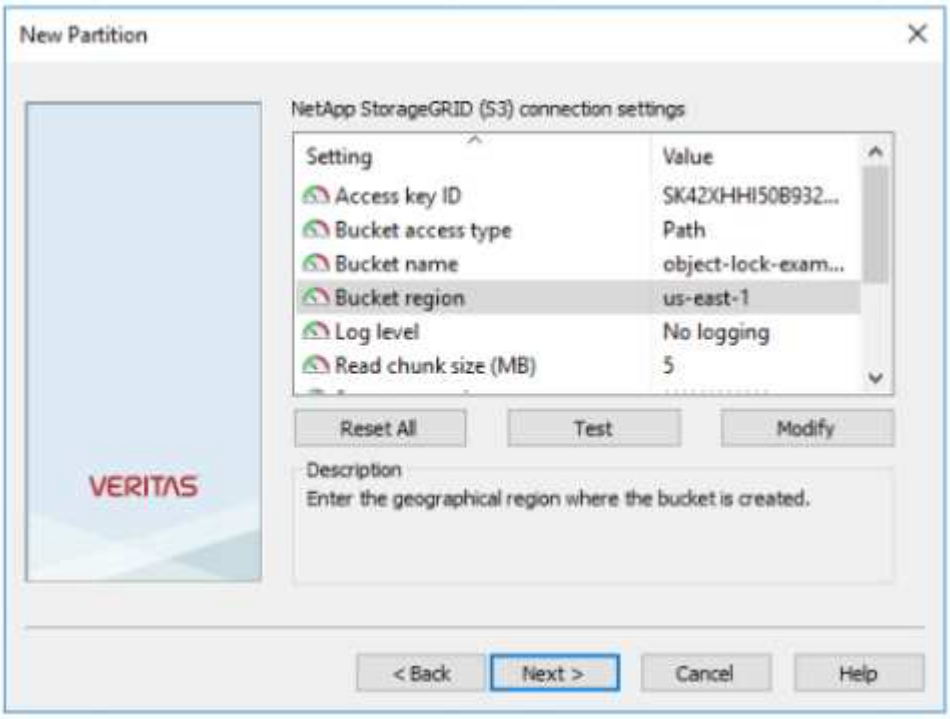


4. Ne cochez pas l'option stocker les données en mode WORM à l'aide du verrouillage d'objet S3. Cliquez sur Suivant.

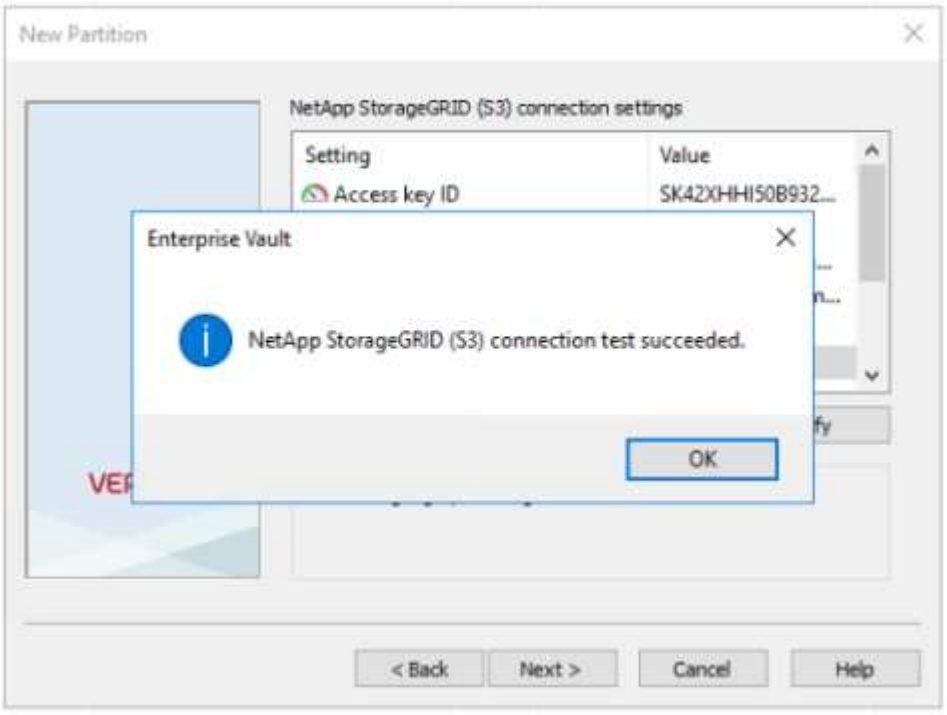


5. Sur la page des paramètres de connexion, fournissez les informations suivantes :
   - ID de clé d'accès
   - Clé d'accès secrète
   - Nom d'hôte du service : assurez-vous d'inclure le port LBE (load balancer Endpoint) configuré dans StorageGRID (tel que https://<hostname>:<LBE_port>)

- Nom du compartiment : nom du compartiment cible précréé. veritas Enterprise Vault ne crée pas le compartiment.
- Région du compartiment : `us-east-1` est la valeur par défaut.

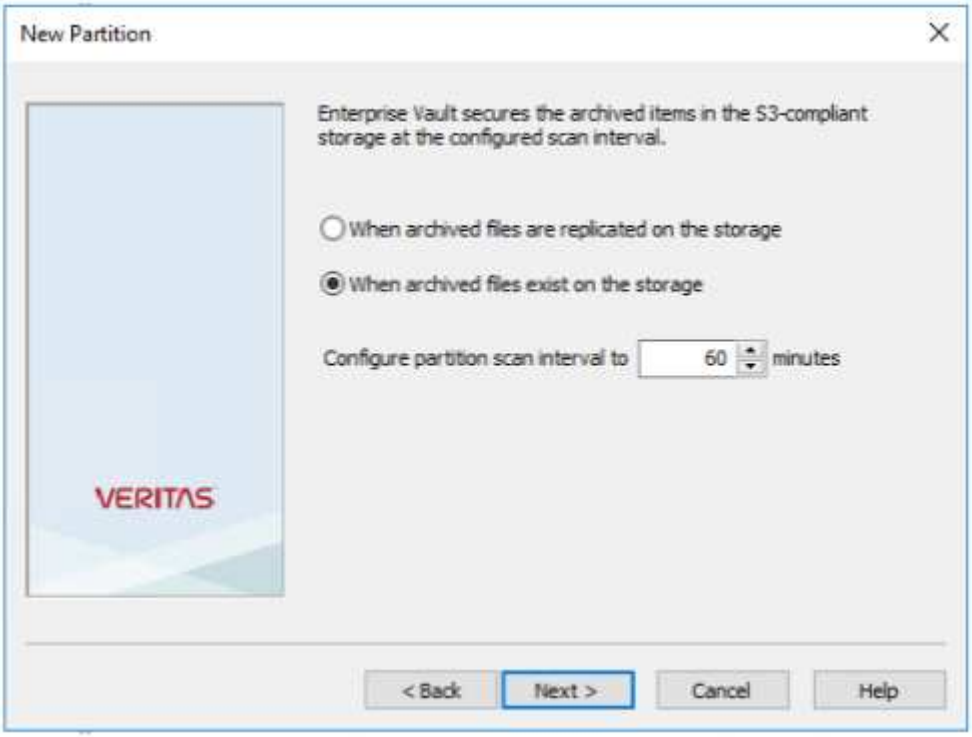


6. Pour vérifier la connexion au compartiment StorageGRID, cliquez sur Test. Vérifiez que le test de connexion a réussi. Cliquez sur OK, puis sur Suivant.

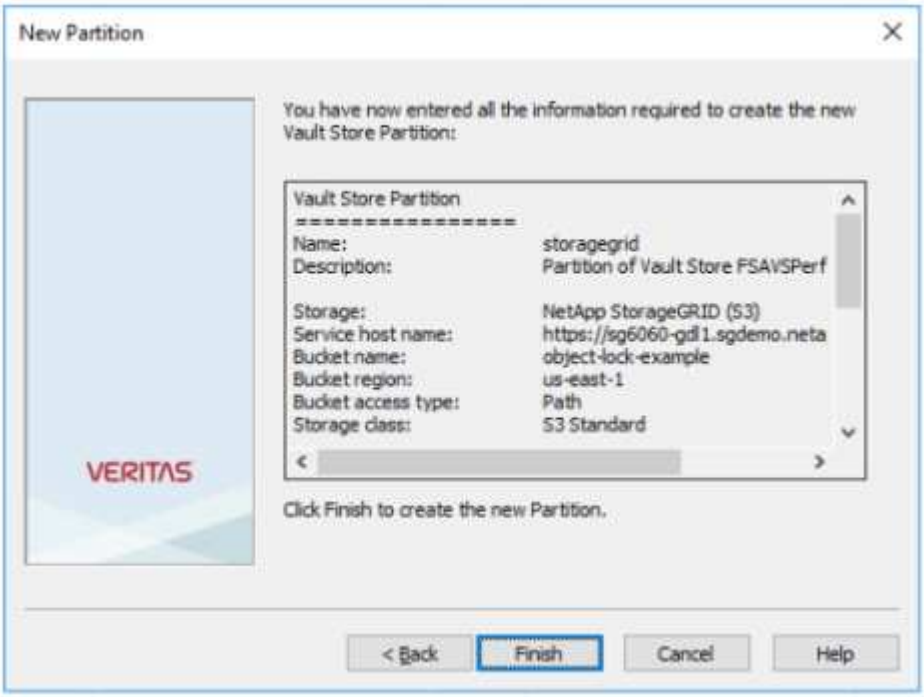


7. StorageGRID ne prend pas en charge le paramètre de réplication S3. Pour protéger vos objets, StorageGRID utilise des règles de gestion du cycle de vie des informations (ILM) afin de spécifier des schémas de protection des données : copies multiples ou code d'effacement. Sélectionnez l'option lorsque

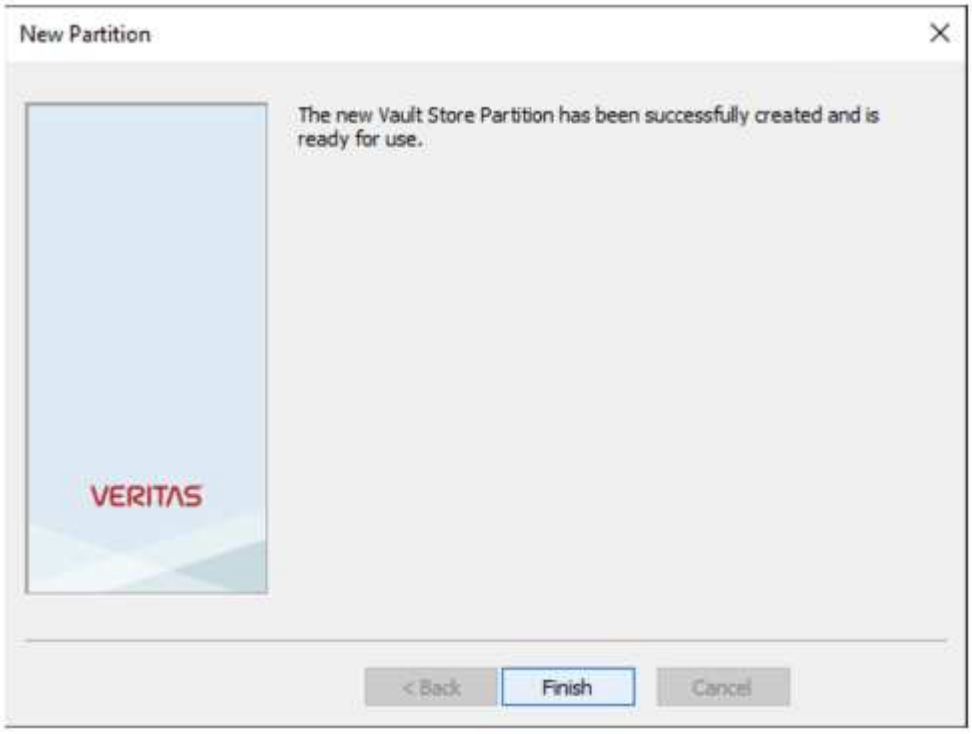
des fichiers archivés existent dans le stockage et cliquez sur Suivant.



8. Vérifiez les informations sur la page de résumé et cliquez sur Terminer.



9. Une fois la nouvelle partition de magasin de coffre-fort créée, vous pouvez archiver, restaurer et rechercher des données dans le coffre-fort d'entreprise avec StorageGRID comme stockage principal.



Configuration du verrouillage objet StorageGRID S3 pour le stockage WORM

Découvrez comment configurer StorageGRID pour le stockage WORM à l'aide du verrouillage objet S3.

Conditions préalables à la configuration de StorageGRID pour le stockage WORM

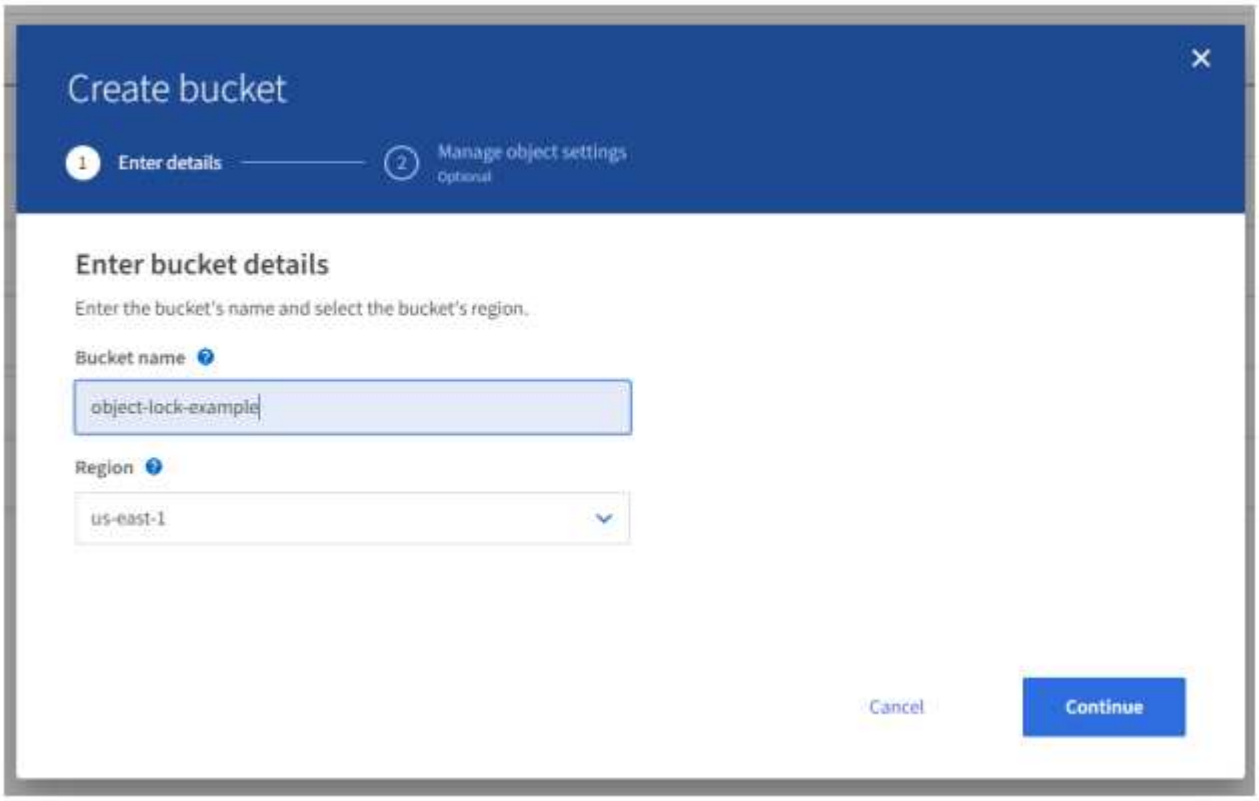
Pour le stockage WORM, StorageGRID utilise le verrouillage objet S3 pour conserver les objets à des fins de conformité. Ceci requiert StorageGRID 11.6 ou version supérieure, où une fonctionnalité de conservation par défaut des compartiments du verrouillage objet S3 a été ajoutée. Enterprise Vault requiert également la version 14.2.2 ou supérieure.

Configuration de la rétention des compartiments par défaut du verrouillage objet StorageGRID S3

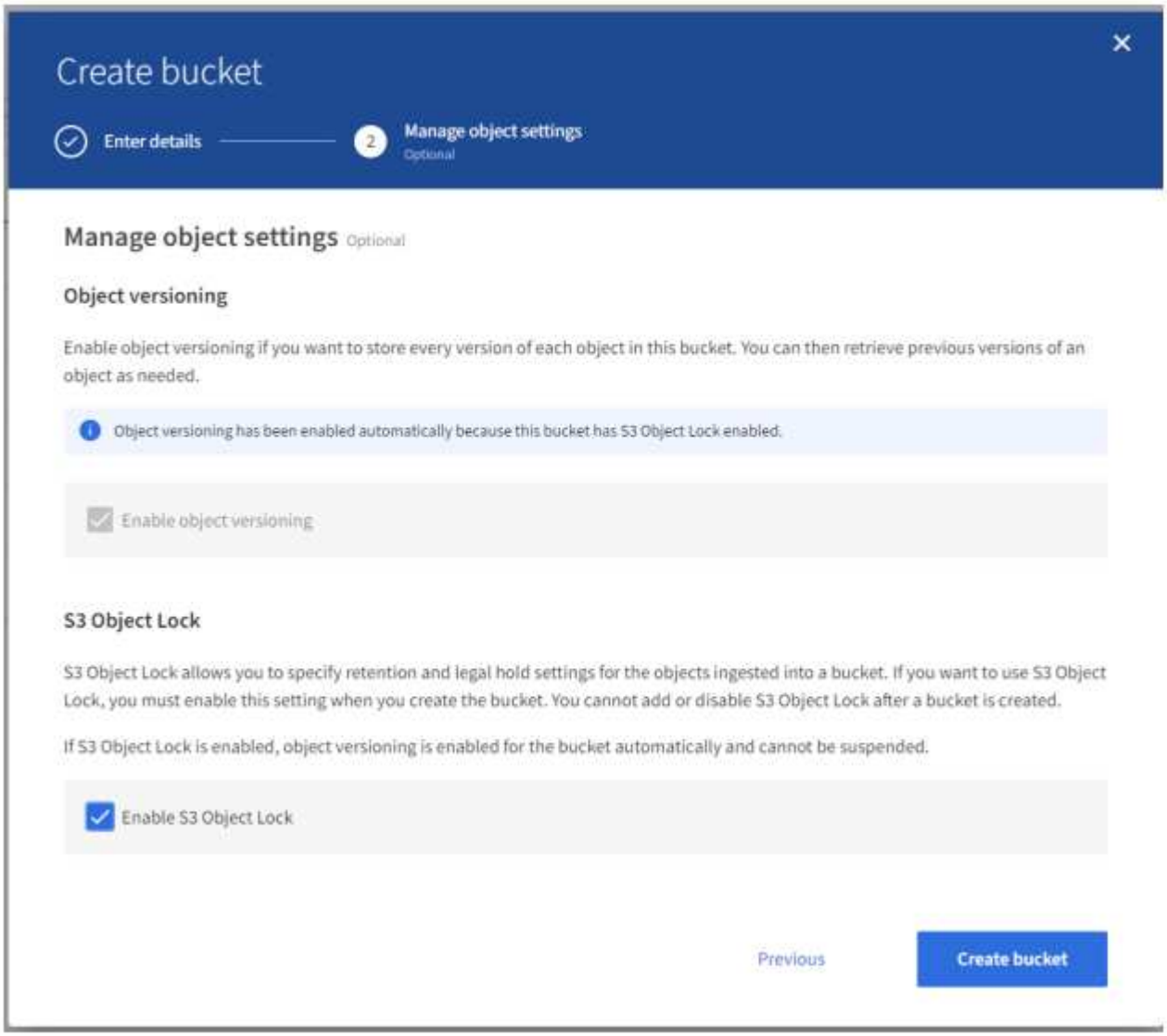
Pour configurer la rétention des compartiments par défaut du verrouillage objet StorageGRID S3, effectuez les opérations suivantes :

Étapes

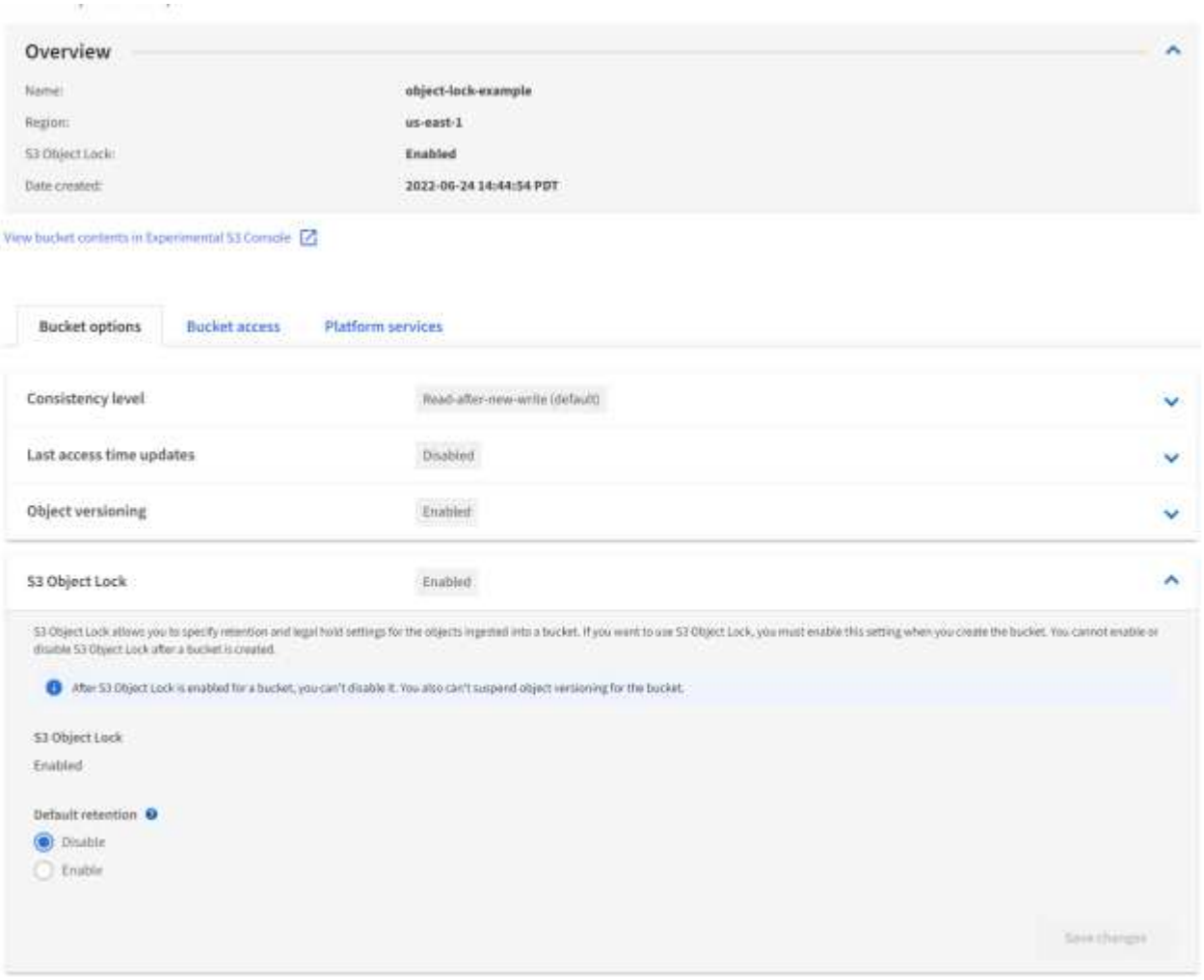
1. Dans le gestionnaire de locataires StorageGRID, créez un compartiment et cliquez sur Continuer



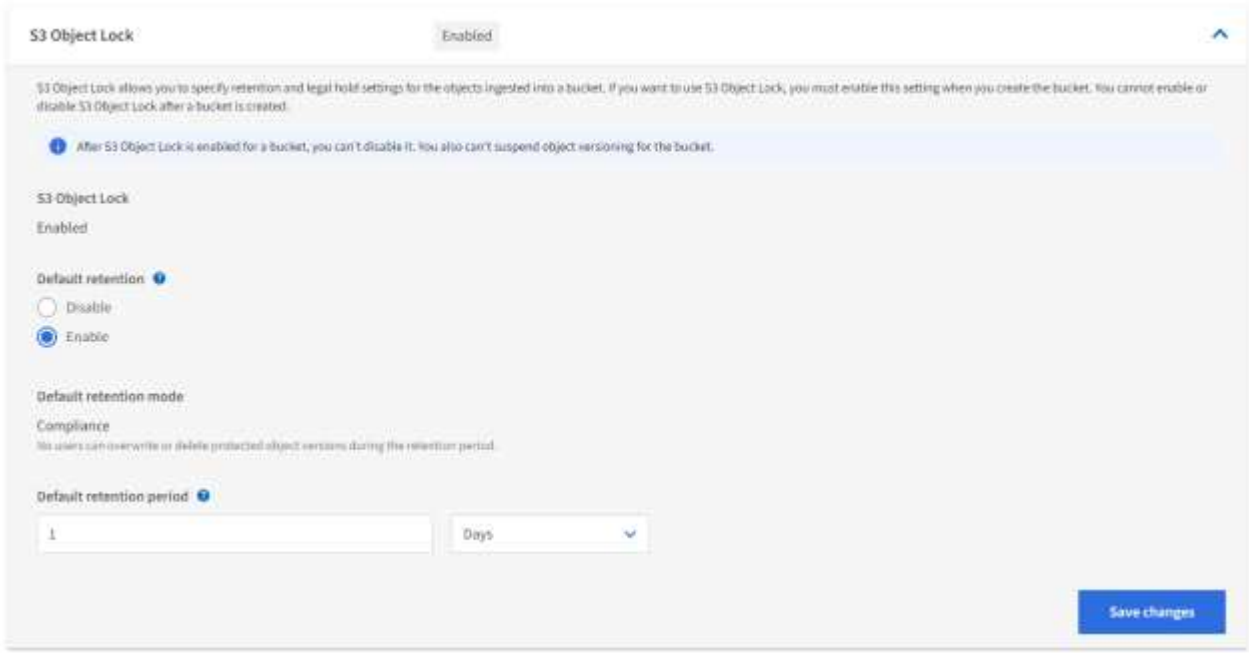
2. Sélectionnez l’option Activer le verrouillage d’objet S3 et cliquez sur Créer un compartiment.



3. Une fois le godet créé, sélectionner le godet pour afficher les options de compartiment. Développez l'option de liste déroulante verrouillage objet S3.



4. Sous conservation par défaut, sélectionnez Activer et définissez une période de conservation par défaut de 1 jour. Cliquez sur Save Changes.



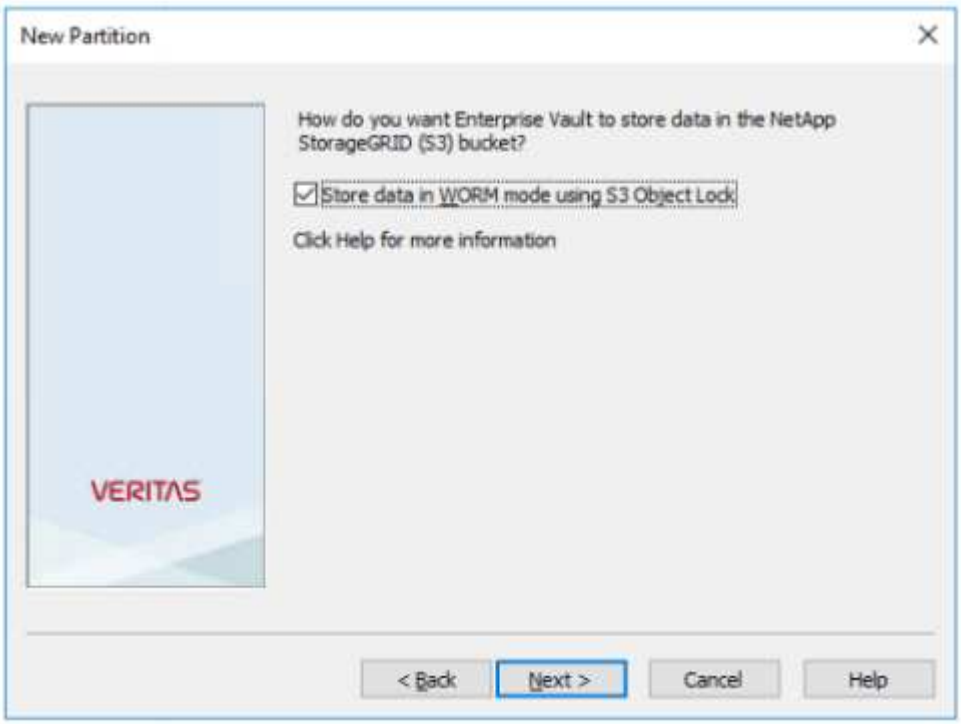
Le compartiment est désormais prêt à être utilisé par Enterprise Vault pour stocker les données WORM.

Configurer Enterprise Vault

Pour configurer Enterprise Vault, procédez comme suit :

Étapes

1. Répétez les étapes 1 à 3 dans la section "Configuration de base", mais cette fois, sélectionnez l'option Stocker les données en mode WORM à l'aide du verrouillage d'objet S3. Cliquez sur Suivant.



2. Lorsque vous entrez vos paramètres de connexion du compartiment S3, assurez-vous d'entrer le nom d'un compartiment S3 pour lequel la conservation par défaut du verrouillage objet S3 est activée.
3. Testez la connexion pour vérifier les paramètres.

Configurez le basculement de site StorageGRID pour la reprise après incident

Découvrez comment configurer le basculement de site StorageGRID dans un scénario de reprise d'activité.

Il est courant que le déploiement d'une architecture StorageGRID soit multisite. Les sites peuvent être de type actif-actif ou actif-passif pour la reprise après incident. En cas de reprise après incident, assurez-vous que veritas Enterprise Vault peut maintenir la connexion à son stockage primaire (StorageGRID) et continuer à ingérer et à récupérer les données en cas de panne sur un site. Cette section fournit des conseils de configuration de haut niveau pour un déploiement actif-passif sur deux sites. Pour plus d'informations sur ces instructions, rendez-vous "Documentation StorageGRID" sur la page ou contactez un expert StorageGRID.

Conditions préalables à la configuration de StorageGRID avec veritas Enterprise Vault

Avant de configurer le basculement de site StorageGRID, vérifiez les conditions préalables suivantes :

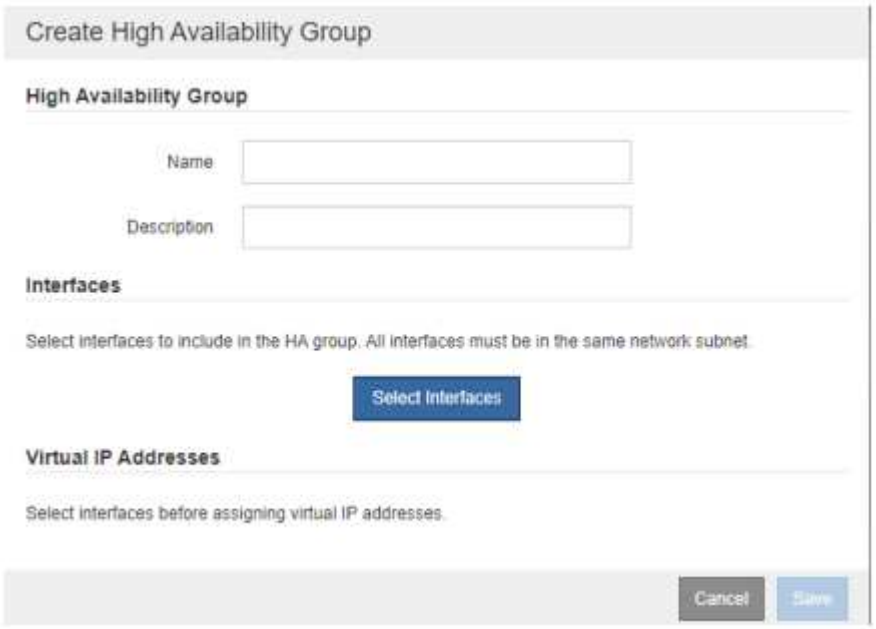
- Il existe un déploiement StorageGRID sur deux sites, par exemple, le SITE 1 et le SITE 2.
- Un nœud d'administration exécutant le service d'équilibrage de la charge ou un nœud de passerelle sur chaque site pour l'équilibrage de la charge a été créé.
- Un terminal de l'équilibreur de charge StorageGRID a été créé.

Configurer le basculement de site StorageGRID

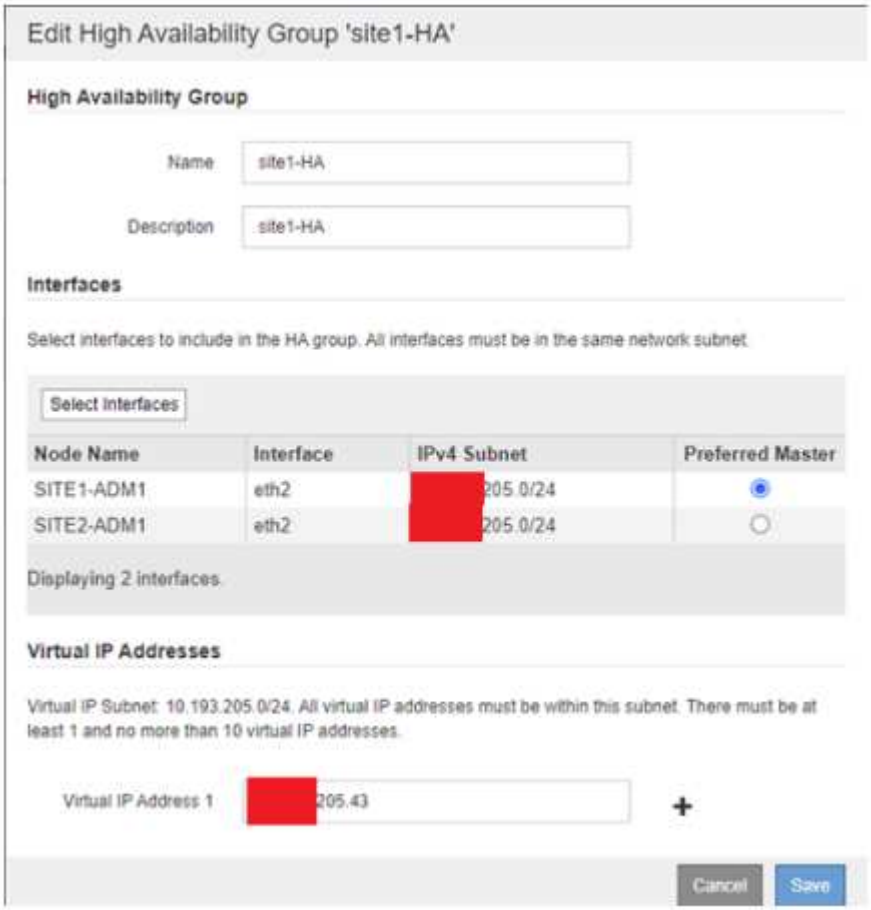
Pour configurer le basculement de site StorageGRID, procédez comme suit :

Étapes

1. Pour assurer la connectivité à StorageGRID en cas de défaillance d'un site, configurez un groupe haute disponibilité (HA). Dans l'interface GMI (StorageGRID Grid Manager interface), cliquez sur Configuration, groupes haute disponibilité, puis sur + Créer.



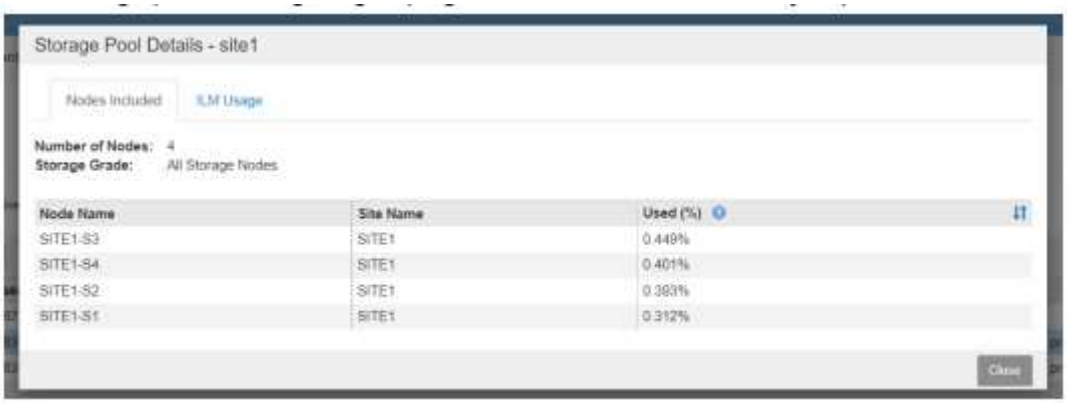
2. Entrez les informations requises. Cliquez sur Sélectionner les interfaces et incluez les interfaces réseau du SITE 1 et du SITE 2 où le site 1 (site principal) est le maître préféré. Attribuez une adresse IP virtuelle au sein du même sous-réseau. Cliquez sur Enregistrer.

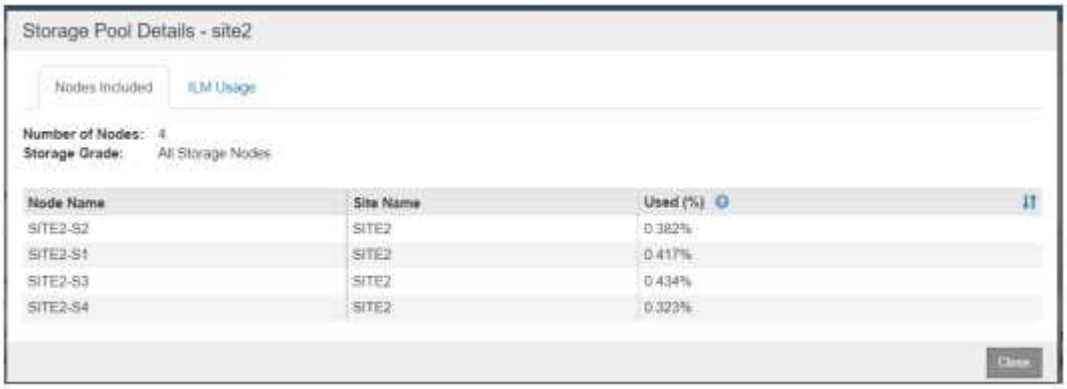


3. Cette adresse IP virtuelle (VIP) doit être associée au nom d'hôte S3 utilisé lors de la configuration de la partition de veritas Enterprise Vault. L'adresse VIP résout le trafic vers le SITE 1 et, en cas de défaillance du SITE 1, l'adresse VIP réachemine le trafic vers le SITE 2 de manière transparente.
4. Assurez-vous que les données sont répliquées sur le SITE 1 et le SITE 2. Ainsi, si SITE1 échoue, les données de l'objet sont toujours disponibles à partir du SITE2. Pour ce faire, vous devez d'abord configurer les pools de stockage.

   Dans l'interface GMI de StorageGRID, cliquez sur ILM, pools de stockage, puis sur + Create. Suivez l'assistant pour créer deux pools de stockage : un pour le SITE 1 et un autre pour le SITE 2.

   Les pools de stockage sont des regroupements logiques de nœuds utilisés pour définir le placement des objets





5. Dans l'interface GMI de StorageGRID, cliquez sur ILM, Rules, puis sur + Create. Suivez les instructions de l'assistant pour créer une règle ILM spécifiant une copie à stocker par site avec un comportement d'ingestion équilibré.

6. Ajoutez la règle ILM à une règle ILM et activez cette règle.

Cette configuration entraîne les résultats suivants :

- IP de point de terminaison S3 virtuel où SITE1 est le point de terminaison principal et SITE2 le point de terminaison secondaire. Si LE SITE 1 échoue, le VIP bascule sur le SITE 2.
- Lorsque des données archivées sont envoyées depuis veritas Enterprise Vault, StorageGRID s'assure qu'une copie est stockée dans LE SITE 1 et qu'une autre copie de reprise après incident est stockée dans le SITE 2. Si SITE1 échoue, Enterprise Vault continue à ingérer et à récupérer depuis le SITE2.

> Ces deux configurations sont transparentes pour veritas Enterprise Vault. Le terminal S3, le nom de compartiment, les clés d'accès, etc. Sont identiques. Il n'est pas nécessaire de reconfigurer les paramètres de connexion S3 sur la partition veritas Enterprise Vault.

Informations sur le copyright

Copyright © 2026 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.