Guides d'utilisation et d'outils

StorageGRID solutions and resources

NetApp
October 12, 2026

This PDF was generated from https://docs.netapp.com/fr-fr/storagegrid-enable/tools-apps-guides/use-cloudera-hadoop-s3a-connector.html on October 12, 2026. Always check docs.netapp.com for the latest.

Sommaire

Guides d'utilisation et d'outils . . . 1
Utilisez le connecteur Cloudera Hadoop S3A avec StorageGRID . . . 1
Pourquoi utiliser S3A pour les flux de travail Hadoop ? . . . 1
Configurer le connecteur S3A pour utiliser StorageGRID . . . 1
Tester la connexion S3A à StorageGRID . . . 4
Utilisez S3cmd pour tester et démontrer l'accès S3 sur StorageGRID . . . 7
Installez et configurez S3cmd . . . 7
Étapes de configuration initiale . . . 7
Exemples de commandes de base . . . 7
Base de données en mode Vertica Eon utilisant NetApp StorageGRID comme stockage communautaire . . . 8
Introduction . . . 8
Recommandations de NetApp StorageGRID . . . 10
Installation du mode Eon sur site avec stockage communautaire sur StorageGRID . . . 11
Où trouver des informations complémentaires . . . 21
Historique des versions . . . 21
Analyse des journaux StorageGRID à l'aide de la pile ELK . . . 21
De formation . . . 21
Exemples de fichiers . . . 21
Hypothèse . . . 22
Instructions . . . 22
Ressources supplémentaires . . . 26
Grâce à Prometheus et Grafana, vous pouvez renforcer la conservation des metrics . . . 27
Introduction . . . 27
Fédérer Prometheus . . . 27
Installer et configurer Grafana . . . 36
Utilisez F5 DNS pour équilibrer la charge globale de StorageGRID. . . . 44
Introduction . . . 44
Configuration F5 BIG-IP StorageGRID multisite . . . 45
Conclusion . . . 60
Configuration SNMP Datalog . . . 61
Configurer Datalog . . . 61
Utilisez rclone pour migrer, DÉPLACER et SUPPRIMER des objets sur StorageGRID . . . 63
Installer et configurer rclone . . . 64
Exemples de commandes de base . . . 70
Bonnes pratiques de déploiement de StorageGRID avec Veeam Backup and Replication . . . 73
Présentation . . . 73
Configuration Veeam . . . 74
Configuration StorageGRID . . . 75
Points clés de la mise en œuvre . . . 78
Surveillance StorageGRID . . . 84
Où trouver des informations complémentaires . . . 86
Configurez la source de données Dremio avec StorageGRID . . . 86
Configurer la source de données Dremio . . . 86

Instructions . . . 87
NetApp StorageGRID avec GitLab . . . 89
Exemple de connexion de stockage objet . . . 89

Guides d’utilisation et d’outils

Utilisez le connecteur Cloudera Hadoop S3A avec StorageGRID

Par Angela Cheng

Hadoop est devenu l’un des préférés des data Scientists depuis un certain temps. Hadoop permet le traitement distribué d’importants jeux de données sur des clusters d’ordinateurs à l’aide d’infrastructures de programmation simples. Hadoop a été conçu pour évoluer verticalement de serveurs uniques à des milliers de machines, chaque machine étant en possession de ressources de calcul et de stockage locales.

Pourquoi utiliser S3A pour les flux de travail Hadoop ?

Comme le volume de données a augmenté au fil du temps, l’approche qui consiste à ajouter de nouveaux ordinateurs avec leurs propres ressources de calcul et de stockage est devenue inefficace. L’évolutivité linéaire engendre des défis pour utiliser les ressources efficacement et gérer l’infrastructure.

Pour relever ces challenges, le client Hadoop S3A propose 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. Qui dissocie le calcul et le stockage pour vous permettre de consacrer la quantité de ressources adaptée à vos tâches de calcul, et d’assurer la capacité en fonction de la taille de votre jeu de données. Par conséquent, vous pouvez réduire votre TCO global pour les workflows Hadoop.

Configurer le connecteur S3A pour utiliser StorageGRID

Prérequis

- Une URL de terminal StorageGRID S3, une clé d’accès s3 pour un locataire et une clé secrète pour le test de connexion à Hadoop S3A.
- Un cluster Cloudera ainsi que l’autorisation root ou sudo pour chaque hôte du cluster afin d’installer le package Java.

En avril 2022, Java 11.0.14 avec Cloudera 7.1.7 a été testé contre StorageGRID 11.5 et 11.6. Cependant, le numéro de version de Java peut être différent au moment d’une nouvelle installation.

Installez le package Java

1. Vérifiez la "Matrice de support Cloudera" pour la version JDK prise en charge.
2. Téléchargez le "Package Java 11.x" Correspondant au système d’exploitation du cluster Cloudera. Copiez ce package sur chaque hôte du cluster. Dans cet exemple, le progiciel rpm est utilisé pour CentOS.
3. Connectez-vous à chaque hôte en tant que root ou en utilisant un compte avec l’autorisation sudo. Effectuez les étapes suivantes sur chaque hôte :
   a. Installez le package :

```
$ sudo rpm -Uvh jdk-11.0.14_linux-x64_bin.rpm
```

b. Vérifiez l'emplacement d'installation de Java. Si plusieurs versions sont installées, définissez la nouvelle version installée par défaut :

```
alternatives --config java

There are 2 programs which provide 'java'.

  Selection    Command
-----------------------------------------------
 +1           /usr/java/jre1.8.0_291-amd64/bin/java
  2           /usr/java/jdk-11.0.14/bin/java

Enter to keep the current selection[+], or type selection number: 2
```

c. Ajoutez cette ligne à la fin de `/etc/profile`. Le chemin doit correspondre au chemin de la sélection ci-dessus :

```
export JAVA_HOME=/usr/java/jdk-11.0.14
```

d. Exécutez la commande suivante pour que le profil prenne effet :

```
source /etc/profile
```

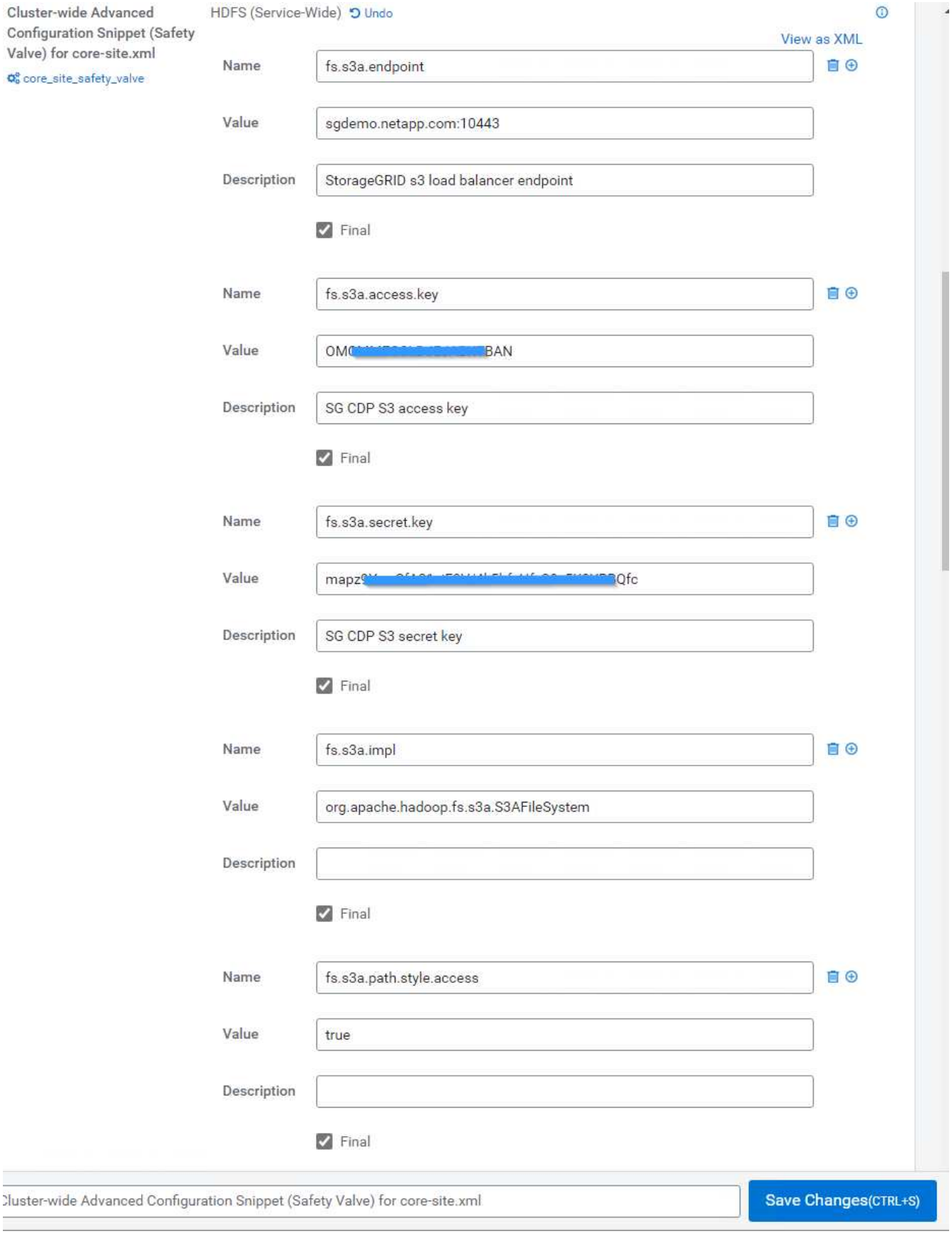
Configuration HDFS S3A de Cloudera

Étapes

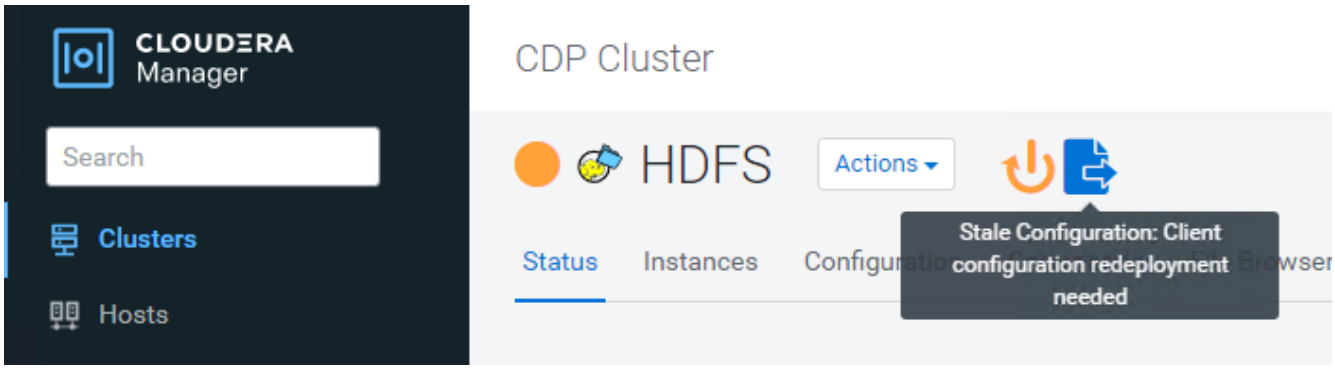
1. Dans l'interface graphique Cloudera Manager, sélectionnez clusters > HDFS et sélectionnez Configuration.
2. Sous CATÉGORIE, sélectionnez Avancé, puis faites défiler vers le bas pour rechercher `Cluster-wide Advanced Configuration Snippet (Safety Valve) for core-site.xml`.
3. Cliquez sur le signe (+) et ajoutez les paires de valeurs suivantes.

Nom	Valeur
fs.s3a.access.key	*<clé d'accès s3 de StorageGRID>*
fs.s3a.secret.key	*<clé secrète S3 du locataire StorageGRID>*
fs.s3a.connection.ssl.enabled	[vrai ou faux] (la valeur par défaut est https si cette entrée est manquante)
fs.s3a.endpoint	*<noeud final StorageGRID S3:port>*
fs.s3a.impl	ORG.apache.hadoop.fs.s3a.S3AFileSystem
fs.s3a.path.style.access	[vrai ou faux] (le style d'hôte virtuel par défaut est défini si cette entrée est manquante)

Exemple de capture d'écran



4. Cliquez sur le bouton Enregistrer les modifications. Sélectionnez l'icône Configuration obsolète dans la barre de menus HDFS, sélectionnez redémarrer les services obsolètes sur la page suivante, puis sélectionnez redémarrer maintenant.



Tester la connexion S3A à StorageGRID

Effectuer un test de connexion de base

Connectez-vous à l'un des hôtes du cluster Cloudera, puis entrez `hadoop fs -ls s3a://<bucket-name>/`.

L'exemple suivant utilise le chemin syle avec un compartiment hdfs-test pré-existant et un objet test.

```
[root@ce-n1 ~]# hadoop fs -ls s3a://hdfs-test/
22/02/15 18:24:37 WARN impl.MetricsConfig: Cannot locate configuration:
tried hadoop-metrics2-s3a-file-system.properties,hadoop-
metrics2.properties
22/02/15 18:24:37 INFO impl.MetricsSystemImpl: Scheduled Metric snapshot
period at 10 second(s).
22/02/15 18:24:37 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system started
22/02/15 18:24:37 INFO Configuration.deprecation: No unit for
fs.s3a.connection.request.timeout(0) assuming SECONDS
Found 1 items
-rw-rw-rw-   1 root root       1679 2022-02-14 16:03 s3a://hdfs-test/test
22/02/15 18:24:38 INFO impl.MetricsSystemImpl: Stopping s3a-file-system
metrics system...
22/02/15 18:24:38 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system stopped.
22/02/15 18:24:38 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system shutdown complete.
```

Dépannage

Scénario 1

Utilisez une connexion HTTPS à StorageGRID et obtenez un `handshake_failure` erreur après un délai de 15 minutes.

Raison : ancienne version JRE/JDK utilisant la suite de chiffrement TLS obsolète ou non prise en charge pour la connexion à StorageGRID.

Exemple de message d'erreur

```
[root@ce-n1 ~]# hadoop fs -ls s3a://hdfs-test/
22/02/15 18:52:34 WARN impl.MetricsConfig: Cannot locate configuration:
tried hadoop-metrics2-s3a-file-system.properties,hadoop-
metrics2.properties
22/02/15 18:52:34 INFO impl.MetricsSystemImpl: Scheduled Metric snapshot
period at 10 second(s).
22/02/15 18:52:34 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system started
22/02/15 18:52:35 INFO Configuration.deprecation: No unit for
fs.s3a.connection.request.timeout(0) assuming SECONDS
22/02/15 19:04:51 INFO impl.MetricsSystemImpl: Stopping s3a-file-system
metrics system...
22/02/15 19:04:51 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system stopped.
22/02/15 19:04:51 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system shutdown complete.
22/02/15 19:04:51 WARN fs.FileSystem: Failed to initialize fileystem
s3a://hdfs-test/: org.apache.hadoop.fs.s3a.AWSClientIOException:
doesBucketExistV2 on hdfs: com.amazonaws.SdkClientException: Unable to
execute HTTP request: Received fatal alert: handshake_failure: Unable to
execute HTTP request: Received fatal alert: handshake_failure
ls: doesBucketExistV2 on hdfs: com.amazonaws.SdkClientException: Unable to
execute HTTP request: Received fatal alert: handshake_failure: Unable to
execute HTTP request: Received fatal alert: handshake_failure
```

Résolution : Assurez-vous que JDK 11.x ou version ultérieure est installé et défini par défaut la bibliothèque Java. Reportez-vous à la Installez le package Java pour plus d'informations.

Scénario 2 :

Impossible de se connecter à StorageGRID avec message d'erreur `Unable to find valid certification path to requested target.`

Raison: le certificat du serveur de noeuds finaux StorageGRID S3 n'est pas approuvé par le programme Java.

Exemple de message d'erreur :

```
[root@hdp6 ~]# hadoop fs -ls s3a://hdfs-test/
22/03/11 20:58:12 WARN impl.MetricsConfig: Cannot locate configuration:
tried hadoop-metrics2-s3a-file-system.properties,hadoop-
metrics2.properties
22/03/11 20:58:13 INFO impl.MetricsSystemImpl: Scheduled Metric snapshot
period at 10 second(s).
22/03/11 20:58:13 INFO impl.MetricsSystemImpl: s3a-file-system metrics
```

```
system started
22/03/11 20:58:13 INFO Configuration.deprecation: No unit for
fs.s3a.connection.request.timeout(0) assuming SECONDS
22/03/11 21:12:25 INFO impl.MetricsSystemImpl: Stopping s3a-file-system
metrics system...
22/03/11 21:12:25 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system stopped.
22/03/11 21:12:25 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system shutdown complete.
22/03/11 21:12:25 WARN fs.FileSystem: Failed to initialize fileystem
s3a://hdfs-test/: org.apache.hadoop.fs.s3a.AWSClientIOException:
doesBucketExistV2 on hdfs: com.amazonaws.SdkClientException: Unable to
execute HTTP request: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find
valid certification path to requested target: Unable to execute HTTP
request: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find
valid certification path to requested target
```

Resolution: NetApp recommande d'utiliser un certificat de serveur délivré par une autorité de signature de certificat public connu pour s'assurer que l'authentification est sécurisée. Vous pouvez également ajouter un certificat d'autorité de certification ou de serveur personnalisé au magasin de confiance Java.

Procédez comme suit pour ajouter une autorité de certification ou un certificat de serveur personnalisé StorageGRID au magasin d'approbation Java.

1. Sauvegardez le fichier Java cacerts existant par défaut.

```
cp -ap $JAVA_HOME/lib/security/cacerts
$JAVA_HOME/lib/security/cacerts.orig
```

2. Importez le certificat de noeud final StorageGRID S3 dans le magasin de confiance Java.

```
keytool -import -trustcacerts -keystore $JAVA_HOME/lib/security/cacerts
-storepass changeit -noprompt -alias sg-lb -file <StorageGRID CA or
server cert in pem format>
```

Conseils de dépannage

1. Augmentez le niveau de journalisation hadoop pour DÉBOGUER.

```
export HADOOP_ROOT_LOGGER=hadoop.root.logger=DEBUG,console
```

2. Exécutez la commande et dirigez les messages du journal vers error.log.

```
hadoop fs -ls s3a://<bucket-name>/ &>error.log
```

Par Angela Cheng

Utilisez S3cmd pour tester et démontrer l'accès S3 sur StorageGRID

Par Aron Klein

S3cmd est un outil de ligne de commande gratuit et un client pour les opérations S3. Vous pouvez utiliser s3cmd pour tester et démontrer l'accès s3 avec StorageGRID.

Installez et configurez S3cmd

Pour installer S3cmd sur un poste de travail ou un serveur, téléchargez-le à partir de "Client S3 en ligne de commande". S3cmd est préinstallé sur chaque nœud StorageGRID comme outil pour faciliter le dépannage.

Étapes de configuration initiale

1. s3cmd --configure
2. Fournissez uniquement Access_Key et secret_key, pour le reste conservez les valeurs par défaut.
3. Tester l'accès avec les informations d'identification fournies ? [O/n] : n (ignorer le test car il échouera)
4. Enregistrer les paramètres ? [o/N] y
   a. Configuration enregistrée dans '/root/.s3cfg'
5. Dans les champs .s3cfg, rendre vide Host_base et Host_bucket après le signe "=" :
   a. host_base =
   b. host_bucket =

Si vous spécifiez Host_base et Host_bucket à l'étape 4, il n'est pas nécessaire de spécifier un noeud final avec --host dans la CLI. Exemple :

```
host_base = 192.168.1.91:8082
host_bucket = bucketX.192.168.1.91:8082
s3cmd ls s3://bucketX --no-check-certificate
```

Exemples de commandes de base

- **Créer un compartiment :**

```
s3cmd mb s3://s3cmdbucket --host=<endpoint>:<port> --no-check-certificate
```

- **Liste de tous les compartiments:**

```
s3cmd ls --host=<endpoint>:<port> --no-check-certificate
```

- **Liste de tous les compartiments et de leur contenu:**

```
s3cmd la --host=<endpoint>:<port> --no-check-certificate
```

- **Liste des objets dans un compartiment spécifique :**

```
s3cmd ls s3://<bucket> --host=<endpoint>:<port> --no-check-certificate
```

- **Supprimer un compartiment :**

```
s3cmd rb s3://s3cmdbucket --host=<endpoint>:<port> --no-check-certificate
```

- **Mettre un objet:**

```
s3cmd put <file> s3://<bucket> --host=<endpoint>:<port> --no-check-certificate
```

- **Obtenir un objet:**

```
s3cmd get s3://<bucket>/<object> <file> --host=<endpoint>:<port> --no-check
-certificate
```

- **Supprimer un objet:**

```
s3cmd del s3://<bucket>/<object> --host=<endpoint>:<port> --no-check
-certificate
```

Base de données en mode Vertica Eon utilisant NetApp StorageGRID comme stockage communautaire

Par Angela Cheng

Ce guide décrit la procédure de création d'une base de données Vertica Eon mode avec stockage communautaire sur NetApp StorageGRID.

Introduction

Vertica est un logiciel de gestion de base de données analytique. C'est une plateforme de stockage orientée colonnes conçue pour gérer d'importants volumes de données, permettant ainsi des performances d'interrogation très rapides dans un scénario très intensif. Une base de données Vertica s'exécute dans l'un des deux modes suivants : EON ou Enterprise. Vous pouvez déployer les deux modes sur site ou dans le cloud.

Les modes EON et Enterprise diffèrent principalement lorsqu'ils stockent des données :

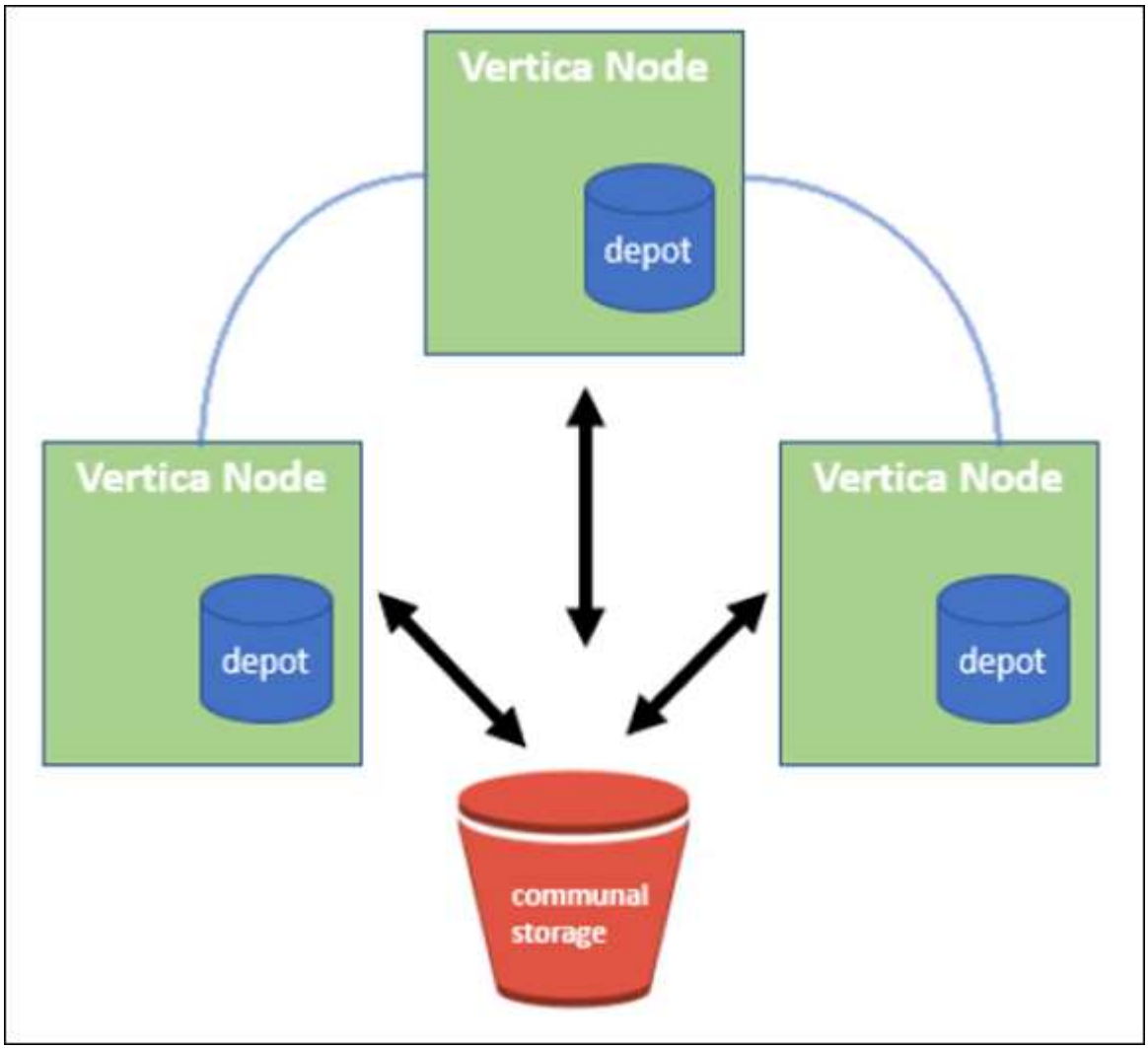
- Les bases de données du mode EON utilisent le stockage communautaire pour leurs données. Ceci est recommandé par Vertica.
- Les bases de données Enterprise mode stockent les données localement dans le système de fichiers des nœuds qui composent la base de données.

Architecture du mode EON

Le mode EON sépare les ressources de calcul de la couche de stockage communautaire de la base de données, ce qui permet l'évolutivité séparée du calcul et du stockage. Vertica en mode Eon est optimisé pour traiter des charges de travail variables et les isoler les unes des autres à l'aide de ressources de calcul et de

stockage distinctes.

EON mode stocke les données dans un magasin d'objets partagés appelé stockage communal : un compartiment S3, hébergé sur site ou sur Amazon S3.



Stockage communautaire

Au lieu de stocker les données localement, le mode Eon utilise un emplacement de stockage commun unique pour toutes les données et le catalogue (métadonnées). Le stockage communal est l'emplacement de stockage centralisé de la base de données, partagé entre les nœuds de base de données.

Le stockage communal a les propriétés suivantes :

- Le stockage communautaire dans le cloud ou dans un stockage objet sur site est plus résilient et moins vulnérable aux pertes de données dues à des défaillances de stockage que sur un stockage sur disque sur des machines individuelles.
- Toutes les données peuvent être lues par n'importe quel nœud utilisant le même chemin d'accès.
- La capacité n'est pas limitée par l'espace disque sur les nœuds.
- Les données étant stockées dans la communauté, vous pouvez faire évoluer votre cluster en toute flexibilité pour répondre aux besoins changeants. Si les données étaient stockées localement sur les nœuds, ajouter ou supprimer des nœuds nécessiterait un déplacement de grandes quantités de données

entre les nœuds pour les déplacer hors des nœuds supprimés, ou vers les nœuds nouvellement créés.

Le dépôt

La vitesse est un inconvénient du stockage commun. L'accès aux données à partir d'un emplacement cloud partagé est plus lent que la lecture à partir d'un disque local. En outre, la connexion au stockage commun peut former un goulot d'étranglement si de nombreux nœuds lisent les données à partir de ce stockage en même temps. Pour améliorer la vitesse d'accès aux données, les nœuds d'une base de données en mode Eon maintiennent un cache de disque local de données appelé dépôt. Lors de l'exécution d'une requête, les nœuds vérifient d'abord si les données dont ils ont besoin se trouvent dans le dépôt. Si c'est le cas, il termine la requête en utilisant la copie locale des données. Si les données ne se trouvent pas dans le dépôt, le nœud extrait les données du stockage commun et enregistre une copie dans le dépôt.

Recommandations de NetApp StorageGRID

Vertica stocke les données de base de données dans le stockage objet sous la forme de milliers (ou de millions) d'objets compressés (dont la taille observée est de 200 à 500 Mo par objet). Lorsqu'un utilisateur exécute des requêtes de base de données, Vertica récupère la plage de données sélectionnée à partir de ces objets compressés en parallèle à l'aide de l'appel GET de plage d'octets. Chaque PLAGE d'octets GET est d'environ 8 Ko.

Lors du test de requêtes utilisateur externes au dépôt de bases de données de 10 To, 4,000 à 10,000 REQUÊTES GET (OCTET-plage) par seconde ont été envoyées dans la grille. Lors de l'exécution de ce test avec des appliances SG6060, si le taux d'utilisation du processeur par nœud d'appliance est faible (environ 20 à 30 %), 2/3 le temps du processeur est en attente des E/S. Un très faible pourcentage (0 % à 0.5 %) d'attente d'E/S est observé sur le SGF6024.

En raison de la forte demande en IOPS peu élevées avec des latences très faibles (la moyenne doit être inférieure à 0.01 secondes), NetApp recommande l'utilisation du système SFG6024 pour les services de stockage objet. Si le SG6060 est nécessaire pour des bases de données très volumineuses, le client doit travailler avec l'équipe des comptes Vertica sur le dimensionnement du dépôt pour prendre en charge le dataset très interrogé.

Pour le nœud d'administration et le nœud de passerelle d'API, le client peut utiliser le SG100 ou le SG1000. Le choix dépend du nombre de requêtes des utilisateurs en parallèle et de la taille de la base de données. Si le client préfère utiliser un équilibreur de charge tiers, NetApp recommande un équilibreur de charge dédié pour une charge de travail hautes performances. Pour connaître le dimensionnement StorageGRID, consultez l'équipe de gestion de compte NetApp.

D'autres recommandations concernant la configuration de StorageGRID incluent :

- **Topologie de grille**. Ne mélangez pas le SGF6024 avec d'autres modèles d'appliance de stockage sur le même site de réseau. Si vous préférez utiliser le SG6060 pour la protection de l'archivage à long terme, conservez le SGF6024 avec un équilibreur de charge dédié dans son propre site de grid (site physique ou logique) pour une base de données active afin d'améliorer les performances. L'utilisation de différents modèles d'appliance sur le même site réduit les performances globales sur le site.
- **Protection des données**. Utilisez des copies répliquées pour la protection. N'utilisez pas le code d'effacement pour une base de données active. Le client peut utiliser un code d'effacement pour protéger à long terme les bases de données inactives.
- **N'activez pas la compression de grille**. Vertica compresse les objets avant de les stocker dans le stockage objet. L'activation de la compression grid n'entraîne pas d'économie supplémentaire en matière d'utilisation du stockage et réduit considérablement les performances GET de plage d'octets.
- **Connexion de terminal HTTP et HTTPS S3**. Lors du test de banc d'essai, nous avons observé une

amélioration des performances d'environ 5 % lors de l'utilisation d'une connexion HTTP S3 du cluster Vertica vers le point de terminaison de l'équilibreur de charge StorageGRID. Ce choix doit être basé sur les exigences de sécurité du client.

Les recommandations pour une configuration Vertica sont les suivantes :

- **Les paramètres de dépôt par défaut de la base de données Vertica sont activés (valeur = 1) pour les opérations de lecture et d'écriture**. NetApp recommande fortement de maintenir ces paramètres de dépôt activés pour améliorer les performances.
- **Désactiver les limitations de diffusion**. Pour plus de détails sur la configuration, reportez-vous à la section Désactivation des restrictions de diffusion en continu.

Installation du mode Eon sur site avec stockage communautaire sur StorageGRID

Les sections suivantes décrivent la procédure, dans l'ordre, d'installation du mode Eon sur site avec un stockage communautaire sur StorageGRID. La procédure de configuration du stockage objet compatible S3 (simple Storage Service) sur site est similaire à la procédure décrite dans le guide Vertica, "Installez une base de données en mode Eon sur site".

La configuration suivante a été utilisée pour le test fonctionnel :

- StorageGRID 11.4.0.4
- Vertica 10.1.0
- Trois machines virtuelles (VM) avec CentOS 7.x OS pour les nœuds Vertica afin de former un cluster. Cette configuration est destinée uniquement au test fonctionnel, pas au cluster de base de données de production Vertica.

Ces trois nœuds sont configurés avec une clé Secure Shell (SSH) afin de permettre SSH sans mot de passe entre les nœuds du cluster.

Informations requises par NetApp StorageGRID

Pour installer Eon mode sur site avec un stockage communautaire sur StorageGRID, vous devez disposer des informations de prérequis suivantes.

- Adresse IP ou nom de domaine complet (FQDN) et numéro de port du terminal StorageGRID S3. Si vous utilisez HTTPS, utilisez un certificat SSL personnalisé (autorité de certification) ou un certificat SSL auto-signé mis en œuvre sur le terminal StorageGRID S3.
- Nom du compartiment. Il doit exister au préalable et être vide.
- L'ID de clé et la clé d'accès secrète avec un accès en lecture et en écriture au compartiment.

Création d'un fichier d'autorisation pour accéder au terminal S3

Les prérequis suivants s'appliquent lors de la création d'un fichier d'autorisation pour accéder au terminal S3 :

- Vertica est installé.
- Un cluster est configuré, configuré et prêt pour la création de bases de données.

Pour créer un fichier d'autorisation pour accéder au terminal S3, effectuez la procédure suivante :

1. Connectez-vous au nœud Vertica sur lequel vous allez exécuter `admintools` Pour créer la base de données du mode Eon.

L'utilisateur par défaut est `dbadmin`, Créé lors de l'installation du cluster Vertica.

2. Utilisez un éditeur de texte pour créer un fichier sous le `/home/dbadmin` répertoire. Le nom du fichier peut être tout ce que vous voulez, par exemple, `sg_auth.conf`.
3. Si le terminal S3 utilise un port HTTP standard 80 ou HTTPS 443, ignorez le numéro de port. Pour utiliser HTTPS, définissez les valeurs suivantes :

   ◦ `awsenablehttps = 1`, sinon, définissez la valeur sur `0`.

   ◦ `awsauth = <s3 access key ID>:<secret access key>`

   ◦ `awsendpoint = <StorageGRID s3 endpoint>:<port>`

   Pour utiliser un certificat SSL personnalisé ou auto-signé pour la connexion HTTPS du noeud final StorageGRID S3, spécifiez le chemin d'accès complet au fichier et le nom du fichier du certificat. Ce fichier doit se trouver au même emplacement sur chaque nœud de la Vertica et avoir des droits d'accès en lecture pour tous les utilisateurs. Ignorez cette étape si le certificat SSL du terminal StorageGRID S3 est signé par une autorité de certification publique.

   - `awscafile = <filepath/filename>`

   Par exemple, consultez le fichier d'exemple suivant :

```
awsauth = MNVU4OYFAY2xyz123:03vuO4M4KmdfwffT8nqnBmnMVTr78Gu9wANabcxyz
awsendpoint = s3.england.connectlab.io:10443
awsenablehttps = 1
awscafile = /etc/custom-cert/grid.pem
```

+

> ⓘ Dans un environnement de production, le client doit implémenter un certificat de serveur signé par une autorité de certification publique sur un terminal d'équilibrage de charge StorageGRID S3.

Sélection d'un chemin de dépôt sur tous les nœuds de la Vertica

Choisissez ou créez un répertoire sur chaque nœud pour le chemin de stockage du dépôt. Le répertoire que vous fournissez pour le paramètre chemin de stockage du dépôt doit avoir les éléments suivants :

- Le même chemin sur tous les nœuds du cluster (par exemple, `/home/dbadmin/depot`)
- Être lisible et inscriptible par l'utilisateur dbadmin
- Un stockage suffisant

  Par défaut, Vertica utilise 60 % de l'espace du système de fichiers contenant le répertoire pour le stockage du dépôt. Vous pouvez limiter la taille du dépôt en utilisant le `--depot-size` argument dans le `create_db` commande. Voir "Dimensionnement du cluster Vertica pour une base de données en mode Eon" article pour les directives générales de dimensionnement de la Vertica ou consultez votre gestionnaire de compte Vertica.

  Le `admintools create_db` l'outil tente de créer le chemin de dépôt pour vous si celui-ci n'existe pas.

Création de la base de données Eon sur site

Pour créer la base de données Eon sur site, procédez comme suit :

1. Pour créer la base de données, utilisez le `admintools create_db` outil.

   La liste suivante fournit une brève explication des arguments utilisés dans cet exemple. Consultez le document Vertica pour obtenir une explication détaillée de tous les arguments requis et facultatifs.

   - `-x <path/filename of authorization file>`

     Pour plus de détails sur le fichier d'autorisation, reportez-vous à Création d'un fichier d'autorisation pour accéder au terminal S3.

   Les détails d'autorisation sont stockés dans la base de données après la création. Vous pouvez supprimer ce fichier pour éviter d'exposer la clé secrète S3.

   - `--communal-storage-location <s3://storagegrid bucketname>`
   - `-s <comma-separated list of Vertica nodes to be used for this database>`
   - `-d <name of database to be created>`
   - `-p <password to be set for this new database>` Par exemple, consultez l'exemple de commande suivant :

     ```
     admintools -t create_db -x sg_auth.conf --communal-storage
     -location=s3://vertica --depot-path=/home/dbadmin/depot --shard
     -count=6 -s vertica-vm1,vertica-vm2,vertica-vm3 -d vmart -p
     '<password>'
     ```

     La création d'une nouvelle base de données prend plusieurs minutes en fonction du nombre de nœuds de la base de données. Lors de la création de la base de données pour la première fois, vous serez invité à accepter le contrat de licence.

Par exemple, reportez-vous à l'exemple de fichier d'autorisation suivant et `create db` commande :

```
[dbadmin@vertica-vm1 ~]$ cat sg_auth.conf
awsauth = MNVU4OYFAY2CPKVXVxxxx:03vuO4M4KmdfwffT8nqnBmnMVTr78Gu9wAN+xxxx
awsendpoint = s3.england.connectlab.io:10445
awsenablehttps = 1

[dbadmin@vertica-vm1 ~]$ admintools -t create_db -x sg_auth.conf
--communal-storage-location=s3://vertica --depot-path=/home/dbadmin/depot
--shard-count=6 -s vertica-vm1,vertica-vm2,vertica-vm3 -d vmart -p
'xxxxxxxx'
Default depot size in use
Distributing changes to cluster.
    Creating database vmart
    Starting bootstrap node v_vmart_node0007 (10.45.74.19)
    Starting nodes:
```

```
        v_vmart_node0007 (10.45.74.19)
    Starting Vertica on all nodes. Please wait, databases with a large
catalog may take a while to initialize.
    Node Status: v_vmart_node0007: (DOWN)
    Node Status: v_vmart_node0007: (DOWN)
    Node Status: v_vmart_node0007: (DOWN)
    Node Status: v_vmart_node0007: (UP)
    Creating database nodes
    Creating node v_vmart_node0008 (host 10.45.74.29)
    Creating node v_vmart_node0009 (host 10.45.74.39)
    Generating new configuration information
    Stopping single node db before adding additional nodes.
    Database shutdown complete
    Starting all nodes
Start hosts = ['10.45.74.19', '10.45.74.29', '10.45.74.39']
    Starting nodes:
        v_vmart_node0007 (10.45.74.19)
        v_vmart_node0008 (10.45.74.29)
        v_vmart_node0009 (10.45.74.39)
    Starting Vertica on all nodes. Please wait, databases with a large
catalog may take a while to initialize.
    Node Status: v_vmart_node0007: (DOWN) v_vmart_node0008: (DOWN)
v_vmart_node0009: (DOWN)
    Node Status: v_vmart_node0007: (DOWN) v_vmart_node0008: (DOWN)
v_vmart_node0009: (DOWN)
    Node Status: v_vmart_node0007: (DOWN) v_vmart_node0008: (DOWN)
v_vmart_node0009: (DOWN)
    Node Status: v_vmart_node0007: (DOWN) v_vmart_node0008: (DOWN)
v_vmart_node0009: (DOWN)
    Node Status: v_vmart_node0007: (UP) v_vmart_node0008: (UP)
v_vmart_node0009: (UP)
Creating depot locations for 3 nodes
Communal storage detected: rebalancing shards

Waiting for rebalance shards. We will wait for at most 36000 seconds.
Installing AWS package
    Success: package AWS installed
Installing ComplexTypes package
    Success: package ComplexTypes installed
Installing MachineLearning package
    Success: package MachineLearning installed
Installing ParquetExport package
    Success: package ParquetExport installed
Installing VFunctions package
    Success: package VFunctions installed
Installing approximate package
```

```
    Success: package approximate installed
Installing flextable package
    Success: package flextable installed
Installing kafka package
    Success: package kafka installed
Installing logsearch package
    Success: package logsearch installed
Installing place package
    Success: package place installed
Installing txtindex package
    Success: package txtindex installed
Installing voltagesecure package
    Success: package voltagesecure installed
Syncing catalog on vmart with 2000 attempts.
Database creation SQL tasks completed successfully. Database vmart created
successfully.
```

Taille de l'objet (octet)	Chemin d'accès complet de la clé de compartiment/objet
61	s3://vertica/051/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a07/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a07_0_0.dfs
145	s3://vertica/2c4/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a3d/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a3d_0_0.dfs
146	s3://vertica/33c/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a1d/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a1d_0_0.dfs
40	s3://vertica/382/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a31/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a31_0_0.dfs
145	s3://vertica/42f/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a21/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a21_0_0.dfs
34	s3://vertica/472/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a25/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a25_0_0.dfs

Taille de l'objet (octet)	Chemin d'accès complet de la clé de compartiment/objet
41	s3://vertica/476/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a2d/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a2d_0_0.dfs
61	s3://vertica/52a/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a5d/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a5d_0_0.dfs
131	s3://vertica/5d2/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a19/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a19_0_0.dfs
91	s3://vertica/5f7/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a11/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a11_0_0.dfs
118	s3://vertica/82d/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a15/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a15_0_0.dfs
115	s3://vertica/9a2/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a61/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a61_0_0.dfs
33	s3://vertica/acd/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a29/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a29_0_0.dfs
133	s3://vertica/b98/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a4d/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a4d_0_0.dfs
38	s3://vertica/db3/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a49/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a49_0_0.dfs
38	s3://vertica/eba/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a59/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a59_0_0.dfs
21521920	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000215e2/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000215e2.tar

Taille de l'objet (octet)	Chemin d'accès complet de la clé de compartiment/objet
6865408	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021602/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021602.tar
204217344	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021610/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021610.tar
16109056	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000217e0/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000217e0.tar
12853248	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021800/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021800.tar
8937984	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a00000002187a/026d63ae9d4a33237bf0e2c2cf2a794a00a000000002187a.tar
56260608	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a000000218b2/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000218b2.tar
53947904	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a000000219ba/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000219ba.tar
44932608	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a000000219de/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000219de.tar
256306688	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a6e/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a6e.tar
8062464	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021e34/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021e34.tar
20024832	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021e70/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021e70.tar

Taille de l'objet (octet)	Chemin d'accès complet de la clé de compartiment/objet
10444	s3://vertica/metadata/VMart/cluster_config.json
823266	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c13_13/chkpt_1.cat.gz
254	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c13_13/completed
2958	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c2_2/chkpt_1.cat.gz
231	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c2_2/completed
822521	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c4_4/chkpt_1.cat.gz
231	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c4_4/completed
746513	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_14_g14.cat
2596	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_3_g3.cat.gz
821065	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_4_g4.cat.gz
6440	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_5_g5.cat
8518	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_8_g8.cat
0	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/tiered_catalog.cat

Taille de l'objet (octet)	Chemin d'accès complet de la clé de compartiment/objet
822922	s3://vertica/metadata/VMart/nodes/v_vmart_node0017/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c14_7/chkpt_1.cat.gz
232	s3://vertica/metadata/VMart/nodes/v_vmart_node0017/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c14_7/completed
822930	s3://vertica/metadata/VMart/nodes/v_vmart_node0017/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_14_g7.cat.gz
755033	s3://vertica/metadata/VMart/nodes/v_vmart_node0017/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_15_g8.cat
0	s3://vertica/metadata/VMart/nodes/v_vmart_node0017/Catalog/859703b06a3456d95d0be28575a673/tiered_catalog.cat
822922	s3://vertica/metadata/VMart/nodes/v_vmart_node0018/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c14_7/chkpt_1.cat.gz
232	s3://vertica/metadata/VMart/nodes/v_vmart_node0018/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c14_7/completed
822930	s3://vertica/metadata/VMart/nodes/v_vmart_node0018/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_14_g7.cat.gz
755033	s3://vertica/metadata/VMart/nodes/v_vmart_node0018/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_15_g8.cat
0	s3://vertica/metadata/VMart/nodes/v_vmart_node0018/Catalog/859703b06a3456d95d0be28575a673/tiered_catalog.cat

Désactivation des restrictions de diffusion en continu

Cette procédure est basée sur le guide Vertica pour d'autres systèmes de stockage objet sur site et doit s'appliquer à StorageGRID.

1. Après avoir créé la base de données, désactivez le `AWSStreamingConnectionPercentage` paramètre de configuration en le définissant sur `0`. Ce paramètre n'est pas nécessaire pour une installation sur site en mode Eon avec stockage communautaire. Ce paramètre de configuration contrôle le nombre de connexions au magasin d'objets utilisé par Vertica pour les lectures en continu. Dans un environnement cloud, ce paramètre évite que les données en streaming à partir du magasin d'objets utilisent tous les descripteurs de fichier disponibles. Certains poignées de fichiers restent disponibles pour d'autres opérations de stockage d'objets. En raison de la faible latence des magasins d'objets sur site, cette option

n’est pas nécessaire.

2. Utiliser un `vsql` instruction permettant de mettre à jour la valeur du paramètre. Le mot de passe est le mot de passe de la base de données que vous avez défini dans la section “création de la base de données Eon sur site”. Par exemple, reportez-vous à l’exemple de résultat suivant :

```
[dbadmin@vertica-vm1 ~]$ vsql
Password:
Welcome to vsql, the Vertica Analytic Database interactive terminal.
Type:   \h or \? for help with vsql commands
        \g or terminate with semicolon to execute query
        \q to quit
dbadmin=> ALTER DATABASE DEFAULT SET PARAMETER
AWSStreamingConnectionPercentage = 0; ALTER DATABASE
dbadmin=> \q
```

Vérification des paramètres du dépôt

Les paramètres de dépôt par défaut de la base de données Vertica sont activés (valeur = 1) pour les opérations de lecture et d’écriture. NetApp recommande fortement de maintenir ces paramètres de dépôt activés pour améliorer les performances.

```
vsql -c 'show current all;' | grep -i UseDepot
DATABASE | UseDepotForReads | 1
DATABASE | UseDepotForWrites | 1
```

Chargement des données d’échantillon (facultatif)

Si cette base de données est destinée aux tests et sera supprimée, vous pouvez charger des données d’échantillon dans cette base de données pour les tests. Vertica est fourni avec un exemple de jeu de données, VMart, sous `/opt/vertica/examples/VMart_Schema/` Sur chaque nœud Vertica. Vous trouverez plus d’informations sur cet exemple de jeu de données "ici".

Procédez comme suit pour charger les données d’échantillon :

1. Connectez-vous en tant que dbadmin à l’un des nœuds de la Vertica : cd /opt/vertica/sou/VMart_Schema/
2. Chargez les exemples de données dans la base de données et entrez le mot de passe de la base de données lorsque vous y êtes invité dans les sous-étapes c et d :
   a. `cd /opt/vertica/examples/VMart_Schema`
   b. `./vmart_gen`
   c. `vsql < vmart_define_schema.sql`
   d. `vsql < vmart_load_data.sql`
3. Il existe plusieurs requêtes SQL prédéfinies, vous pouvez les exécuter pour confirmer que les données de test sont chargées correctement dans la base de données. Par exemple : `vsql < vmart_queries1.sql`

Où trouver des informations complémentaires

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

- "Documentation du produit NetApp StorageGRID 11.7"
- "Fiche technique StorageGRID"
- "Documentation produit de Vertica 10.1"

Historique des versions

Version	Date	Historique des versions du document
Version 1.0	Septembre 2021	Version initiale.

Par Angela Cheng

Analyse des journaux StorageGRID à l'aide de la pile ELK

Par Angela Cheng

Grâce à la fonction de transfert syslog StorageGRID, vous pouvez configurer un serveur syslog externe pour collecter et analyser les messages journaux StorageGRID. ELK (Elasticsearch, Logstash, Kibana) est devenu l'une des solutions d'analytique des journaux les plus populaires. Regardez la "Analyse du journal StorageGRID à l'aide de la vidéo ELK" pour afficher un exemple de configuration ELK et découvrir comment elle peut être utilisée pour identifier et dépanner les requêtes S3 ayant échoué. StorageGRID 11.9 prend en charge l'exportation du journal d'accès aux noeuds finaux de l'équilibreur de charge vers le serveur syslog externe. Regardez cette "Vidéo YouTube" vidéo pour en savoir plus sur cette nouvelle fonctionnalité. Cet article fournit des exemples de fichiers de configuration Logstash, de requêtes Kibana, de graphiques et de tableau de bord, pour vous offrir un démarrage rapide de la gestion des journaux et de l'analytique StorageGRID.

De formation

- StorageGRID 11.6.0.2 ou version ultérieure
- ELK (Elasticsearch, Logstash et Kibana) 7.1x ou plus installé et en fonctionnement

Exemples de fichiers

- "Téléchargez le paquet Logstash 7.x." + **md5 checksum** 148c23d0021d9a4bb4a6c0287464deab + **sha256 checksum** f51ec9e2e3f842d5a781566b167a561b4373038b4e7bb3c8b5d52f2f2d2f2f2f2f2d2f2f2f2f2f2f2f2f6f6f
- "Téléchargez le paquet Logstash 8.x." + **md5 checksum** e11bae3a662f87c310ef363d0fe06835 + **total de contrôle sha256** 5c670755742cfdfd5aa723a596ba087e0153a65bcaef3934afdb682f61cd278d
- "Téléchargez le paquet Logstash 8.x des fichiers d'exemple pour StorageGRID 11.9" + **somme de contrôle md5** 41272857c4a54600f95995f6ed74800d + **somme de contrôle sha256** 67048ee8661052719990851e1ad960d4902fe537a6e135e8600177188da677c9

Hypothèse

Les lecteurs connaissent la terminologie et les opérations de StorageGRID et d'ELK.

Instructions

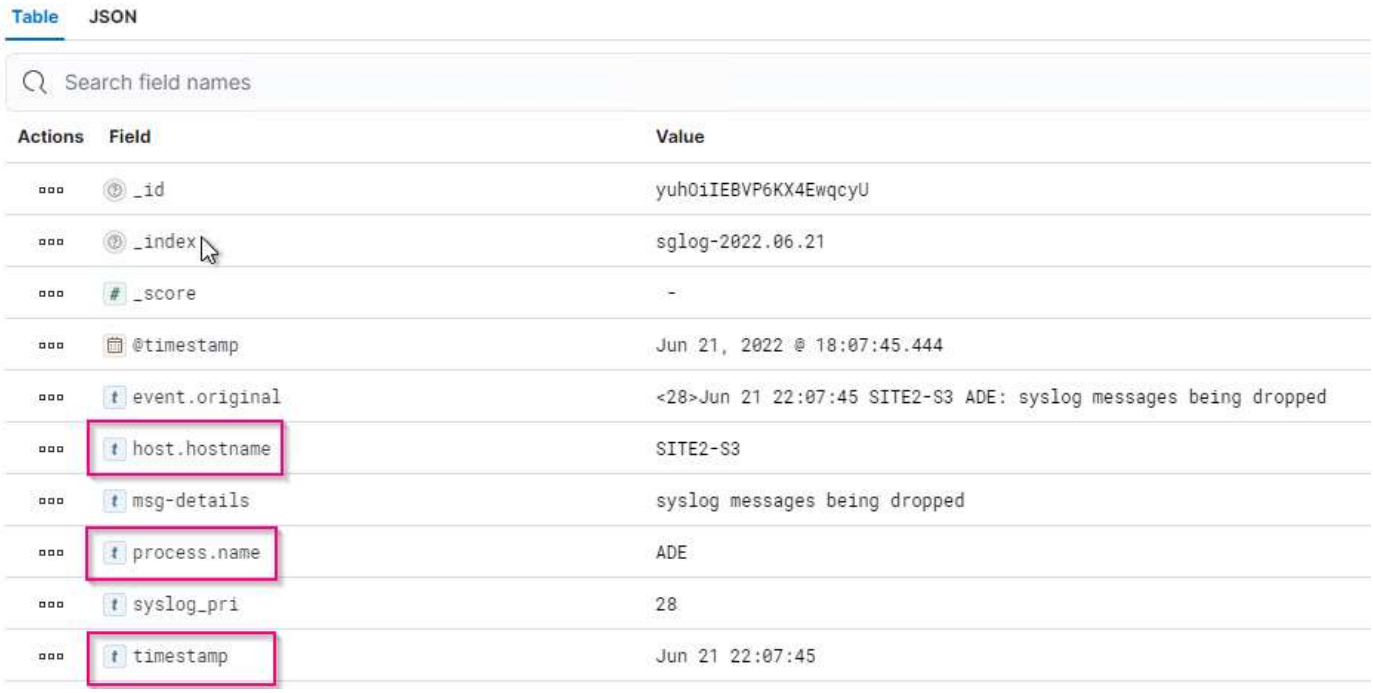
Deux exemples de versions sont fournis en raison des différences de noms définies par des motifs grk. + par exemple, le modèle SYSLOGBASE grok dans le fichier de configuration Logstash définit les noms de champs différemment en fonction de la version Logstash installée.

```
match => {"message" => '<%{POSINT:syslog_pri}>%{SYSLOGBASE}
%{GREEDYDATA:msg-details}'}
```

Logstash 7.17 échantillon

Field	Value
t _id	7C1MaYEBRH8UbfKnIls8
t _index	sgrid2-2022.06.15
# _score	-
t _type	_doc
@timestamp	Jun 15, 2022 @ 17:36:46.038
t host	grid2-site2-s1
t logsource	SITE2-S1
t msg-details	Reloading syslog service
t pid	628
t program	update-sysl
t syslog_pri	37
t timestamp	Jun 15 21:36:46

Logstash 8.23 échantillon



Étapes

1. Décompressez l'échantillon fourni en fonction de la version ELK installée. + l'exemple de dossier inclut deux exemples de configuration de Logstash : + **sglog-2-file.conf:** ce fichier de configuration envoie des messages de journal StorageGRID vers un fichier sur Logstash sans transformation de données. Vous pouvez l'utiliser pour confirmer que Logstash reçoit des messages StorageGRID ou pour vous aider à comprendre les modèles de journaux StorageGRID. + **sglog-2-es.conf:** ce fichier de configuration transforme les messages du journal StorageGRID en utilisant divers modèles et filtres. Il comprend des exemples d'instructions de DROP, qui sont basées sur des motifs ou des filtres. Le résultat est envoyé à Elasticsearch pour l'indexation. + Personnalisez le fichier de configuration sélectionné en fonction de l'instruction dans le fichier.
2. Testez le fichier de configuration personnalisé :

```
/usr/share/logstash/bin/logstash --config.test_and_exit -f <config-file-path/file>
```

   Si la dernière ligne renvoyée est similaire à la ligne ci-dessous, le fichier de configuration n'a pas d'erreurs de syntaxe :

```
[LogStash::Runner] runner - Using config.test_and_exit mode. Config Validation Result: OK. Exiting Logstash
```

3. Copiez le fichier conf personnalisé dans la configuration du serveur Logstash : /etc/logstash/conf.d + si vous n'avez pas activé config.reload.automatic dans /etc/logstash/logstash.yml, redémarrez le service Logstash. Dans le cas contraire, attendez que l'intervalle de rechargement de la configuration s'écoule.

```
grep reload /etc/logstash/logstash.yml
```

```
# Periodically check if the configuration has changed and reload the
pipeline
config.reload.automatic: true
config.reload.interval: 5s
```

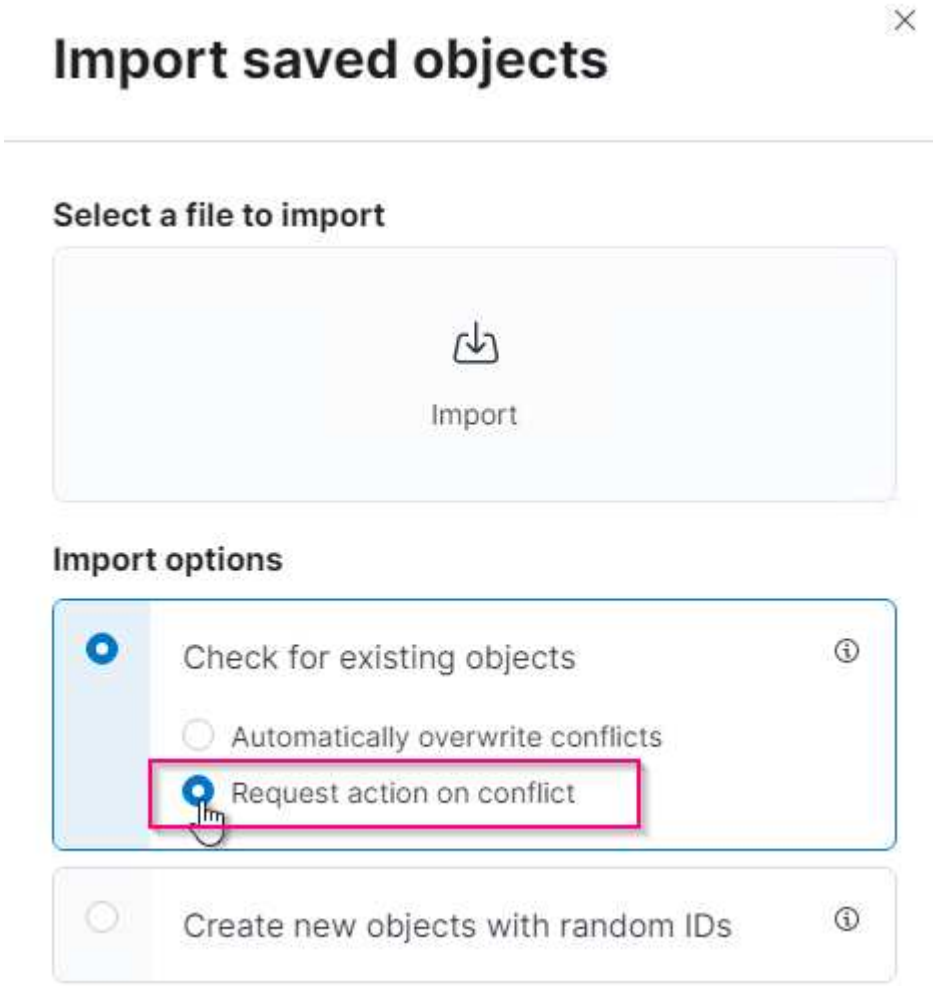
4. Vérifiez /var/log/logstash/logstash-plain.log et assurez-vous qu'il n'y a pas d'erreur lors du démarrage de Logstash avec le nouveau fichier de configuration.
5. Vérifiez que le port TCP est démarré et que vous écoutez. + dans cet exemple, le port TCP 5000 est utilisé.

```
netstat -ntpa | grep 5000
tcp6       0      0 :::5000                 :::*
LISTEN      25744/java
```

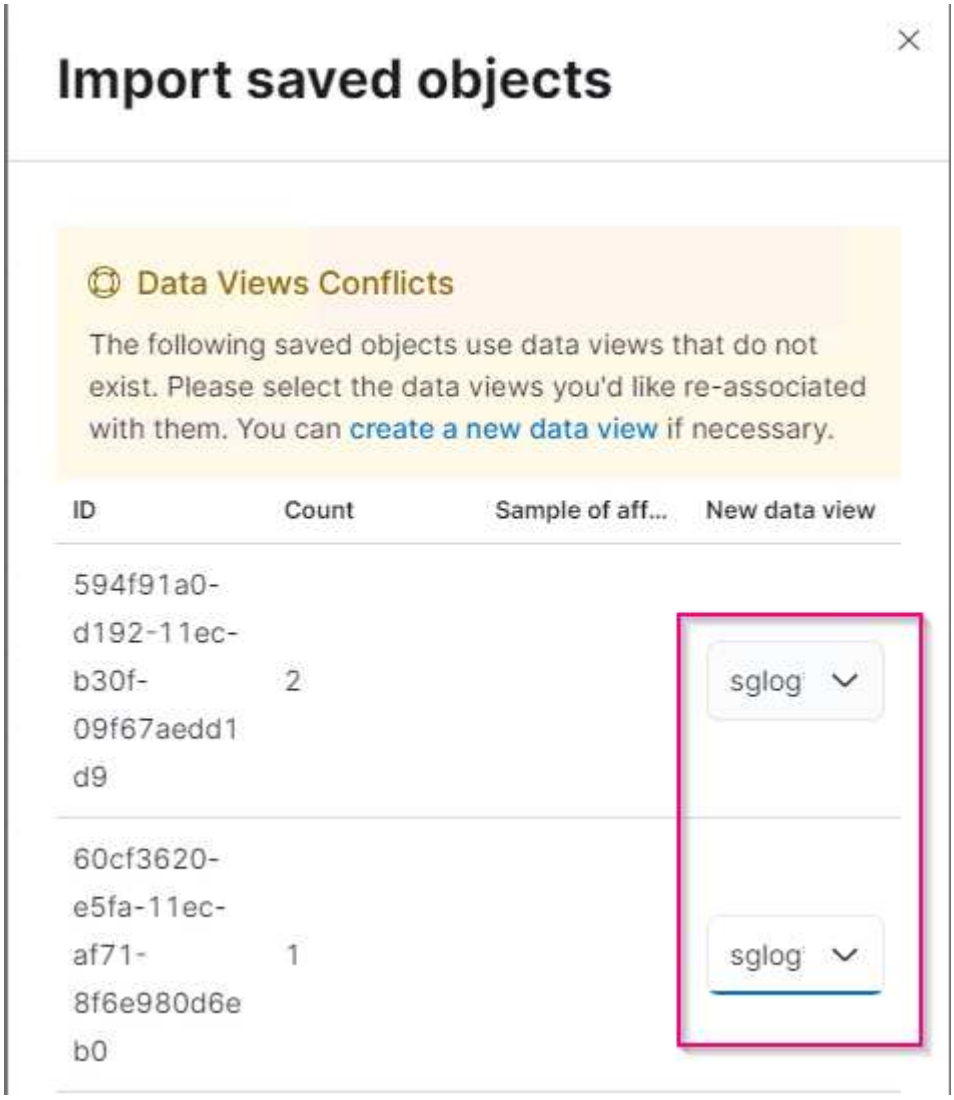
6. À partir de l'interface graphique du gestionnaire StorageGRID, configurez le serveur syslog externe pour envoyer des messages de journal à Logstash. Reportez-vous au "vidéo de démonstration" pour plus de détails.
7. Vous devez configurer ou désactiver le pare-feu sur le serveur Logstash pour autoriser la connexion des nœuds StorageGRID au port TCP défini.
8. Dans l'interface graphique Kibana, sélectionnez Management → Dev Tools. Sur la page Console, exécutez cette commande OBTENIR pour confirmer la création de nouveaux index sur Elasticsearch.

```
GET /_cat/indices/*?v=true&s=index
```

9. A partir de l'interface graphique Kibana, créez un motif d'index (ELK 7.x) ou une vue de données (ELK 8.x).
10. Dans l'interface utilisateur graphique de Kibana, entrez « objets lavés » dans la zone de recherche située en haut au centre. + sur la page objets enregistrés, sélectionnez Importer. Sous Options d'importation, sélectionnez « demander une action en cas de conflit »



Importez elk<version>-query-chart-sample.ndjson. + lorsque vous êtes invité à résoudre le conflit, sélectionnez le modèle d'index ou la vue de données que vous avez créé à l'étape 8.



Les objets Kibana suivants sont importés : + **Query** + * audit-msg-s3rq-orlm + * bycast log s3 messages liés + * loglevel warning or above + * échec de l'événement de sécurité + bycast.log * nginx-gw journal d'accès au point final (disponible uniquement dans elk8-sample-for-sgg.zip) + **Chart** analyse de type de sécurité + nombre moyen de messages HTTP * s3 sur la base du tableau de temps de réponse * s3 * s3 + nombre de demandes supérieur à la demande * s3 *.

Vous êtes maintenant prêt à effectuer une analyse des journaux StorageGRID à l'aide de Kibana.

Ressources supplémentaires

- "syslog101"
- "Qu'est-ce que la pile ELK"
- "Motifs Grok"
- "Guide débutant de Logstash: Grok"
- "Guide pratique de Logstash : plongée en profondeur syslog"
- "Guide Kibana - Explorez le document"
- "Référence des messages du journal d'audit StorageGRID"

Grâce à Prometheus et Grafana, vous pouvez renforcer la conservation des metrics

Par Aron Klein

Ce rapport technique fournit des instructions détaillées pour la configuration de NetApp StorageGRID avec les services externes Prometheus et Grafana.

Introduction

StorageGRID stocke les metrics à l'aide de Prometheus et fournit des visualisations de ces metrics via des tableaux de bord intégrés. Vous pouvez accéder en toute sécurité aux metrics Prometheus depuis StorageGRID en configurant des certificats d'accès client et en activant l'accès prometheus pour le client spécifié. Aujourd'hui, la conservation de ces données de mesure est limitée par la capacité de stockage du nœud d'administration. Pour gagner plus de temps et pouvoir créer des visualisations personnalisées de ces metrics, nous déploierons un nouveau serveur Prometheus et Grafana, configurerons notre nouveau serveur afin de grattez les metrics à partir de l'instance IDS, et nous concevons un tableau de bord avec les mesures importantes. Vous pouvez obtenir plus d'informations sur les metrics Prometheus collectés dans la "Documentation StorageGRID".

Fédérer Prometheus

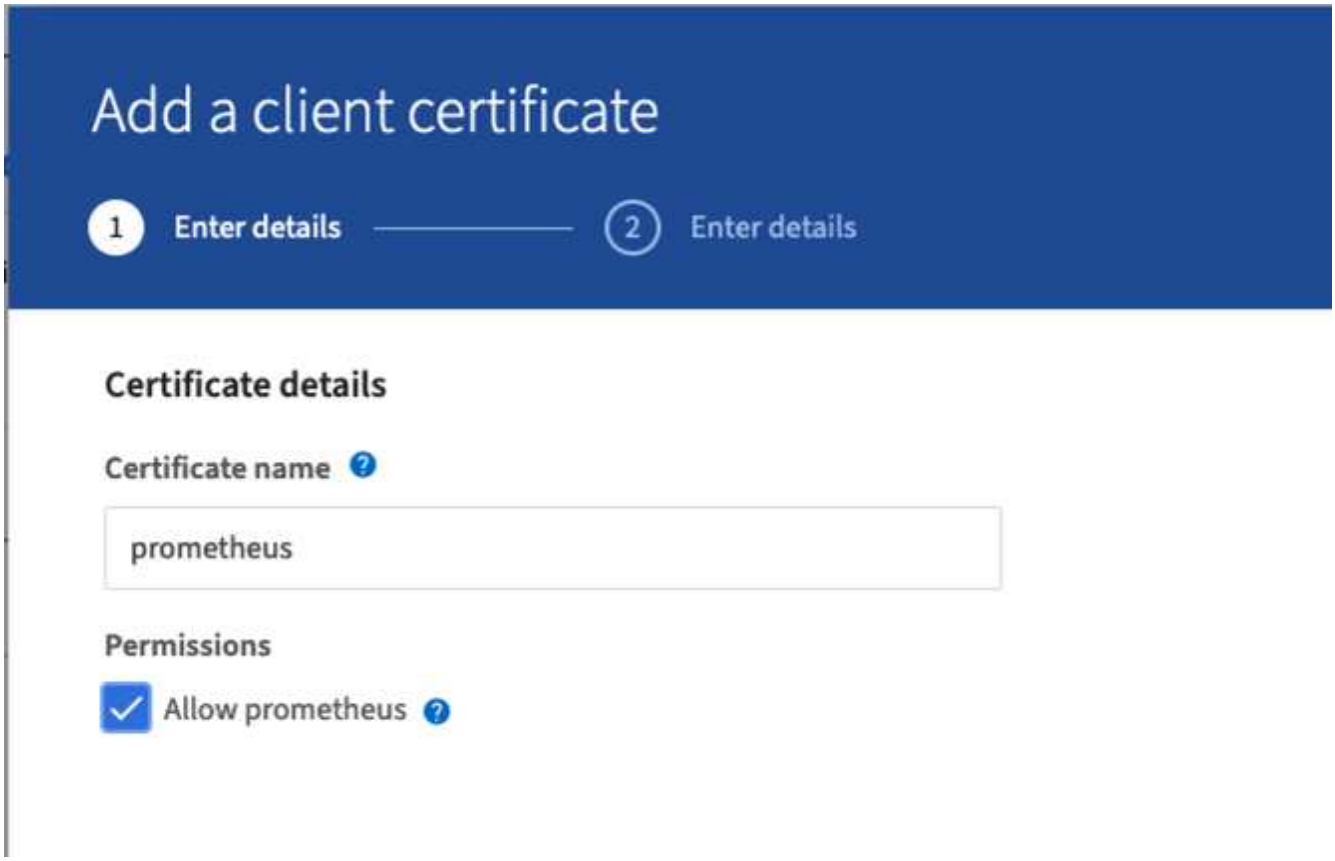
Détails de laboratoire

Pour les besoins de cet exemple, j'utiliserai toutes les machines virtuelles pour les nœuds StorageGRID 11.6 et un serveur Debian 11. L'interface de gestion StorageGRID est configurée avec un certificat d'autorité de certification public approuvé. Cet exemple ne passera pas par l'installation et la configuration du système StorageGRID ou de l'installation de Debian linux. Vous pouvez utiliser toutes les versions Linux que vous souhaitez prendre en charge par Prometheus et Grafana. Prometheus et Grafana peuvent être installés en tant que conteneurs docker, qu'ils soient issus de la source ou binaires précompilés. Dans cet exemple, je vais installer les binaires Prometheus et Grafana directement sur le même serveur Debian. Téléchargez et suivez les instructions d'installation de base sur https://prometheus.io et https://grafana.com/grafana/ respectivement.

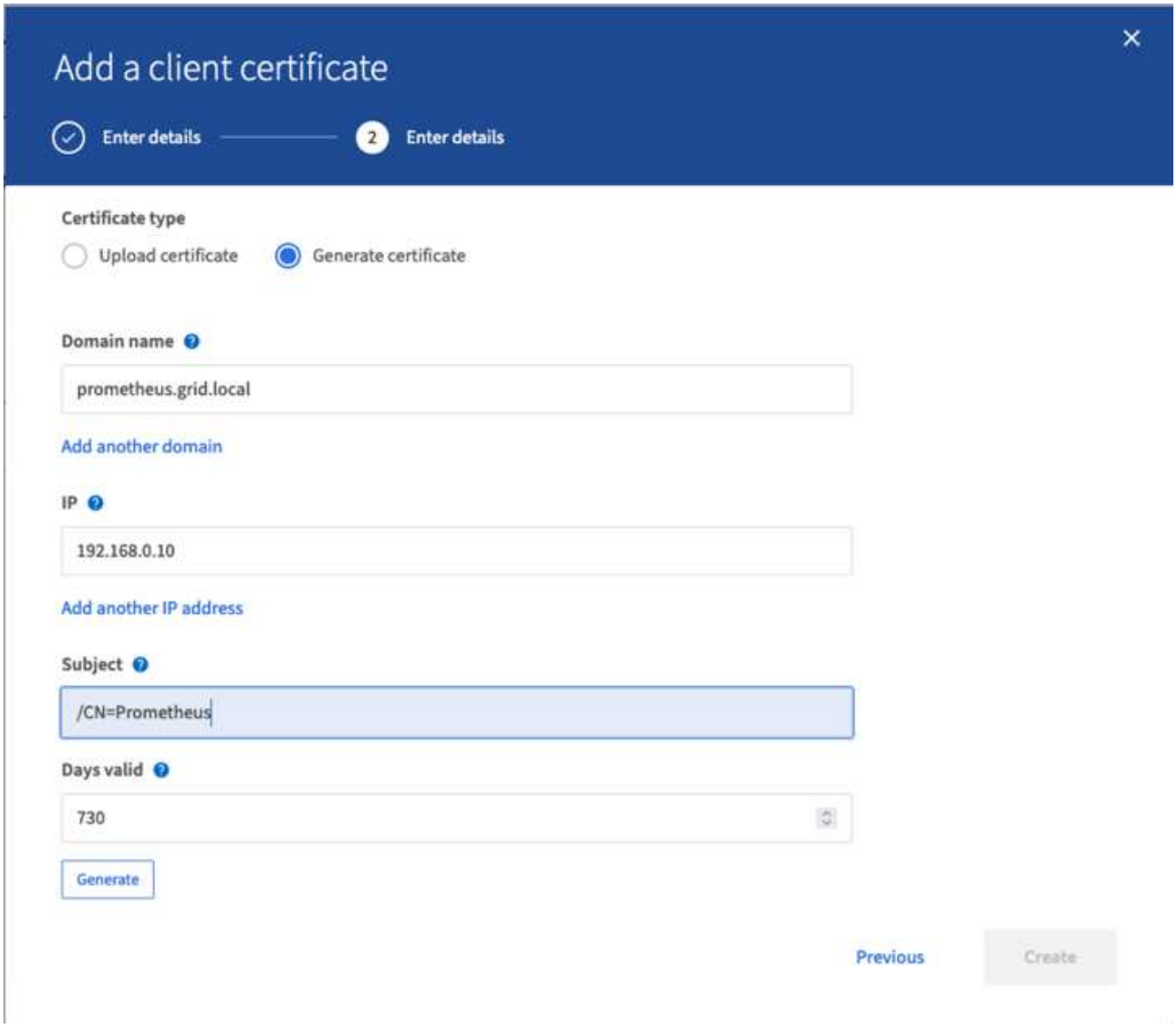
Configurez StorageGRID pour l'accès client Prometheus

Afin d'accéder aux identifiants de paramètres de la mémoire de la solution, vous devez générer ou télécharger un certificat client avec une clé privée et activer l'autorisation pour le client. L'interface de gestion StorageGRID doit posséder un certificat SSL. Ce certificat doit être approuvé par le serveur prometheus soit par une autorité de certification approuvée, soit manuellement approuvé s'il est auto-signé. Pour en savoir plus, consultez le "Documentation StorageGRID".

1. Dans l'interface de gestion StorageGRID, sélectionnez « CONFIGURATION » en bas à gauche, puis dans la deuxième colonne sous « sécurité », cliquez sur certificats.
2. Sur la page certificats, sélectionnez l'onglet « client » et cliquez sur le bouton « Ajouter ».
3. Indiquez un nom pour le client auquel l'accès sera accordé et utilisez ce certificat. Cliquez sur la case sous "permissions", devant "Autoriser Prometheus" et cliquez sur le bouton Continuer.

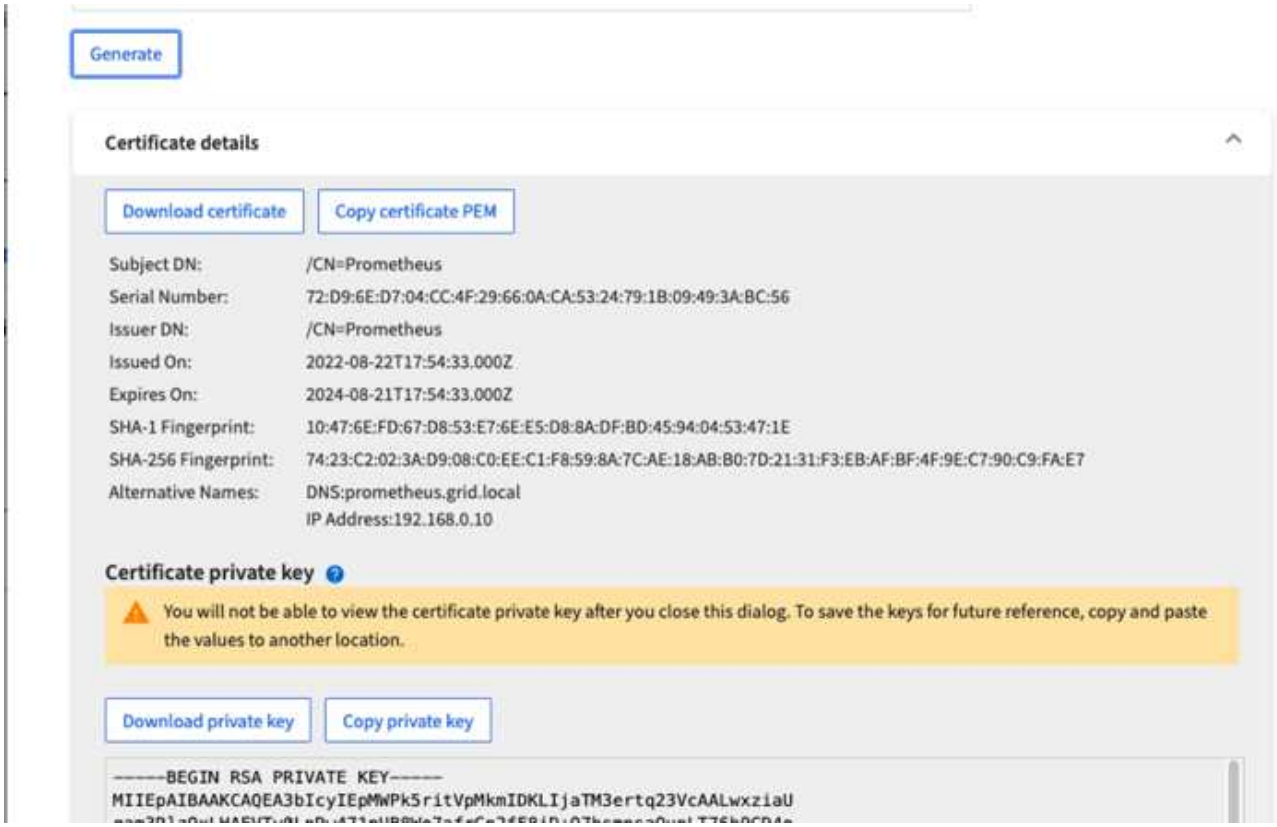


4. Si vous disposez d'un certificat signé par l'autorité de certification, vous pouvez sélectionner le bouton radio « Télécharger le certificat », mais dans notre cas, nous allons permettre à StorageGRID de générer le certificat client en sélectionnant le bouton radio « générer le certificat ». Les champs obligatoires s'affichent pour être renseignés. Saisissez le FQDN du serveur client, l'adresse IP du serveur, l'objet et les jours valides. Cliquez ensuite sur le bouton « générer ».



Be mindful of the certificate days valid entry as you will need to renew this certificate in both StorageGRID and the Prometheus server before it expires to maintain uninterrupted collection.

1. Téléchargez le fichier pem de certificat et le fichier pem de clé privée.



This is the only time you can download the private key, so make sure you do not skip this step.

Préparez le serveur Linux pour l'installation de Prometheus

Avant d'installer Prometheus, je souhaite préparer mon environnement avec un utilisateur Prometheus, la structure de répertoires et configurer la capacité pour l'emplacement de stockage des metrics.

1. Créez l'utilisateur Prometheus.

```
sudo useradd -M -r -s /bin/false Prometheus
```

2. Créez les répertoires pour les données Prometheus, les certificats client et les metrics.

```
sudo mkdir /etc/Prometheus /etc/Prometheus/cert /var/lib/Prometheus
```

3. J'ai formaté le disque que j'utilise pour la rétention des metrics avec un système de fichiers ext4.

```
mkfs -t ext4 /dev/sdb
```

4. Je ai ensuite monté le système de fichiers dans le répertoire des metrics de Prometheus.

```
sudo mount -t auto /dev/sdb /var/lib/prometheus/
```

5. Obtenez l'UUID du disque que vous utilisez pour les données de metrics.

```
sudo ls -al /dev/disk/by-uuid/
   lrwxrwxrwx 1 root root   9 Aug 18 17:02 9af2c5a3-bfc2-4ec1-85d9-
ebab850bb4a1 -> ../../sdb
```

6. Ajout d'une entrée dans /etc/fstab/ pour que le montage persiste entre les redémarrages à l'aide de l'UUID de /dev/sdb.

```
/etc/fstab
UUID=9af2c5a3-bfc2-4ec1-85d9-ebab850bb4a1 /var/lib/prometheus   ext4
defaults    0   0
```

Installez et configurez Prometheus

Lorsque le serveur est prêt, je peux commencer l'installation de Prometheus et configurer le service.

1. Extraire le pack d'installation Prometheus

```
tar xzf prometheus-2.38.0.linux-amd64.tar.gz
```

2. Copiez les binaires dans /usr/local/bin et modifiez la propriété de l'utilisateur prometheus créé précédemment

```
sudo cp prometheus-2.38.0.linux-amd64/{prometheus,promtool}
/usr/local/bin
sudo chown prometheus:prometheus /usr/local/bin/{prometheus,promtool}
```

3. Copiez les consoles et les bibliothèques dans /etc/prometheus

```
sudo cp -r prometheus-2.38.0.linux-amd64/{consoles,console_libraries}
/etc/prometheus/
```

4. Copiez le certificat client et les fichiers pem de clé privée téléchargés précédemment de StorageGRID vers /etc/prometheus/certs
5. Créez le fichier yaml de configuration prometheus

```
sudo nano /etc/prometheus/prometheus.yml
```

6. Insérez la configuration suivante. Le nom du travail peut être tout ce que vous souhaitez. Remplacez les « cibles : ['] » par le FQDN du nœud admin, et si vous avez modifié les noms des certificats et des fichiers de clé privée, mettez à jour la section tls_config pour qu'elle corresponde. enregistrez ensuite le fichier. Si votre interface de gestion de grille utilise un certificat auto-signé, téléchargez le certificat et placez-le avec un nom unique, et dans la section tls_config, ajoutez ca_file: /Etc/prometheus/cert/UIcert.pem

   a. Dans cet exemple, je collecterai tous les metrics commençant par alertManager, cassandra, nœud et StorageGRID. Vous trouverez plus d'informations sur les metrics Prometheus dans la "Documentation StorageGRID".

```
# my global config
global:
  scrape_interval: 60s # Set the scrape interval to every 15 seconds.
Default is every 1 minute.

scrape_configs:
  - job_name: 'StorageGRID'
    honor_labels: true
    scheme: https
    metrics_path: /federate
    scrape_interval: 60s
    scrape_timeout: 30s
    tls_config:
      cert_file: /etc/prometheus/cert/certificate.pem
      key_file: /etc/prometheus/cert/private_key.pem
    params:
      match[]:
        -
'{__name__=~"alertmanager_.*|cassandra_.*|node_.*|storagegrid_.*"}'
    static_configs:
    - targets: ['sgdemo-rtp.netapp.com:9091']
```

Si votre interface de gestion du grid utilise un certificat auto-signé, téléchargez le certificat et placez-le avec le certificat client portant un nom unique. Dans la section tls_config, ajoutez le certificat au-dessus du certificat client et des lignes de clé privée

```
        ca_file: /etc/prometheus/cert/UIcert.pem
```

1. Modifiez la propriété de tous les fichiers et répertoires dans /etc/prometheus et /var/lib/prometheus pour l'utilisateur prometheus

```
sudo chown -R prometheus:prometheus /etc/prometheus/
sudo chown -R prometheus:prometheus /var/lib/prometheus/
```

2. Créez un fichier de service prometheus dans /etc/systemd/system

```
sudo nano /etc/systemd/system/prometheus.service
```

3. Insérez les lignes suivantes, notez le --Storage.tsdb.rerétention=1A qui définit la conservation des données de mesure sur 1 an. Vous pouvez également utiliser --Storage.tsdb.Retention.size=300 Gio pour la conservation sur les limites de stockage. C'est le seul emplacement pour définir la conservation des métriques.

```
[Unit]
Description=Prometheus Time Series Collection and Processing Server
Wants=network-online.target
After=network-online.target

[Service]
User=prometheus
Group=prometheus
Type=simple
ExecStart=/usr/local/bin/prometheus \
        --config.file /etc/prometheus/prometheus.yml \
        --storage.tsdb.path /var/lib/prometheus/ \
        --storage.tsdb.retention.time=1y \
        --web.console.templates=/etc/prometheus/consoles \
        --web.console.libraries=/etc/prometheus/console_libraries

[Install]
WantedBy=multi-user.target
```

4. Rechargez le service systemd pour enregistrer le nouveau service prometheus. démarrez et activez ensuite le service prometheus.

```
sudo systemctl daemon-reload
sudo systemctl start prometheus
sudo systemctl enable prometheus
```

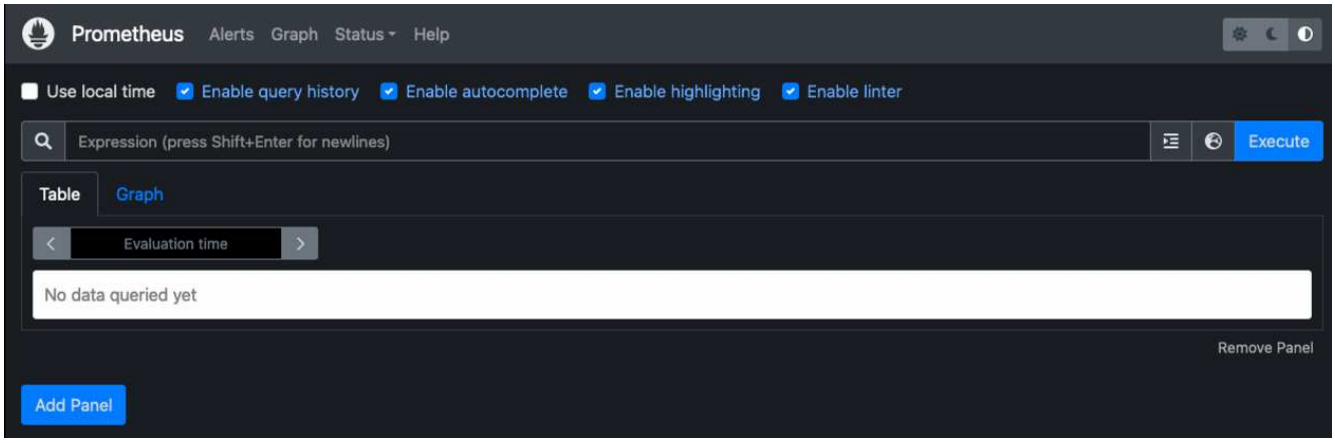
5. Vérifiez que l'entretien fonctionne correctement

```
sudo systemctl status prometheus
```

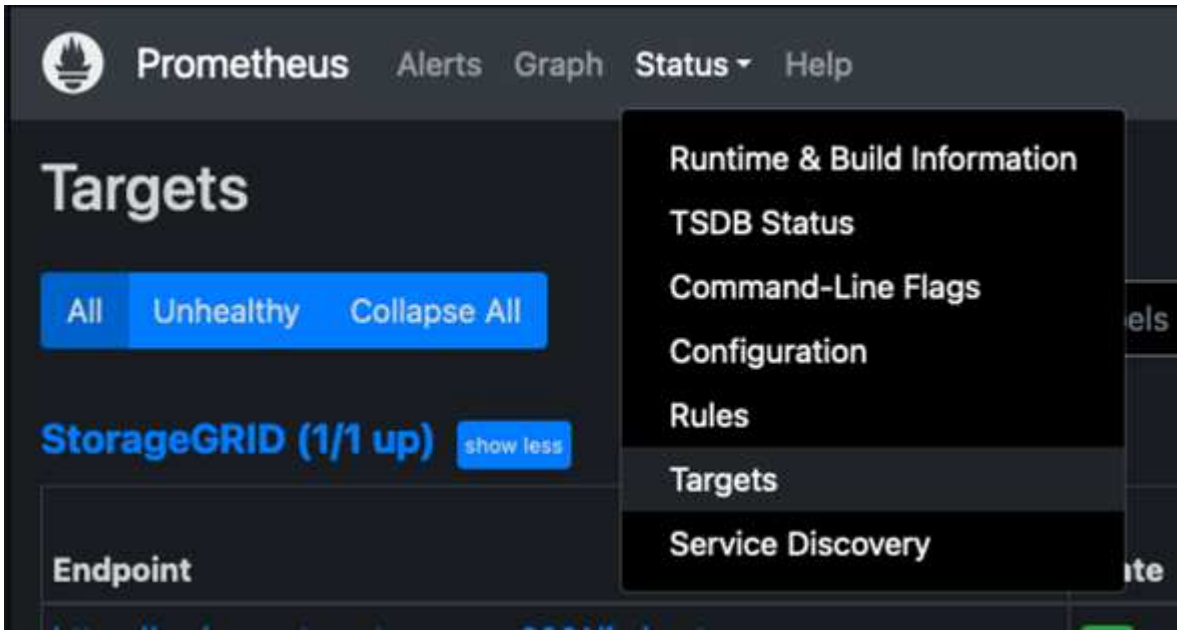
```
● prometheus.service - Prometheus Time Series Collection and Processing
Server
     Loaded: loaded (/etc/systemd/system/prometheus.service; enabled;
vendor preset: enabled)
     Active: active (running) since Mon 2022-08-22 15:14:24 EDT; 2s ago
```

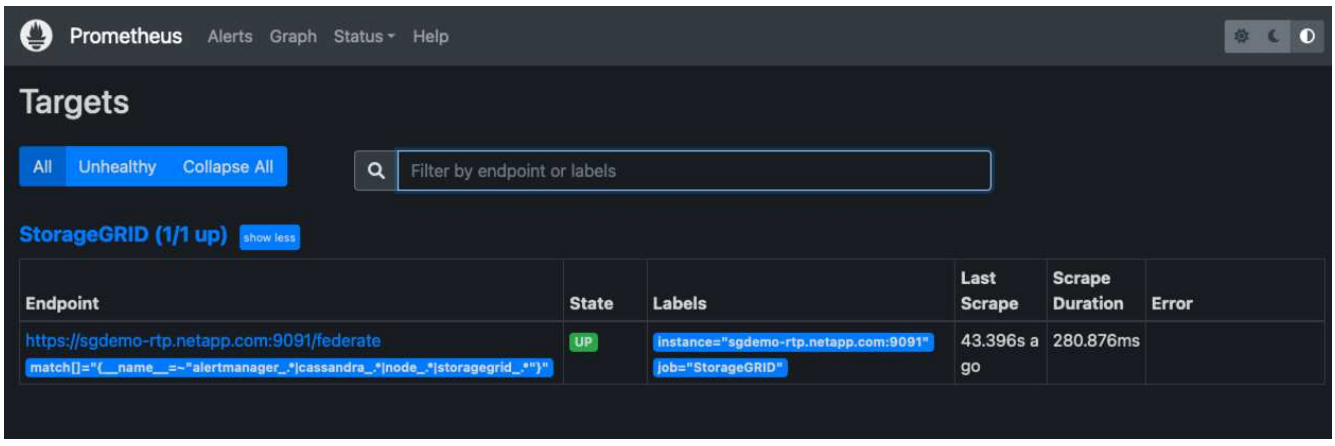
```
   Main PID: 6498 (prometheus)
      Tasks: 13 (limit: 28818)
     Memory: 107.7M
        CPU: 1.143s
     CGroup: /system.slice/prometheus.service
             └─6498 /usr/local/bin/prometheus --config.file
/etc/prometheus/prometheus.yml --storage.tsdb.path /var/lib/prometheus/
--web.console.templates=/etc/prometheus/consoles --web.con>

Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.510Z caller=head.go:544 level=info component=tsdb
msg="Replaying WAL, this may take a while"
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.816Z caller=head.go:615 level=info component=tsdb msg="WAL
segment loaded" segment=0 maxSegment=1
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.816Z caller=head.go:615 level=info component=tsdb msg="WAL
segment loaded" segment=1 maxSegment=1
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.816Z caller=head.go:621 level=info component=tsdb msg="WAL
replay completed" checkpoint_replay_duration=55.57µs wal_rep>
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.831Z caller=main.go:997 level=info fs_type=EXT4_SUPER_MAGIC
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.831Z caller=main.go:1000 level=info msg="TSDB started"
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.831Z caller=main.go:1181 level=info msg="Loading
configuration file" filename=/etc/prometheus/prometheus.yml
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.832Z caller=main.go:1218 level=info msg="Completed loading
of configuration file" filename=/etc/prometheus/prometheus.y>
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.832Z caller=main.go:961 level=info msg="Server is ready to
receive web requests."
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.832Z caller=manager.go:941 level=info component="rule
manager" msg="Starting rule manager..."
```

6. Vous devriez maintenant pouvoir accéder à l'interface utilisateur de votre serveur Prometheus à l'adresse http://<prometheus-server-ip>:9090 et voir l'interface utilisateur

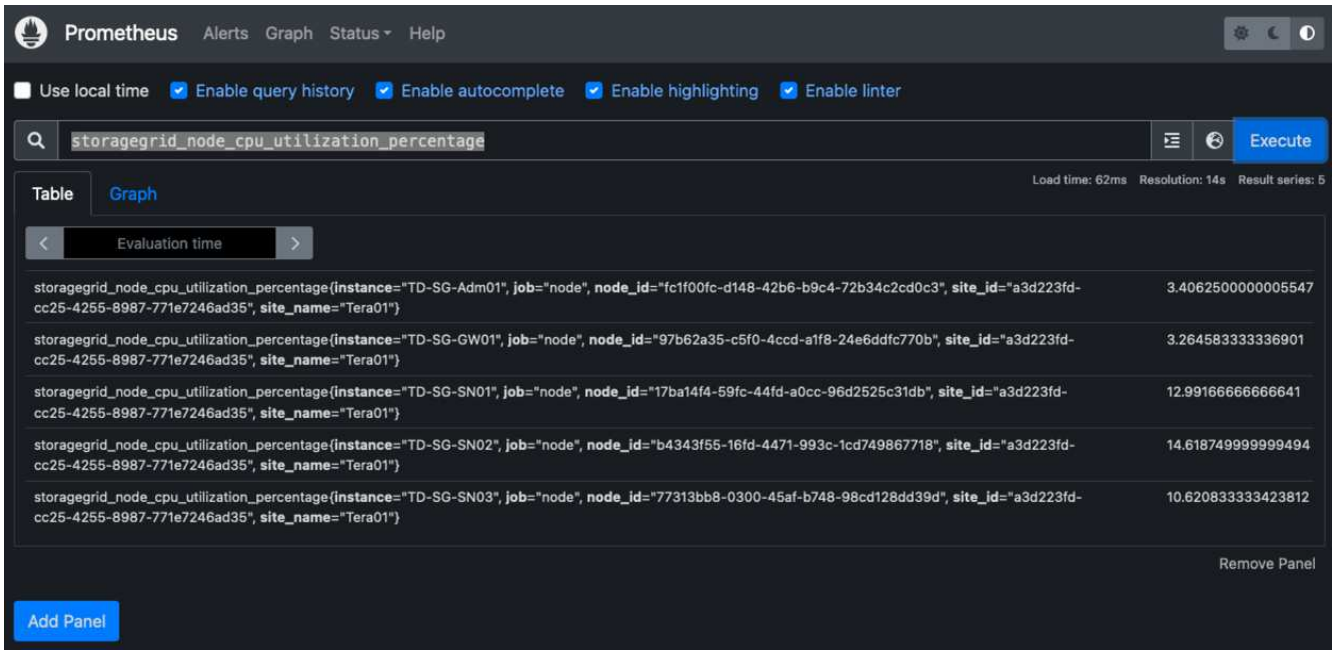


7. Sous cibles « Status », vous pouvez consulter le statut du noeud final StorageGRID configuré dans prometheus.yml





8. Sur la page graphique, vous pouvez exécuter une requête de test et vérifier que les données sont scrapées avec succès. Par exemple, entrez « storagegrid_node_cpu_usage_percent » dans la barre de requêtes et cliquez sur le bouton Exécuter.



Installer et configurer Grafana

Vous pouvez désormais installer Grafana et configurer un tableau de bord

Grafana Installation

1. Installez la dernière édition Enterprise de Grafana

```
sudo apt-get install -y apt-transport-https
sudo apt-get install -y software-properties-common wget
sudo wget -q -O /usr/share/keyrings/grafana.key
https://packages.grafana.com/gpg.key
```

2. Ajouter ce référentiel pour les versions stables :

```
echo "deb [signed-by=/usr/share/keyrings/grafana.key]
https://packages.grafana.com/enterprise/deb stable main" | sudo tee -a
/etc/apt/sources.list.d/grafana.list
```

3. Après avoir ajouté le référentiel.

```
sudo apt-get update
sudo apt-get install grafana-enterprise
```

4. Rechargez le service systemd pour enregistrer le nouveau service grafana. Démarrez et activez ensuite le service Grafana.

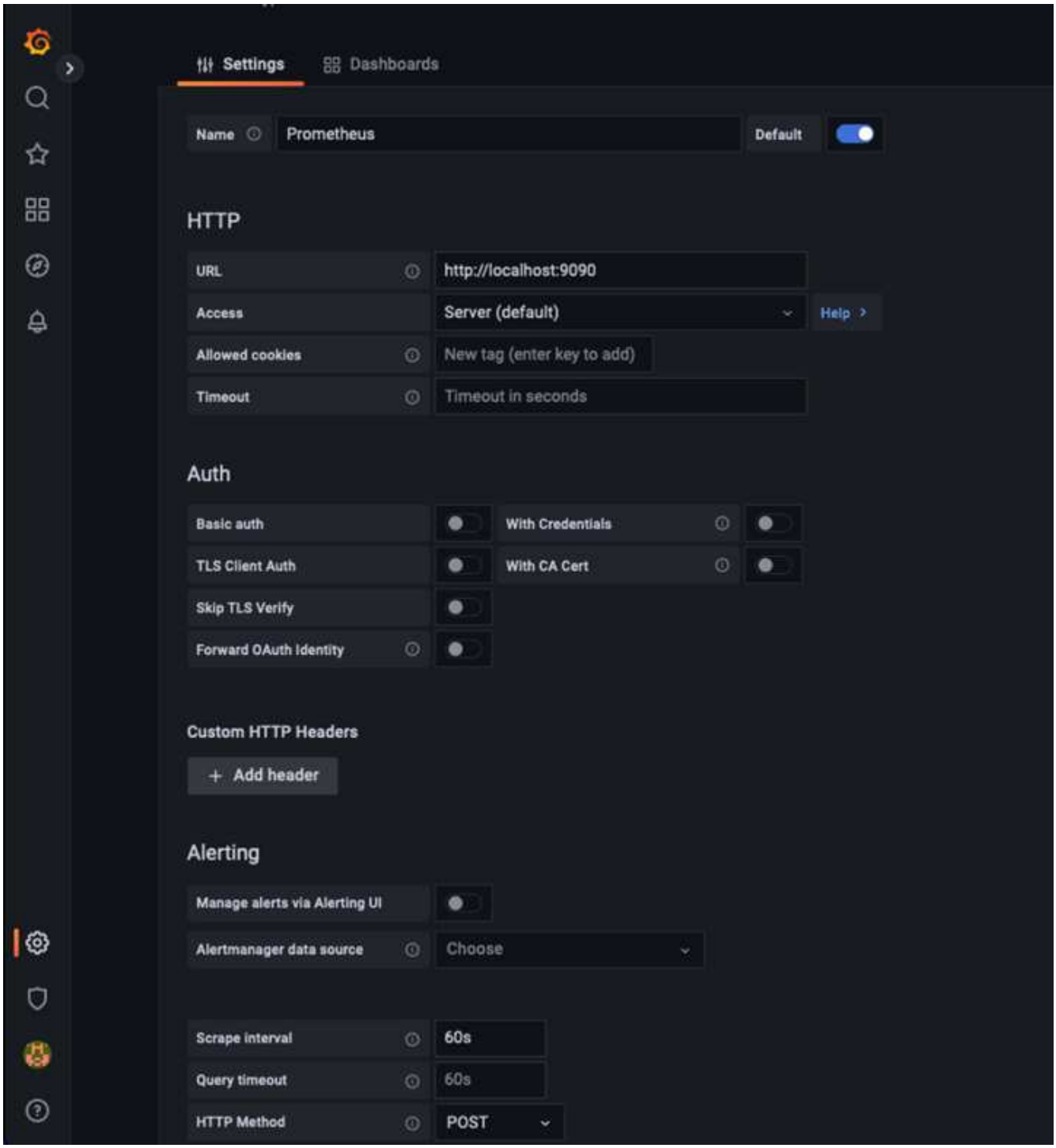
```
sudo systemctl daemon-reload
sudo systemctl start grafana-server
sudo systemctl enable grafana-server.service
```

5. Grafana est maintenant installé et en cours d'exécution. Lorsque vous ouvrez un navigateur à l'adresse http://<prometheus-server-ip>:3000, la page de connexion de Grafana s'affiche.
6. Les informations d'identification par défaut sont admin/admin et vous devez définir un nouveau mot de passe à mesure qu'il vous invite à.

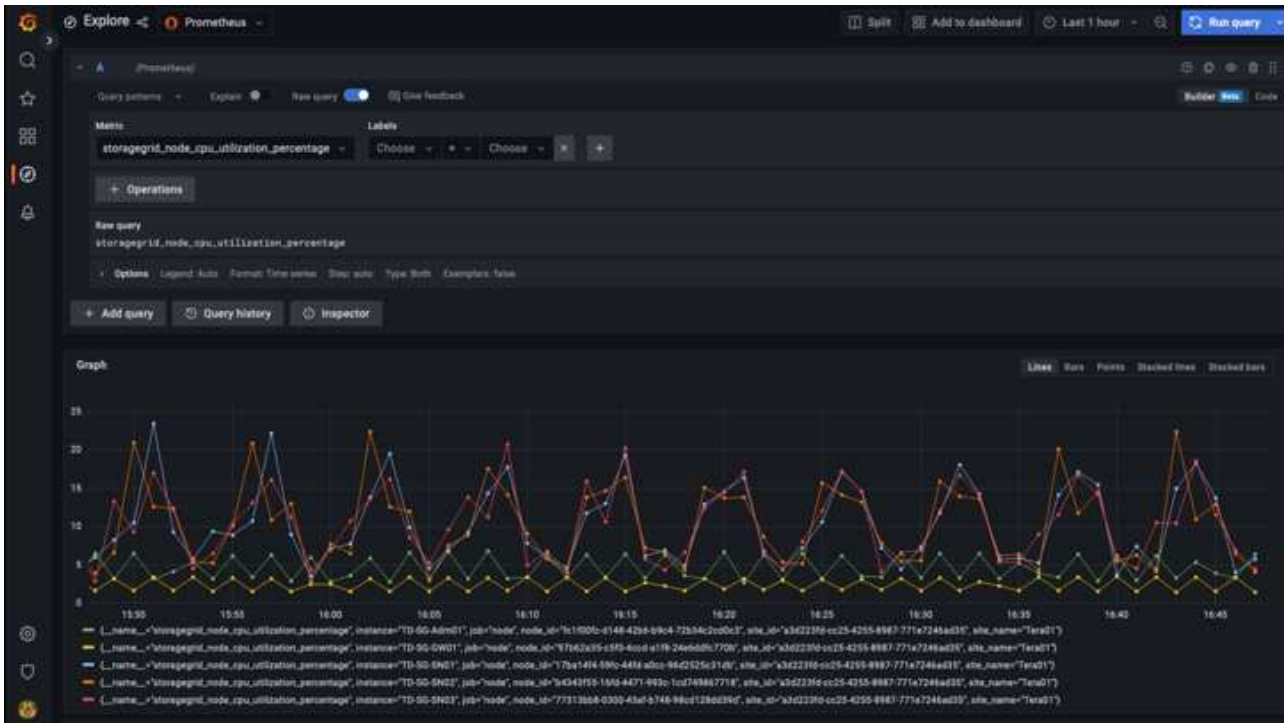
Créez un tableau de bord Grafana pour StorageGRID

Lorsque vous installez et exécutez Grafana et Prometheus, vous pouvez désormais vous connecter en créant une source de données et en créant un tableau de bord

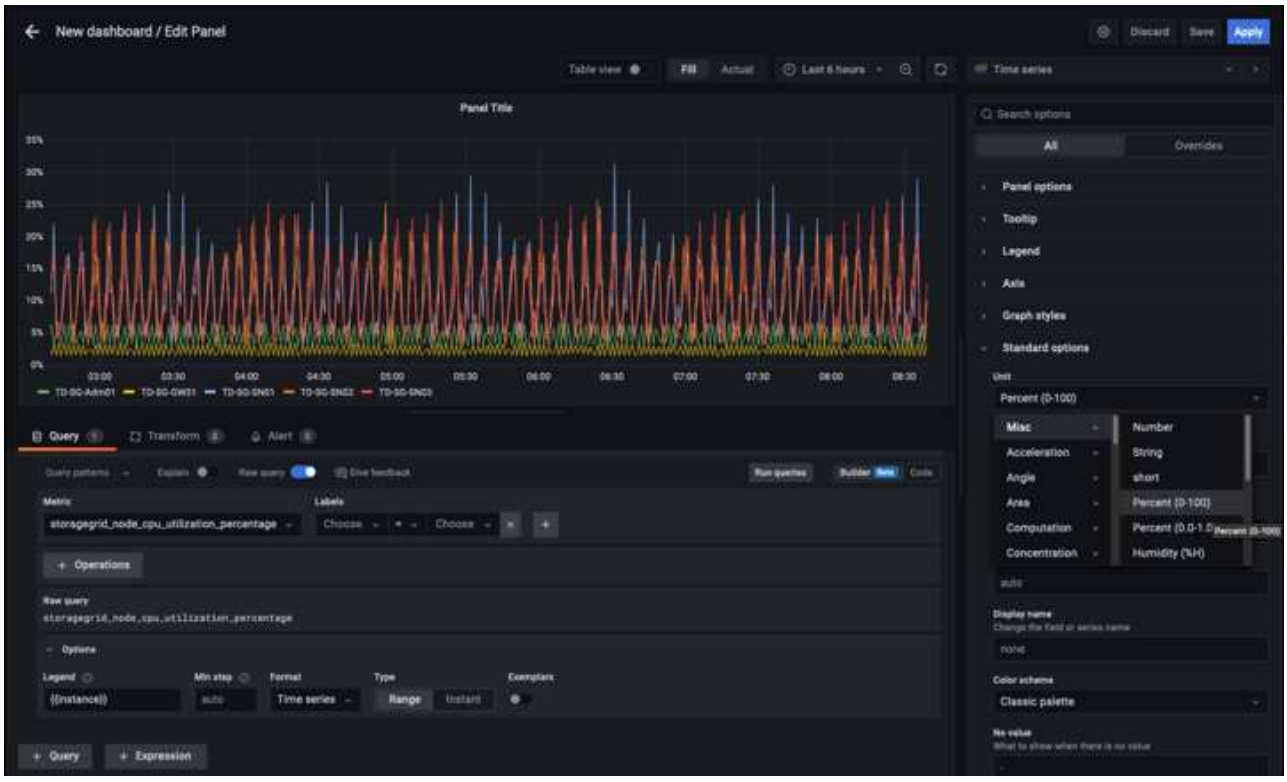
1. Dans le volet de gauche, développez « Configuration » et sélectionnez « sources de données », puis cliquez sur le bouton « Ajouter une source de données »
2. Prometheus est une des principales sources de données. Si ce n'est pas le cas, utilisez la barre de recherche pour trouver Prometheus
3. Configurez la source Prometheus en entrant l'URL de l'instance prometheus et l'intervalle de récupération en fonction de l'intervalle Prometheus. J'ai également désactivé la section d'alertes car je n'ai pas configuré le gestionnaire d'alertes sur prometheus.



4. Une fois les paramètres souhaités saisis, faites défiler l'écran vers le bas et cliquez sur « Enregistrer et tester ».
5. Une fois le test de configuration réussi, cliquez sur le bouton Explorer.
    a. Dans la fenêtre d'exploration, vous pouvez utiliser la même mesure que Prometheus testée avec « storagegrid_node_cpu_use_percent », puis cliquez sur le bouton Run Query



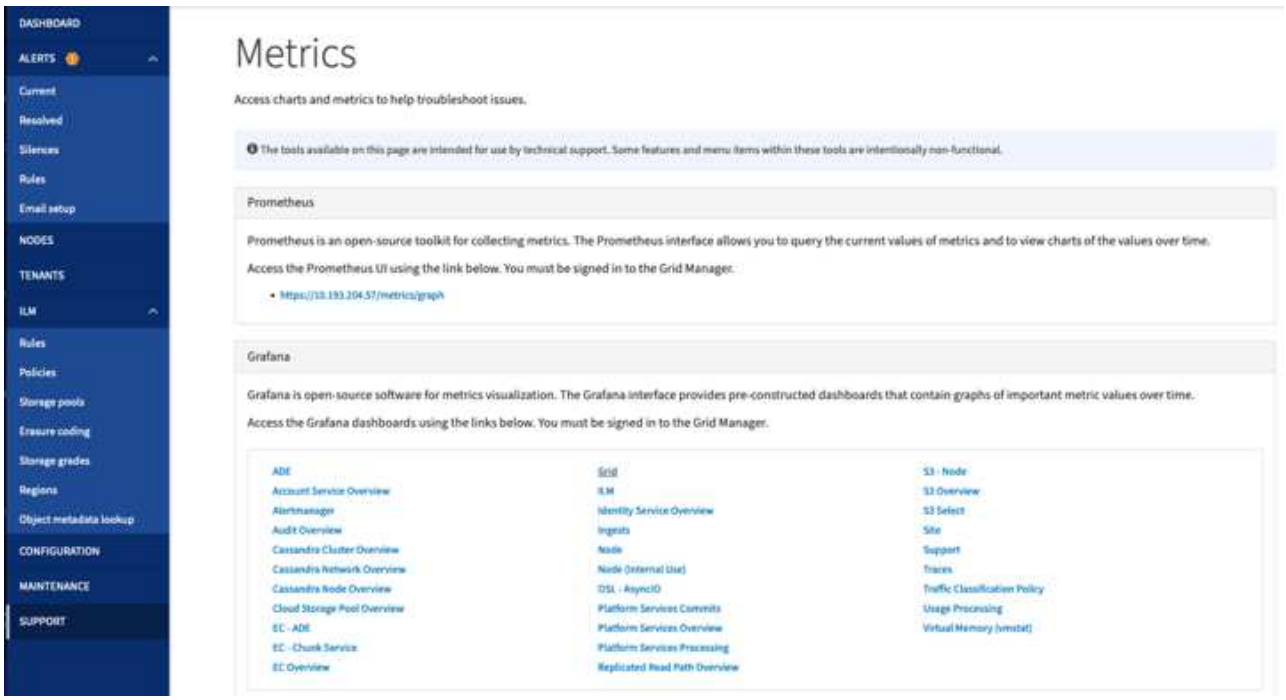
6. Comme la source de données est configurée, nous pouvons créer un tableau de bord.
   a. Dans le volet de gauche, développez « tableaux de bord » et sélectionnez « + nouveau tableau de bord ».
   b. Sélectionnez « Ajouter un nouveau panneau »
   c. Configurez le nouveau panneau en sélectionnant une mesure, puis j'utiliserai à nouveau « storagegrid_node_cpu_use_percentage », saisissez un titre pour le panneau, développez « Options » en bas et pour changer de légende en personnalisé et entrez «{{instance} » pour définir les noms de nœud, et à droite sous « Options standard » définissez « unité » sur « 100 % ». Cliquez ensuite sur « appliquer » pour enregistrer le panneau dans le tableau de bord.



7. Nous pouvons continuer à concevoir notre tableau de bord de ce type pour chaque metric souhaité, mais heureusement que StorageGRID dispose déjà de tableaux de bord avec des panneaux que nous pouvons copier dans nos tableaux de bord personnalisés.

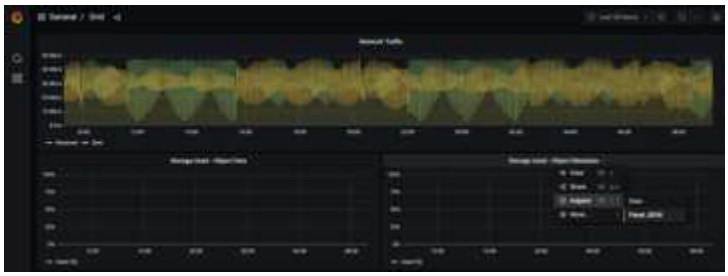
   a. Dans le volet gauche de l'interface de gestion StorageGRID, sélectionnez « support », et en bas de la colonne « Outils », cliquez sur métriques.

   b. Dans les mesures, je vais sélectionner le lien « grille » en haut de la colonne centrale.



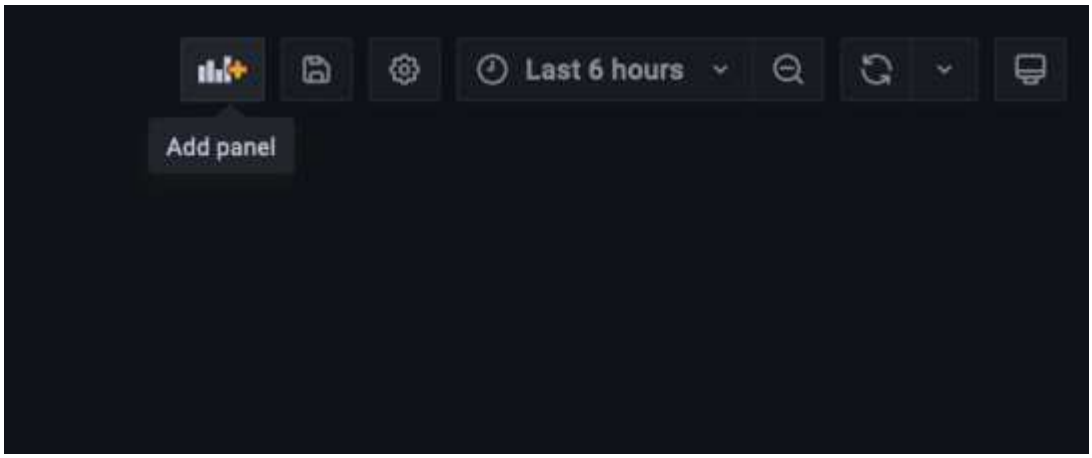
   c. Dans le tableau de bord Grid, sélectionnez le panneau « stockage utilisé - métadonnées de l'objet ».

Cliquez sur la petite flèche vers le bas et sur la fin du titre du panneau pour faire descendre un menu. Dans ce menu, sélectionnez « inspection » et « panneau JSON ».



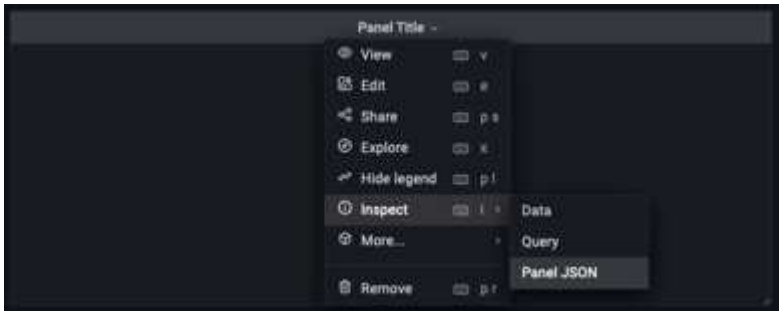
d. Copiez le code JSON et fermez la fenêtre.

e. Dans notre nouveau tableau de bord, cliquez sur l'icône pour ajouter un nouveau panneau.

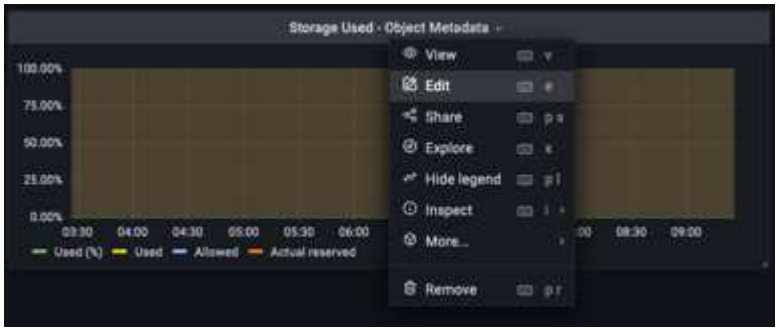


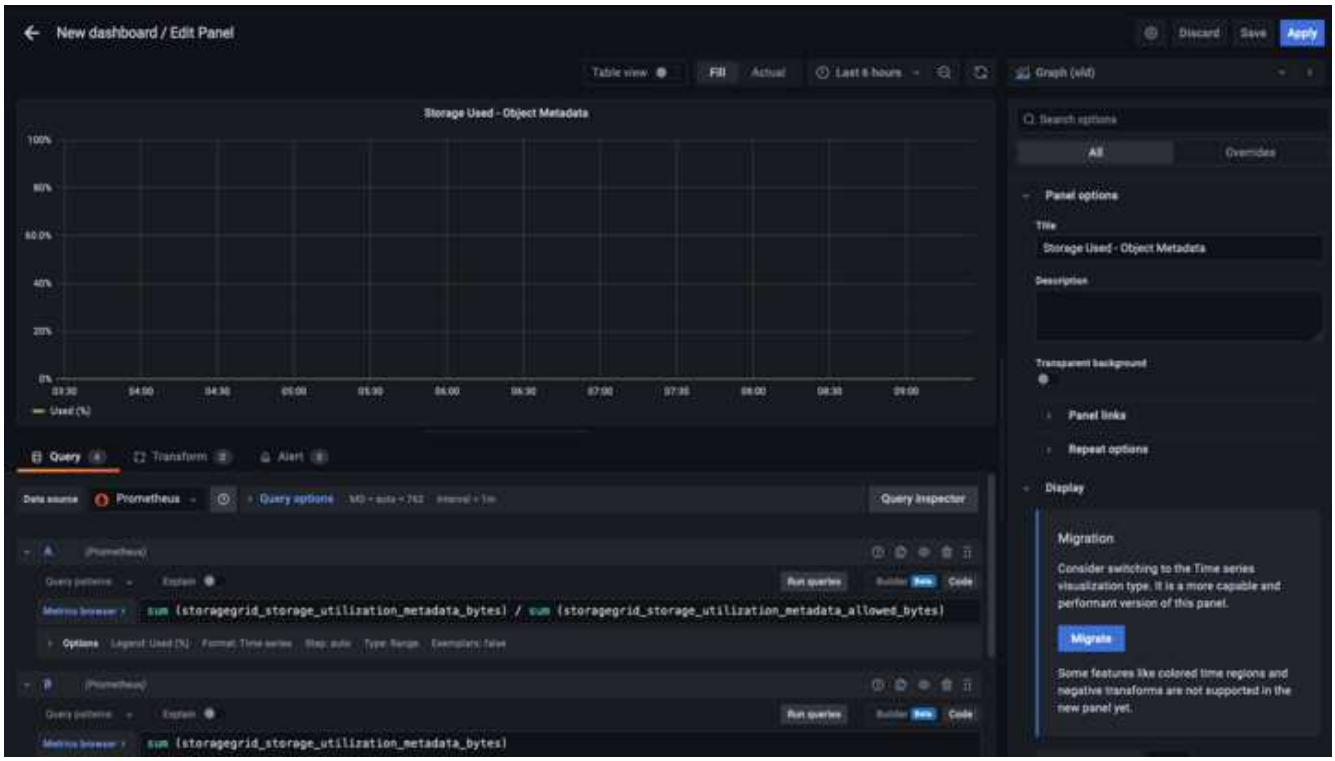
f. Appliquez le nouveau panneau sans apporter de modifications

g. Inspecter le fichier JSON, et tout comme dans le panneau StorageGRID. Supprimez tout code JSON et remplacez-le par le code copié du panneau StorageGRID.



h. Modifiez le nouveau panneau et, à droite, un message migration s'affiche avec un bouton « migrer ». Cliquez sur le bouton, puis sur le bouton « appliquer ».





8. Une fois tous les panneaux en place et configurés comme vous le souhaitez. Enregistrez le tableau de bord en cliquant sur l'icône du disque dans le coin supérieur droit et donnez un nom à votre tableau de bord.

Conclusion

Nous disposons désormais d'un serveur Prometheus avec une capacité de stockage et de conservation des données personnalisables. Grâce à cela, nous pouvons continuer à élaborer nos propres tableaux de bord avec les mesures les plus pertinentes pour nos opérations. Vous pouvez obtenir plus d'informations sur les metrics Prometheus collectés dans la "Documentation StorageGRID".

Utilisez F5 DNS pour équilibrer la charge globale de StorageGRID.

Par Steve Gorman (F5)

Ce rapport technique fournit des instructions détaillées pour configurer NetApp StorageGRID avec les services DNS F5 pour l'équilibrage de charge global afin d'offrir une meilleure disponibilité des données, une plus grande cohérence des données et d'optimiser le routage des transactions S3 lorsque votre grille est distribuée sur plusieurs sites et/ou groupes HA.

Introduction

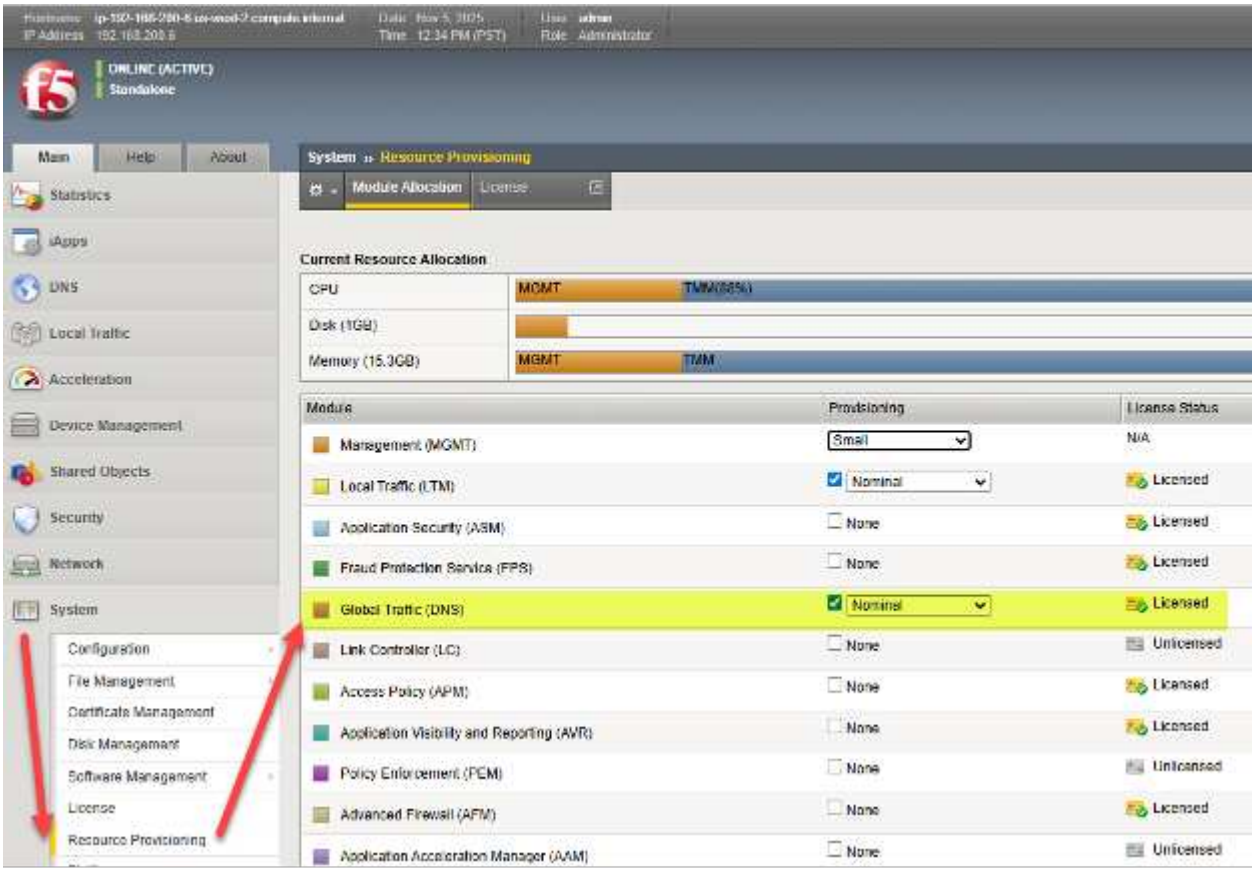
La solution F5 BIG-IP DNS, anciennement appelée BIG-IP GTM (Global Traffic Manager) et GSLB (Global Server Load Balancing), permet un accès transparent à travers plusieurs groupes HA actifs-actifs et des solutions StorageGRID multisites actives-actives.

Configuration F5 BIG-IP StorageGRID multisite

Quel que soit le nombre de sites StorageGRID à prendre en charge, au moins deux appliances BIG-IP, physiques ou virtuelles, doivent avoir le module DNS BIG-IP activé et configuré. Plus une entreprise dispose de serveurs DNS, plus son degré de redondance sera élevé.

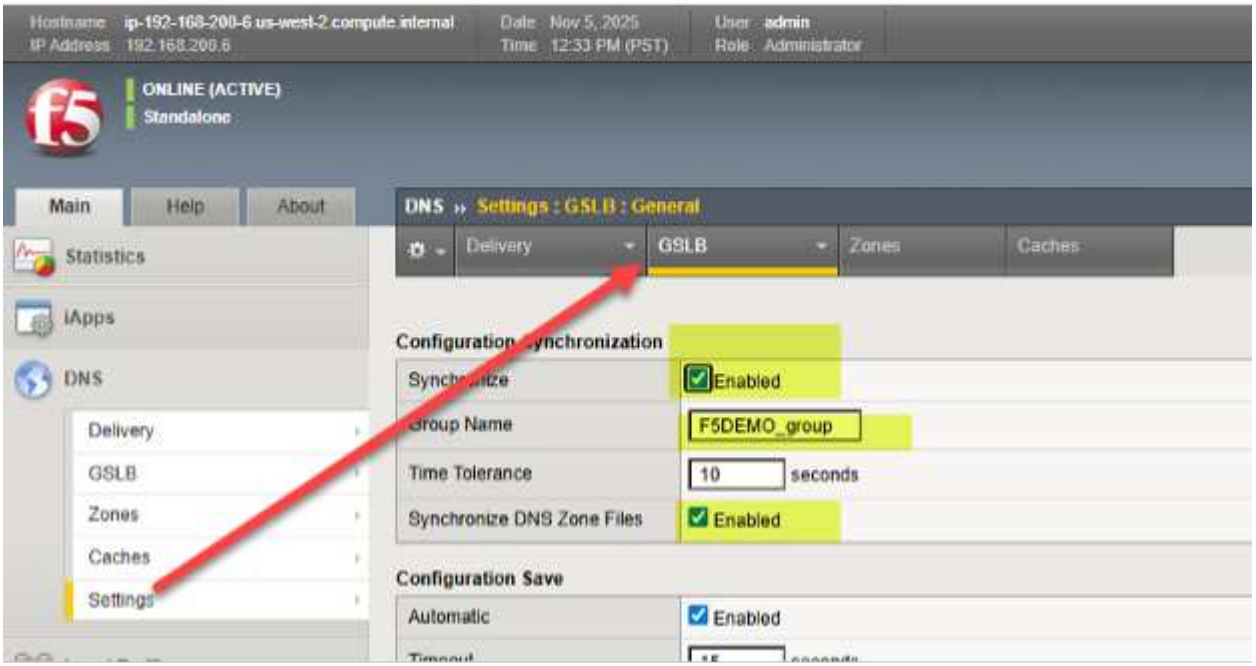
BIG-IP DNS - Premiers pas de la configuration initiale

Une fois que l'appliance BIG-IP a subi au moins la configuration initiale, utilisez un navigateur Web pour vous connecter à l'interface TMUI (interface graphique BIG-IP) et choisissez Système → Provisionnement des ressources. Comme indiqué, assurez-vous que le module « Trafic global (DNS) » est coché et qu'il est bien sous licence. Notez, comme sur l'image, qu'il est courant que le « trafic local (LTM) » puisse être provisionné sur le même appareil.

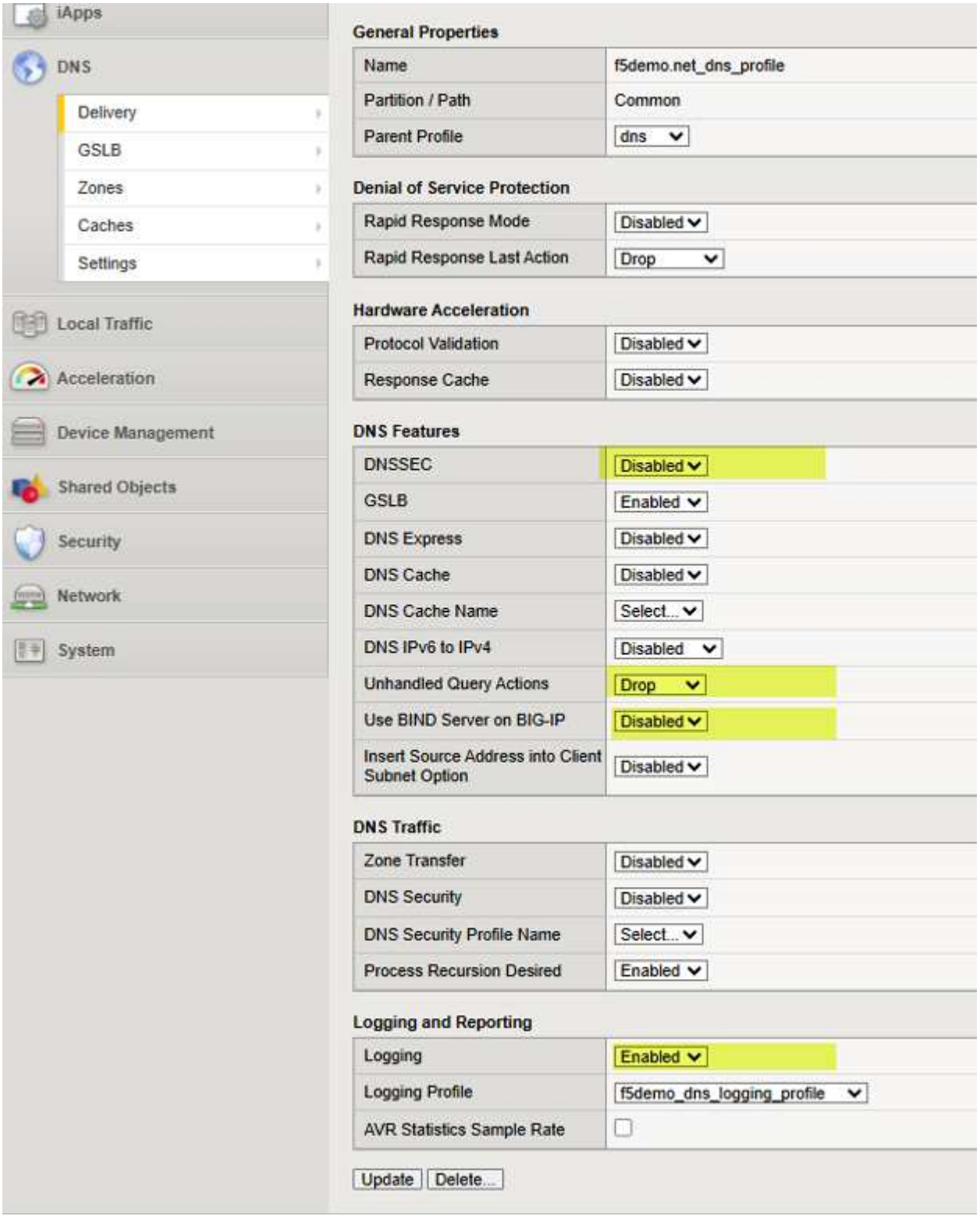


Configurer les éléments fondamentaux du protocole DNS

La première étape vers la gestion du trafic global pour les sites StorageGRID consiste à choisir l'onglet DNS, où sera configurée la quasi-totalité du routage du trafic global, puis à sélectionner Paramètres → GLSB. Activez les deux options de synchronisation et choisissez un nom de groupe DNS qui sera partagé entre les appliances BIG-IP participantes.



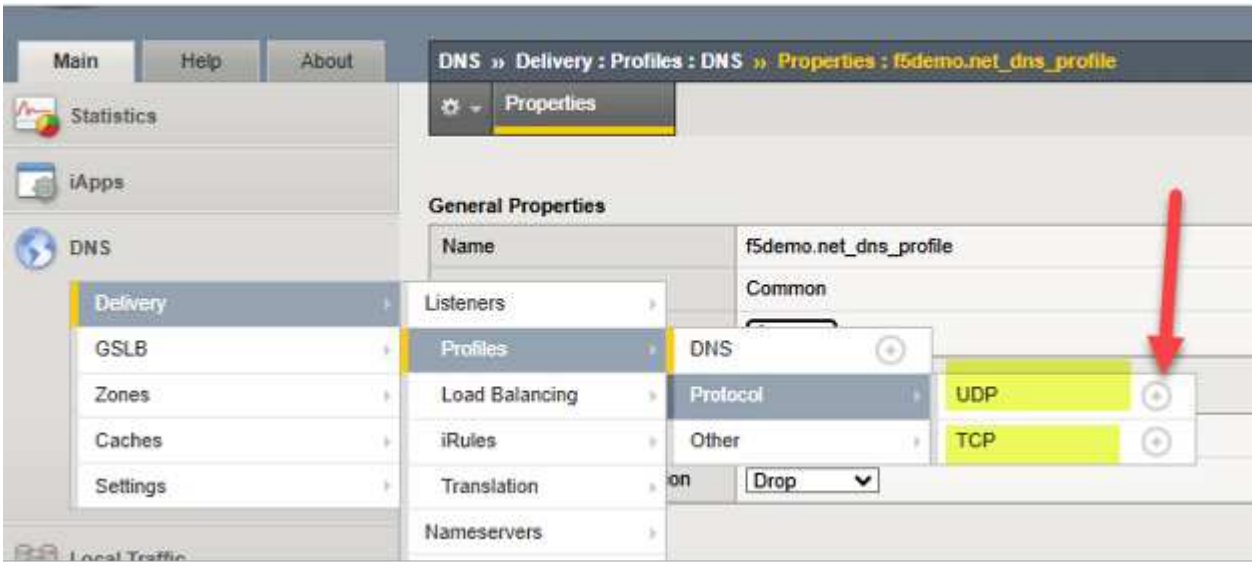
Ensuite, accédez à DNS > Distribution > Profils > DNS : Créer et créez un profil qui gérera les fonctionnalités DNS que vous souhaitez activer ou désactiver. Consultez le lien précédent pour accéder au guide pédagogique DNS si la génération de journaux DNS spécifiques vous intéresse. Voici un exemple de profil DNS fonctionnel ; notez les quatre éléments mis en évidence qui représentent des paramètres importants. Pour plus d'informations, chaque configuration possible est expliquée dans l'article suivant de la base de connaissances F5. "ici".



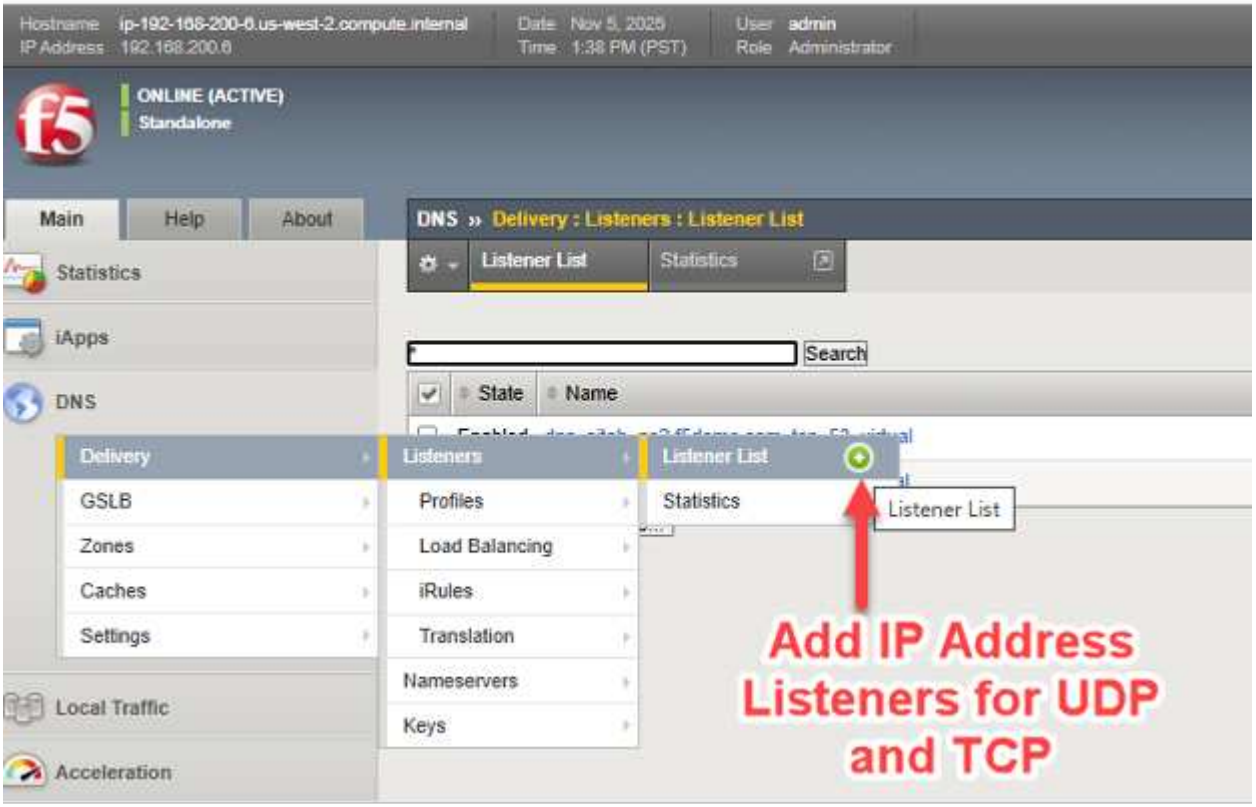
À ce stade, nous pouvons ajuster les caractéristiques des protocoles UDP et TCP, grâce à des « profils » créés, qui peuvent tous deux transporter du trafic DNS impliquant BIG-IP. Il suffit de créer un nouveau profil pour UDP et TCP. Partant du principe que le trafic DNS transitera par des liaisons WAN, une bonne pratique consiste simplement à hériter des caractéristiques UDP et TCP reconnues pour leurs bonnes performances dans les environnements WAN. Pour ajouter chaque protocole, cliquez simplement sur l'icône « + » située à côté de celui-ci, puis définissez le profil parent comme suit :

UDP → utiliser le profil « parent » « udp_gtm_dns »

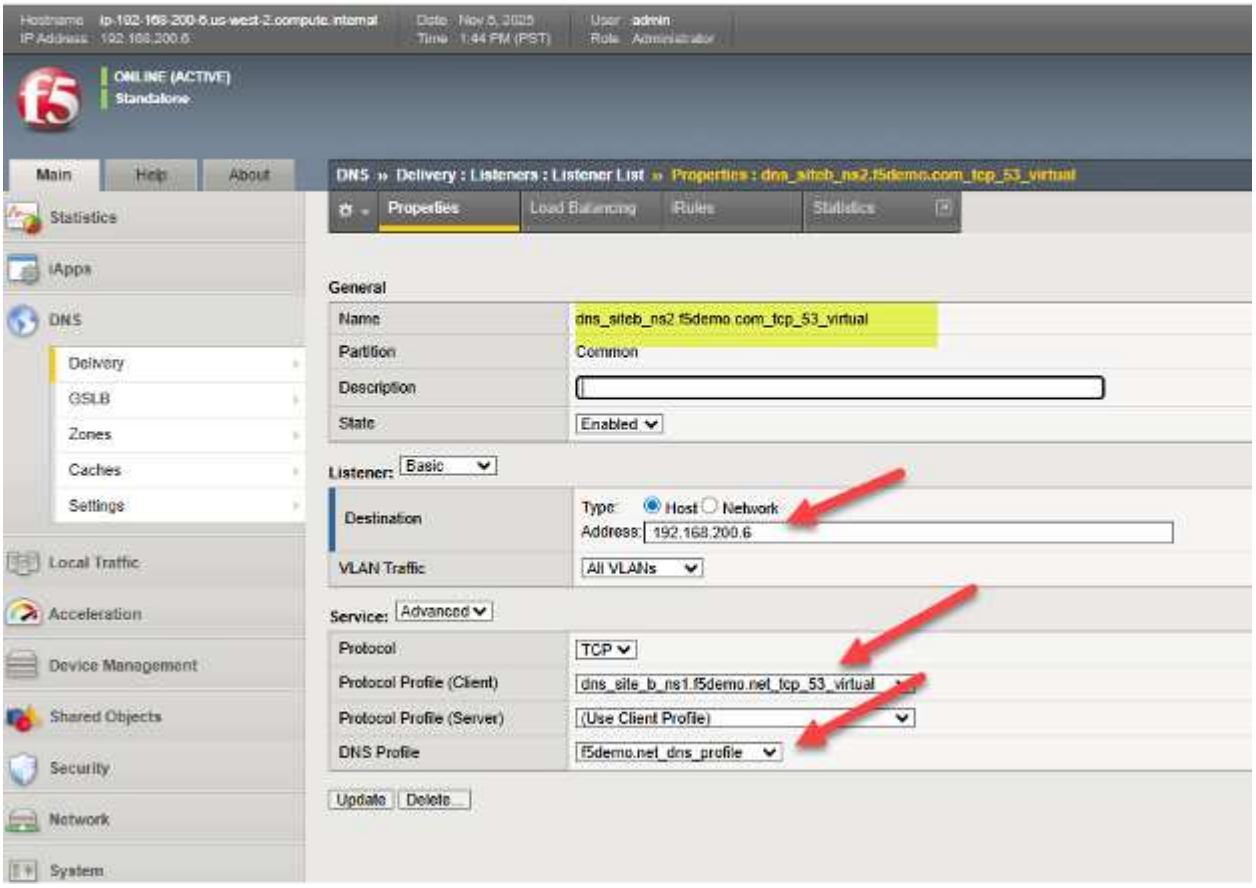
TCP → utiliser le profil « parent » « f5-tcp-wan »



Il nous suffit maintenant d'attribuer une adresse IP au trafic UDP et TCP impliquant le DNS BIG-IP. Pour ceux qui connaissent BIG-IP LTM, il s'agit essentiellement de la création de serveurs virtuels DNS, et les serveurs virtuels ont besoin d'adresses IP « d'écoute ». Comme indiqué dans la capture d'écran, suivez les flèches pour créer des serveurs d'écoute/virtuels pour DNS/UDP et DNS/TCP.



Voici un exemple tiré d'un serveur DNS BIG-IP en production ; on y voit les paramètres d'écoute du serveur virtuel TCP et on peut constater comment ils relient plusieurs des étapes précédentes. Cela inclut la référence au profil DNS et au profil de protocole (TCP), ainsi que la configuration d'une adresse IP valide que le DNS pourra utiliser. Comme pour tous les objets créés avec BIG-IP, il est utile d'utiliser un nom significatif qui permette d'identifier l'objet, comme dns/siteb/TCP53 dans l'exemple donné.



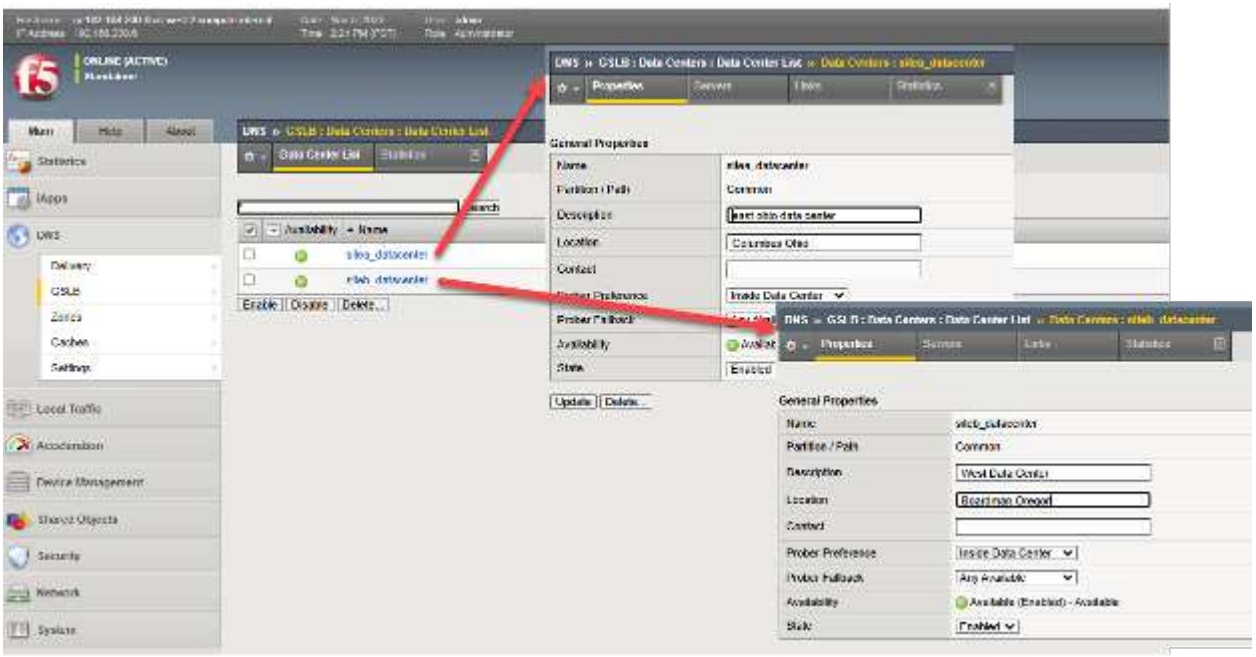
Ceci conclut les étapes préliminaires, généralement « uniques », de configuration d'un dispositif BIG-IP avec le module DNS activé. Nous sommes maintenant prêts à aborder les détails de la mise en place d'une solution globale de gestion du trafic avec nos appliances, qui sera bien sûr liée aux caractéristiques des sites StorageGRID .

Mise en place de sites de centres de données et établissement de communications inter-BIG-IP en quatre étapes

Première étape : Créer des centres de données

Chaque site qui hébergera des groupes de nœuds à équilibrer localement la charge par BIG-IP LTM doit être enregistré dans le DNS BIG-IP. Cette opération ne doit être effectuée que sur un seul serveur DNS BIG-IP, car nous créons un groupe DNS synchronisé pour la gestion du trafic ; cette configuration sera donc partagée entre les membres DNS du groupe.

Dans l'interface graphique TMUI, sélectionnez DNS > GSLB > Centres de données > Liste des centres de données et créez une entrée pour chacun des sites StorageGRID . Si vous utilisez une configuration réseau alignée sur la figure 1, un dispositif DNS situé sur d'autres sites non StorageGRID , ajoutez des centres de données pour ces sites en plus des sites de stockage. Dans cet exemple, les sites a et b sont créés dans l'Ohio et l'Oregon, les BIG-IP sont des appliances double DNS et LTM.



Deuxième étape : Créer des serveurs (Liste de tous les équipements BIG-IP de la solution)

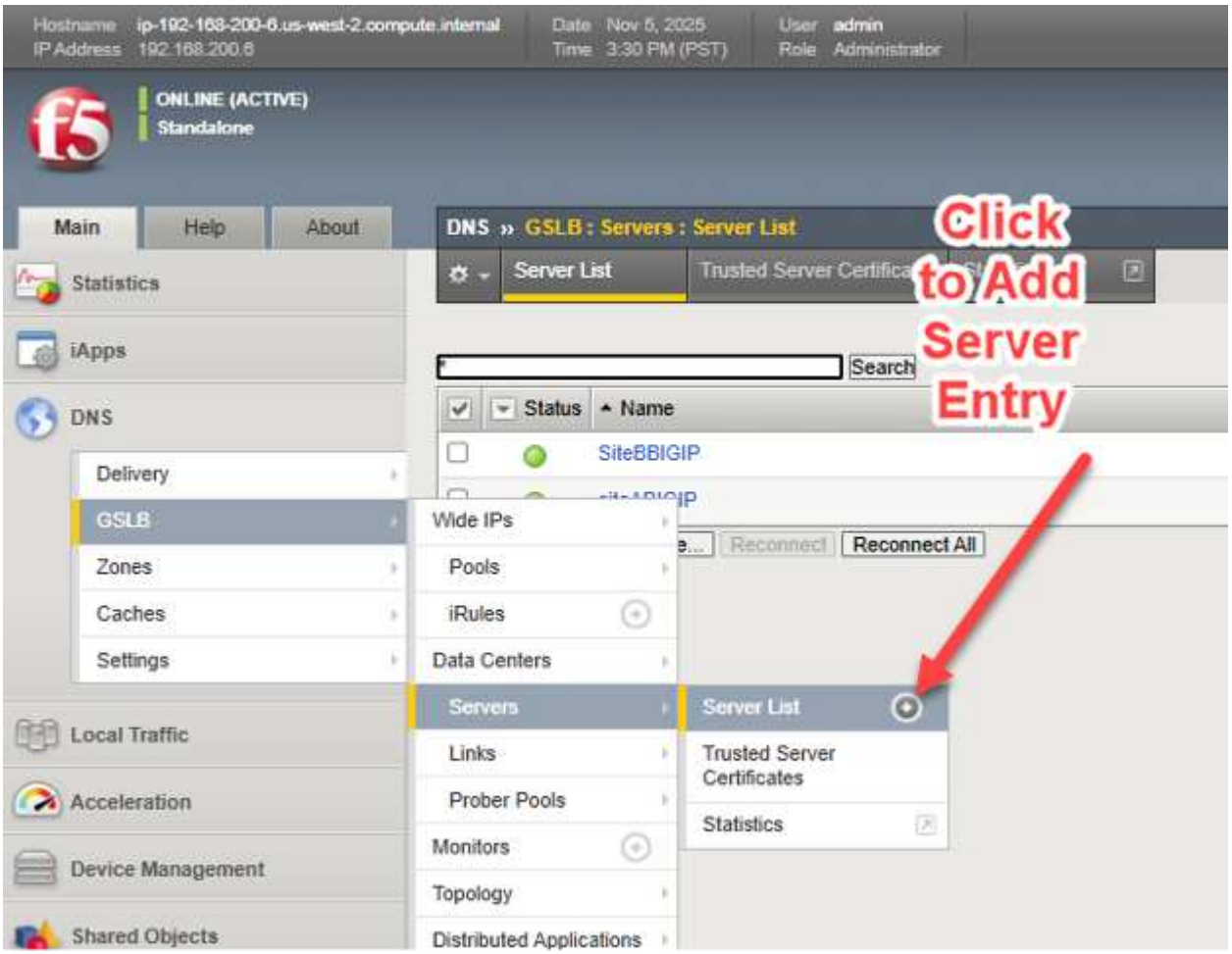
Nous sommes maintenant prêts à connecter les clusters de sites StorageGRID individuels à la configuration DNS BIG-IP. Rappelons que le dispositif BIG-IP de chaque site effectuera l'équilibrage de charge réel du trafic S3, grâce à la configuration de serveurs virtuels qui lient une adresse IP/port accessible « front-end » à un ensemble de « pool » de dispositifs Storage Node « back-end », en utilisant des adresses IP/ports « back-end ».

Si, par exemple, tous les nœuds de stockage d'un pool sont mis hors ligne administrativement, peut-être pour la mise hors service d'un site, ou de manière inattendue suite à des contrôles d'intégrité en temps réel ayant échoué, le trafic sera dirigé vers d'autres sites en modifiant les réponses aux requêtes DNS.

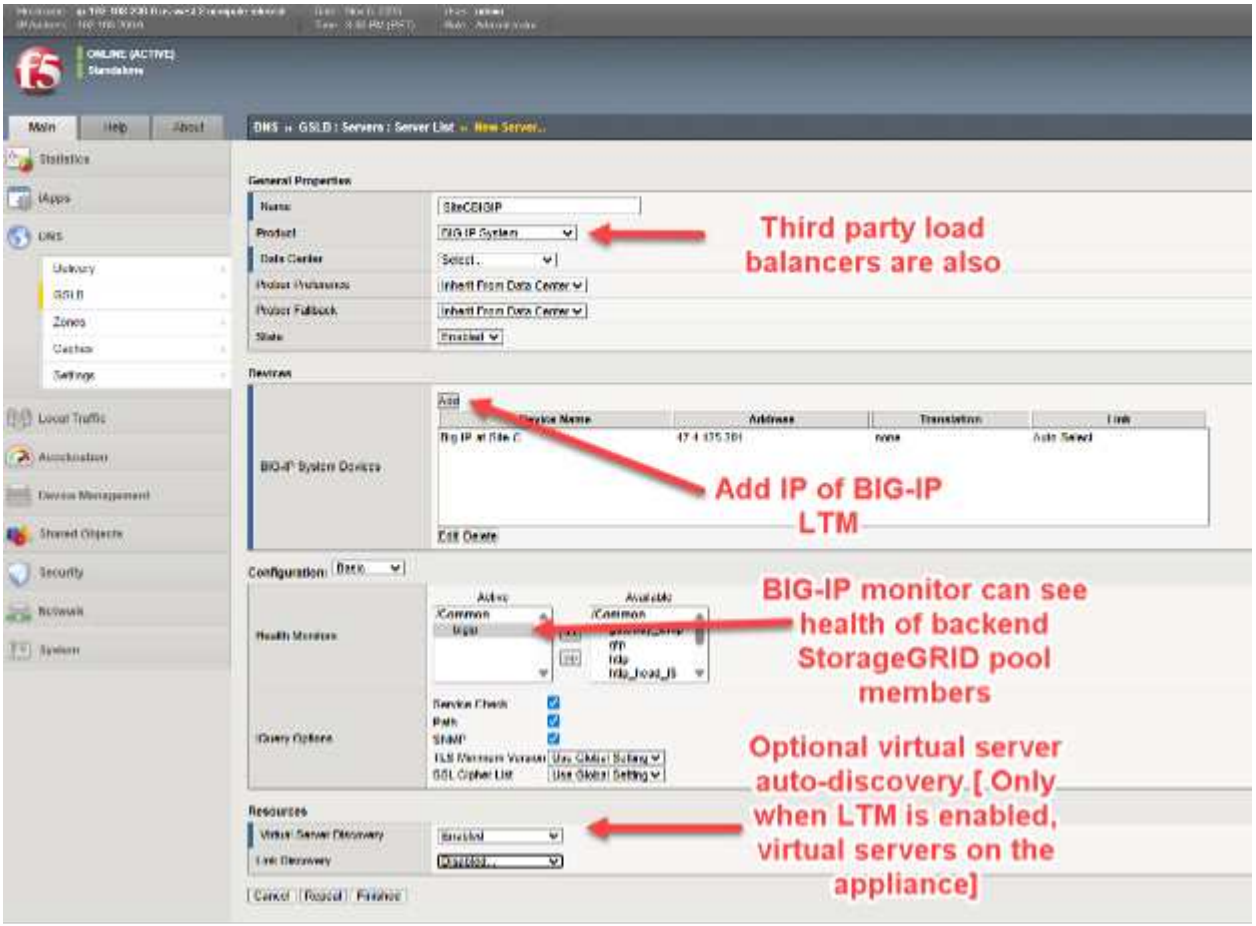
Pour intégrer les sites StorageGrid, et plus précisément les serveurs virtuels locaux, à la configuration DNS BIG-IP sur chaque appliance, la configuration n'est nécessaire qu'une seule fois. L'ensemble des appliances DNS BIG-IP seront configurées dans une prochaine étape.

En termes simples, nous allons créer une liste, appelée liste de serveurs, de tous nos équipements BIG-IP, qu'ils soient sous licence pour DNS, LTM ou les deux (DNS et LTM). Cette liste principale sera synchronisée avec tous les équipements DNS BIG-IP une fois la liste complétée.

Sur un appareil BIG-IP DNS sous licence, choisissez DNS > GSLB > Serveurs > Liste des serveurs et choisissez le bouton ajouter (+).



Les quatre éléments clés lors de l'ajout de chaque BIG-IP sont les suivants : * Sélectionner BIG-IP dans le menu déroulant des produits ; d'autres équilibreurs de charge sont possibles, mais ils manquent généralement de réactivité en temps réel lorsque l'état des nœuds backend se détériore sur chaque site. Ajoutez l'adresse IP du serveur DNS BIG-IP. Lors du premier ajout d'un serveur DNS BIG-IP, l'adresse sera probablement celle du serveur accessible via l'interface graphique ; pour les serveurs suivants, il s'agira des autres serveurs de la solution. * Choisissez un moniteur d'intégrité, utilisez toujours « BIG-IP » lorsque l'équilibreur de charge ajouté est un dispositif BIG-IP, pour tenir compte de l'intégrité du nœud StorageGRID en arrière-plan. * En option, demandez la découverte automatique du serveur virtuel si l'appliance est une appliance double DNS/LTM.

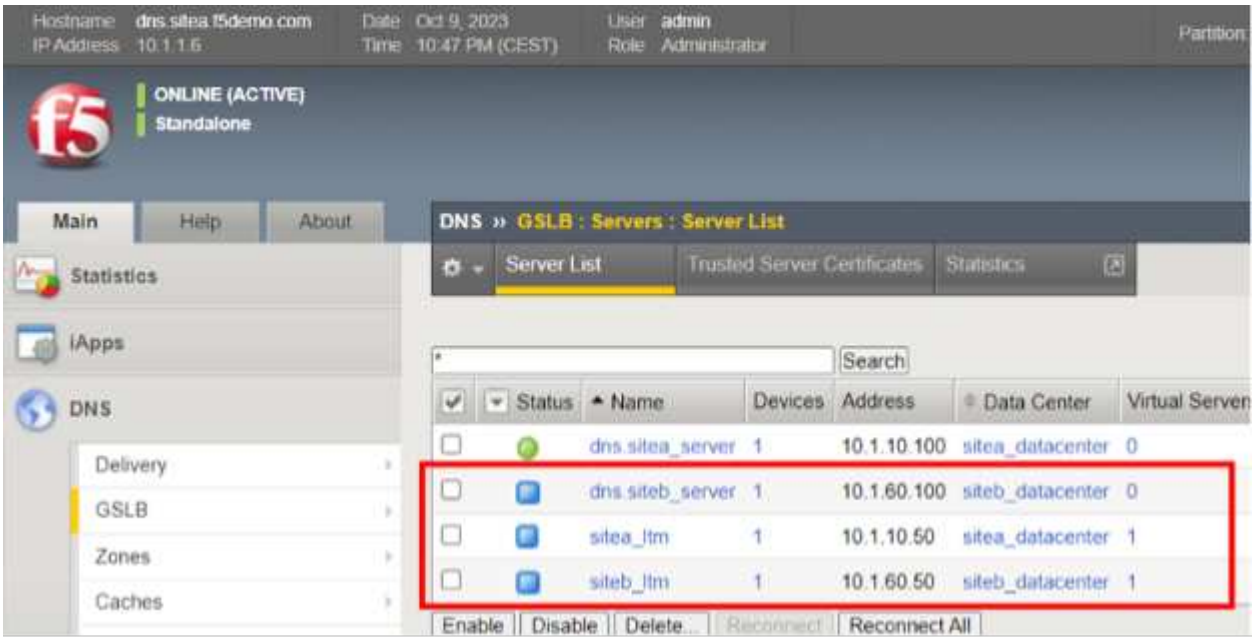


Dans certaines situations, comme des problèmes de réseau transitoires ou des règles ACL de pare-feu entre les emplacements du réseau, lors de l'ajout d'un dispositif distant à ce stade, la découverte du serveur virtuel peut ne pas afficher les entrées pour les dispositifs distants avec LTM configuré. Dans de tels cas, après avoir ajouté le nouvel appareil (« serveur »), on peut ajouter manuellement les serveurs virtuels comme indiqué ci-dessous. Si vous ajoutez un dispositif BIG-IP DNS uniquement, aucun serveur virtuel ne sera découvert ni ajouté à ce dispositif.

Nous devons ajouter ces entrées de serveur pour chaque appareil de notre solution sur tous les sites, y compris les appareils BIG-IP DNS, les appareils BIG-IP LTM et tous les appareils assurant les rôles à la fois d'unités DNS et LTM.

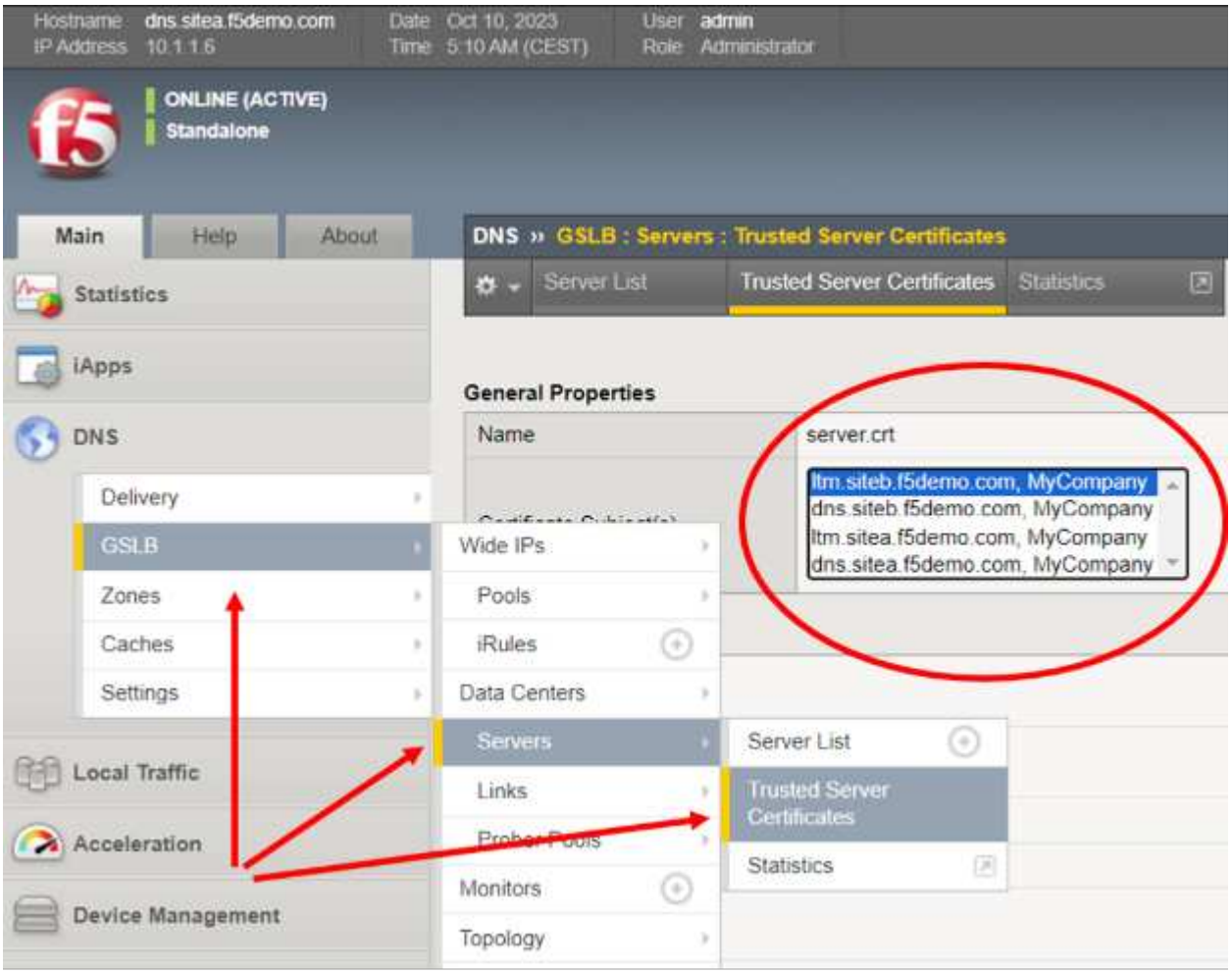
Troisième étape : Établir la confiance entre tous les équipements BIG-IP

Dans l'exemple suivant, quatre appareils ont été ajoutés en tant que serveurs ; ils sont répartis sur deux sites. Notez que chaque site dispose d'un serveur DNS BIG-IP et d'un serveur LTM BIG-IP dédiés. Cependant, tous les appareils, à l'exception de celui sur lequel je suis actuellement connecté, affichent des icônes bleues dans la colonne « État ». Cela signifie qu'une relation de confiance n'a pas encore été établie avec les autres appliances BIG-IP.



Pour ajouter de la confiance, connectez-vous en SSH au BIG-IP où les détails de configuration viennent d'être saisis via l'interface graphique, et utilisez le compte « root » pour accéder à l'interface de ligne de commande du BIG-IP. Saisissez la commande unique suivante à l'invite : *bigip_add*

La commande « bigip_add » récupère le certificat de gestion des périphériques BIG-IP de destination afin de l'utiliser lors de la configuration du canal chiffré « iQuery » entre les serveurs GSLB du cluster. Par défaut, iQuery utilise le port TCP 4353 et sert de signal de synchronisation permettant aux membres DNS BOG-IP de rester synchronisés. Il utilise XML et gzip dans le canal chiffré. Lorsque vous exécutez la commande « bigip_add » sans aucune option, elle sera exécutée sur tous les périphériques BIGIP de la liste des serveurs GSLB en utilisant le nom d'utilisateur actuel pour se connecter aux points de terminaison. Pour vérifier rapidement que tout a bien fonctionné, retournez simplement à l'interface graphique de BIG-IP et assurez-vous que tous les serveurs possèdent désormais des certificats listés dans le menu déroulant affiché.



Étape 4 : Synchroniser tous les appliances DNS BIG-IP avec le groupe DNS

La dernière étape permettra de configurer entièrement tous les équipements DNS BIG-IP en utilisant simplement l'interface graphique TMUI d'une seule unité. Dans un cas concret, où il existe deux sites StorageGRID , cela signifie désormais utiliser SSH pour accéder à la ligne de commande du DNS BIG-IP de l'**autre** site. Après vous être connecté en tant que root et avoir vérifié que les règles de pare-feu/ACL autorisent les deux périphériques BIG-IP DNS à communiquer sur les ports TCP 22 (SSH), 443 (HTTPS) et 4354 (protocole F5 iQuery), saisissez la commande suivante à l'invite : *gtm_add <adresse IP du premier serveur BIG-IP DNS du site où toutes les étapes de l'interface graphique ont été effectuées précédemment>*

À ce stade, toute configuration DNS supplémentaire peut être effectuée sur n'importe quel dispositif DNS BIG-IP ajouté au groupe. La commande ci-dessus, gtm_add, n'a pas besoin d'être appliquée aux membres de l'appliance qui sont uniquement LTM. Seuls les appareils prenant en charge le DNS nécessitent cette commande pour faire partie du groupe DNS synchronisé.

Mise en place de sites de centres de données et établissement de communications inter-BIG-IP

À ce stade, toutes les étapes nécessaires à la création du groupe d'appliances DNS BIG-IP sous-jacent et sain sont terminées. Nous pouvons maintenant procéder à la création de noms, FQDN, qui pointent vers nos services web/S3 distribués exposés dans chaque centre de données StorageGRID .

Ces noms sont appelés « Wide IPs », ou WIP en abrégé, et ce sont des noms de domaine pleinement qualifiés (FQDN) DNS normaux avec des enregistrements de ressources DNS de type A. Cependant, au lieu de pointer vers un serveur comme un enregistrement de ressource A traditionnel, ils pointent en interne vers des pools de serveurs virtuels BIG-IP. Chaque pool peut, individuellement, être constitué d'un ou plusieurs

serveurs virtuels. Un client S3 demandant une résolution d'adresse IP vers un nom recevra l'adresse du serveur virtuel S3 sur le site StorageGRID optimal sélectionné par la politique.

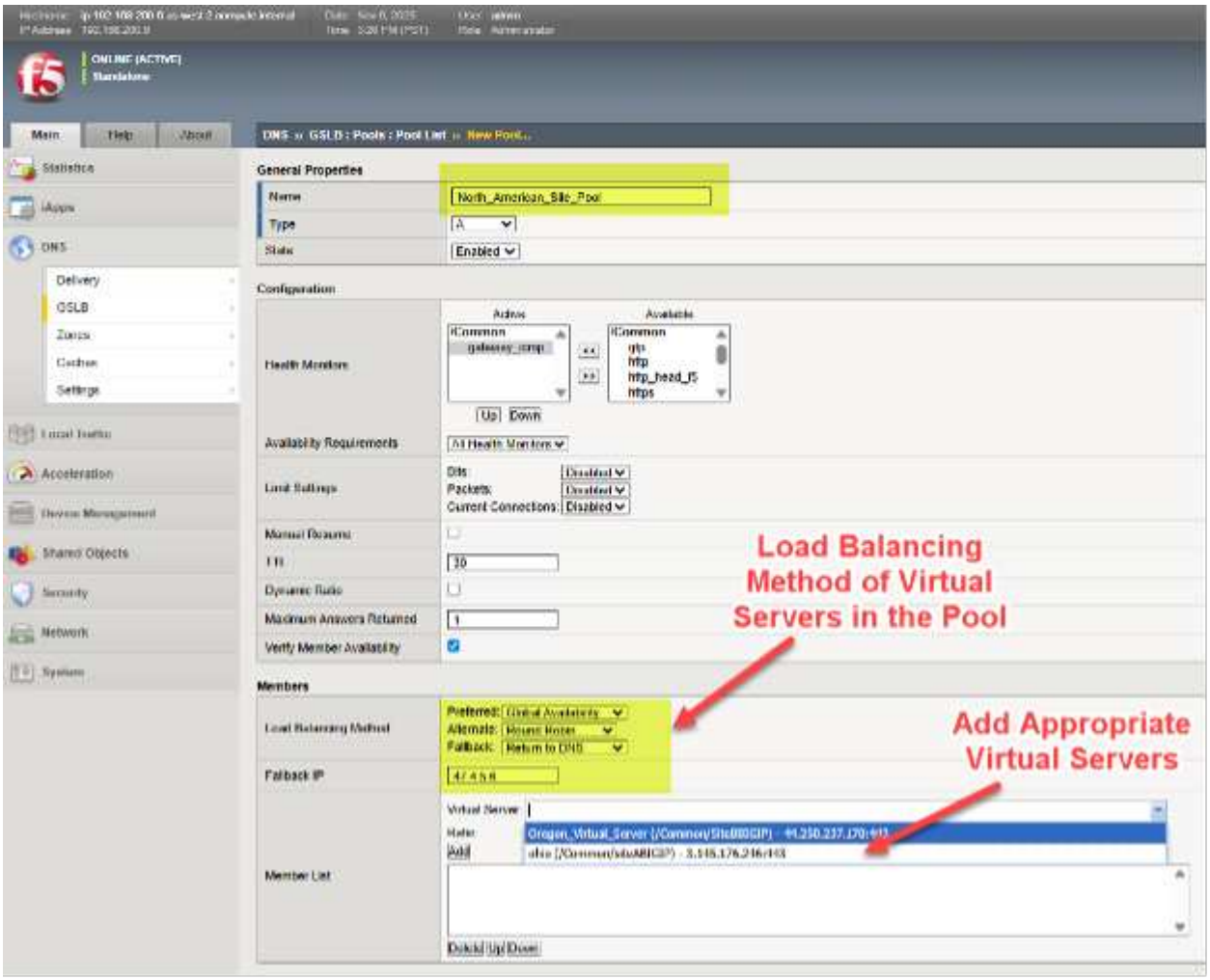
En bref : adresses IP étendues, pools et serveurs virtuels

Pour donner un exemple simple et fictif, un WIP pour le nom **storage.quantumvault.com** pourrait voir la solution DNS BIG-IP liée à deux pools de serveurs virtuels potentiels. Le premier groupe pourrait être composé de 4 sites en Amérique du Nord ; le second groupe pourrait être composé de 3 sites en Europe.

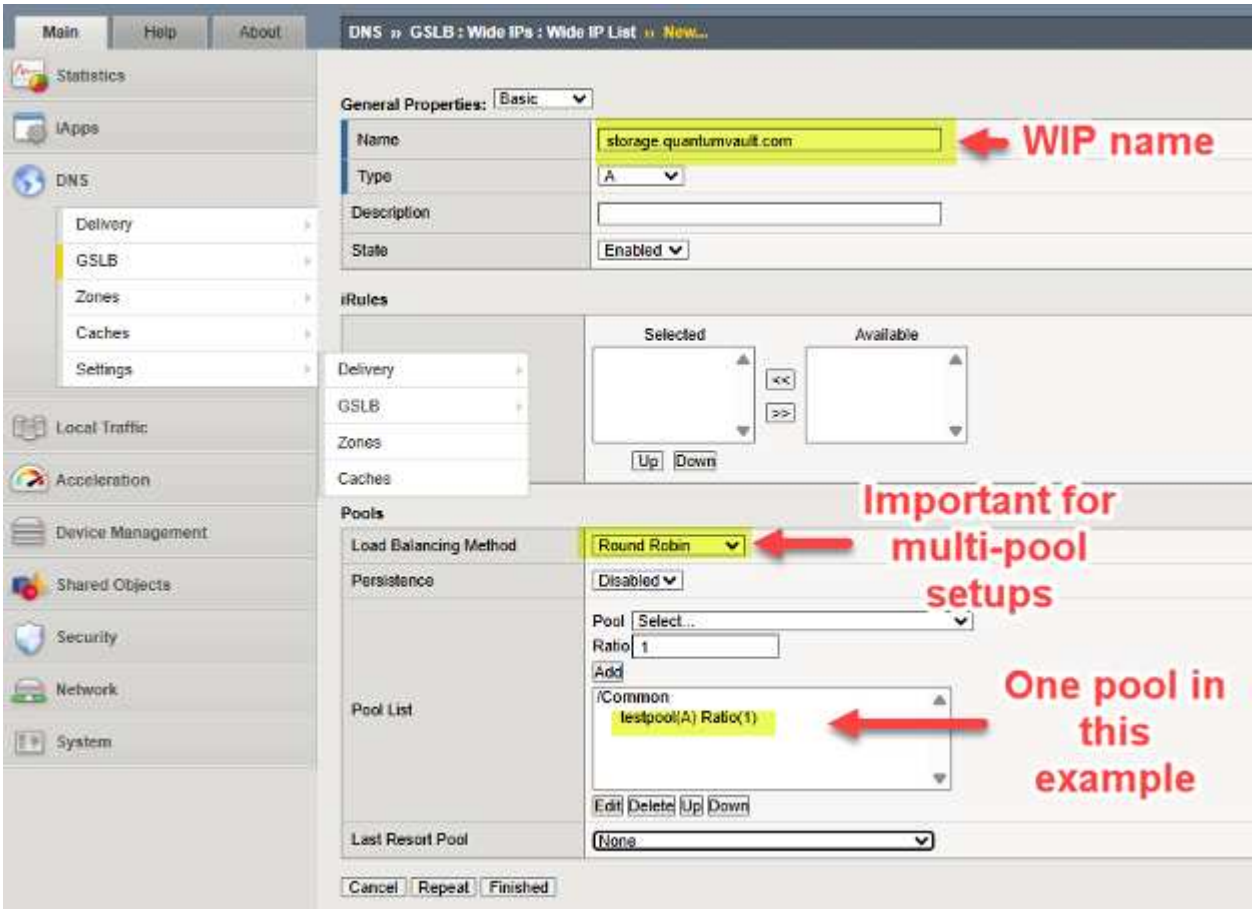
Le choix du pool sélectionné pourrait résulter d'une série de décisions politiques ; un simple ratio de 5:1 pourrait par exemple être utilisé pour diriger la majeure partie du trafic vers les sites StorageGRID nord-américains. Plus probablement, un choix basé sur la topologie où le pool est choisi de telle sorte que, par exemple, tout le trafic S3 d'origine européenne soit dirigé vers des sites européens, et le reste du trafic S3 mondial vers des centres de données nord-américains.

Une fois qu'un pool est trouvé par BIG-IP DNS, supposons que le pool nord-américain ait été sélectionné, l'enregistrement de ressource DNS A réel renvoyé pour résoudre storage.quantumvault.com peut être l'un des 4 serveurs virtuels pris en charge par BIG-IP LTM dans l'un des 4 sites nord-américains. Là encore, le choix est guidé par des politiques ; des approches « statiques » simples comme Round-Robin existent, tandis que des sélections « dynamiques » plus avancées, telles que des sondes de performance pour mesurer la latence de chaque site à partir des résolveurs DNS locaux, sont maintenues et utilisées comme critères de sélection des sites.

Pour configurer un pool de serveurs virtuels sur un BIG-IP DNS, suivez le chemin de menu **DNS > GSLB > Pools > Pool List > Add (+)**. Dans cet exemple, nous pouvons voir que différents serveurs virtuels nord-américains sont ajoutés à un pool et que l'approche privilégiée en matière d'équilibrage de charge, lorsque ce pool est sélectionné, est choisie de manière hiérarchisée.



Nous ajoutons le WIP (Wide IP), le nom de notre service qui sera résolu par DNS, à un déploiement en suivant DNS > GSLB > Wide IPs > Liste des Wide IP > Créer (+). Dans l'exemple suivant, nous fournissons un exemple de travail en cours pour un service de stockage compatible S3.



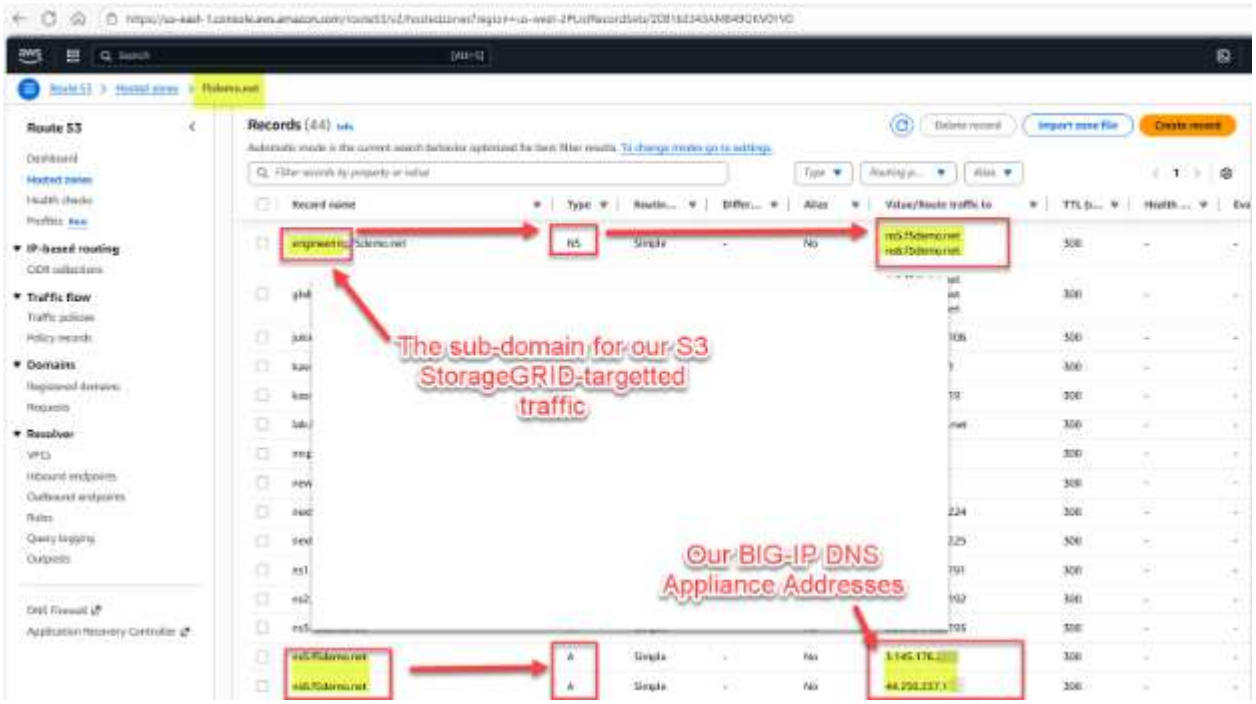
Ajuster le DNS pour prendre en charge la gestion du trafic global

À ce stade, tous nos équipements BIG-IP sous-jacents sont prêts à effectuer le GSLB (équilibrage de charge global des serveurs). Il nous suffit d'ajuster et d'attribuer les noms utilisés pour les flux de trafic S3 pour tirer parti de la solution. L'approche générale consiste à déléguer une partie d'un domaine DNS existant d'une entreprise au contrôle de BIG-IP DNS. Cela revient à « découper » une section de l'espace de noms, un sous-domaine, et à déléguer le contrôle de ce sous-domaine aux appliances DNS BIG-IP. Techniquement, cela se fait en s'assurant que les appliances DNS BIG-IP possèdent des enregistrements de ressources DNS de type A (RR) dans le DNS de l'entreprise, puis en faisant de ces noms/adresses des enregistrements de ressources DNS de serveur de noms (NS) pour le domaine délégué.

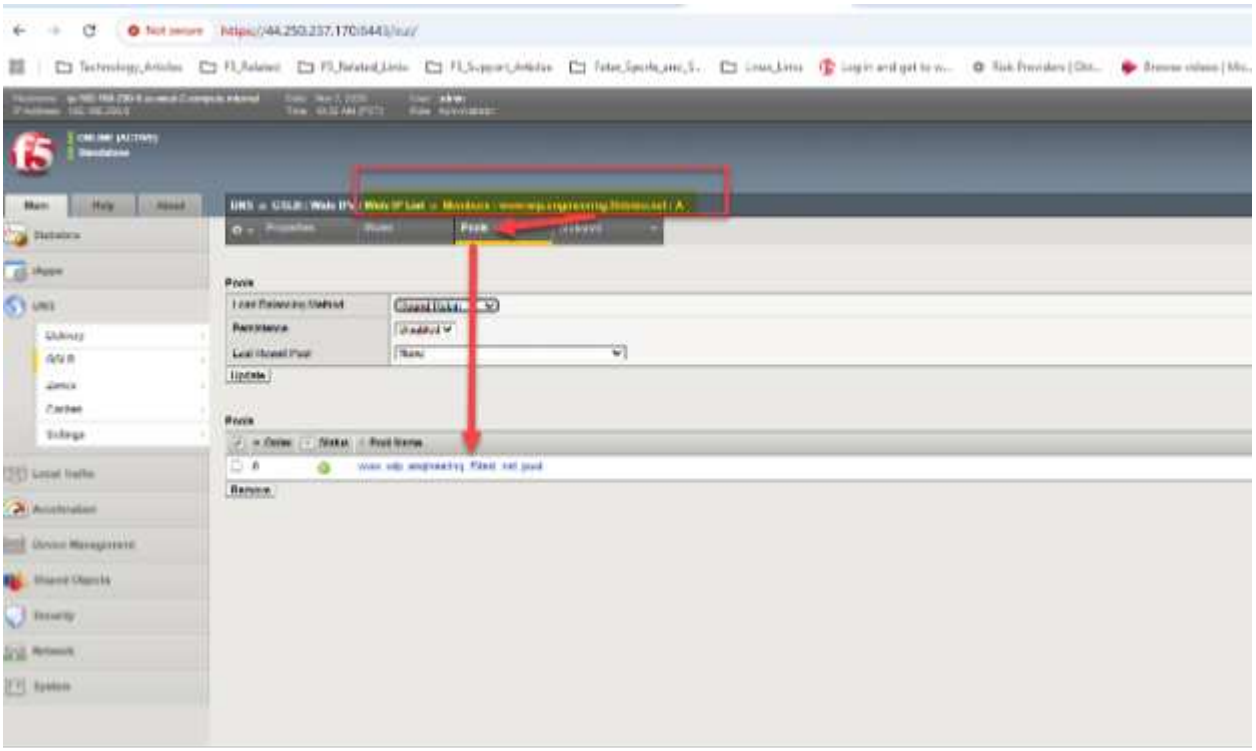
Il existe aujourd'hui différentes manières pour les entreprises de gérer leur DNS, dont une solution entièrement hébergée. Un exemple de ceci serait l'exploitation et la gestion du DNS via Windows Server 2025. Une autre solution consiste pour une entreprise à tirer parti de fournisseurs de DNS cloud comme AWS Route53 ou Squarespace.

Voici un exemple fictif à titre d'illustration. Nous disposons StorageGRID prenant en charge la lecture et l'écriture d'objets via le protocole S3 avec un domaine existant géré par AWS Route53 ; le domaine d'exemple existant est f5demo.net.

Nous souhaiterions attribuer le sous-domaine engineering.f5demo.net aux appliances DNS BIG-IP pour la gestion du trafic global. Pour ce faire, nous créons un nouvel enregistrement de ressource NS (serveur de noms) pour engineering.f5demo.net et le faisons pointer vers la liste des noms d'appliances DNS BIG-IP. Dans notre exemple, nous avons deux appliances DNS BIG-IP, et nous créons donc deux enregistrements de ressources A pour chacune d'elles.



Nous allons maintenant, à titre d'exemple, configurer un Wide IP (WIP) dans notre DNS BIG-IP. Étant donné que le DNS utilise la synchronisation de groupe, nous n'avons besoin de l'ajuster qu'à l'aide de l'interface graphique d'un seul appareil. Dans l'interface graphique DNS de BIG-IP, accédez à **DNS > GSLB > Wide IPs > Wide IP List (+)**. Rappelons que, dans une configuration DNS FQDN traditionnelle, on entrerait une ou plusieurs adresses IPv4 ; dans notre cas, nous pointons simplement vers un ou plusieurs pools de serveurs virtuels StorageGRID .

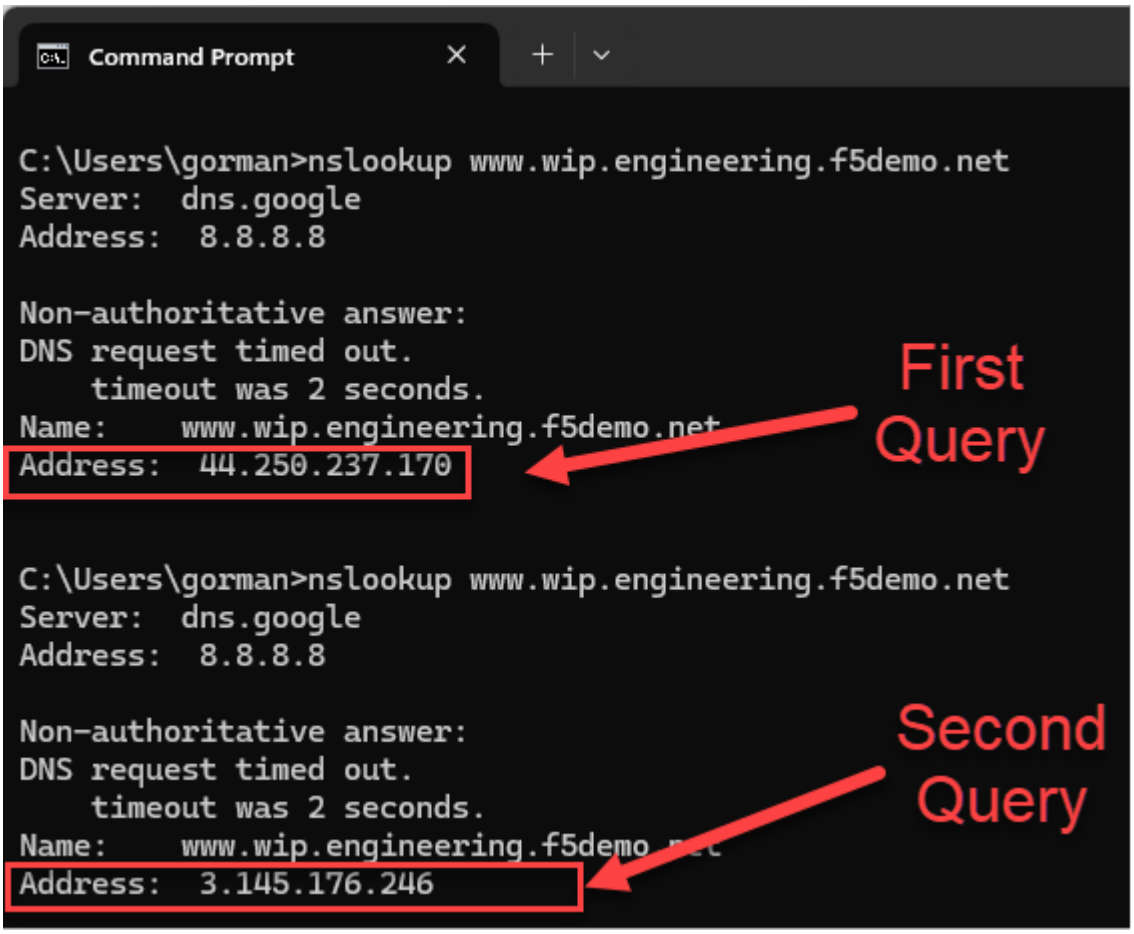


Dans notre exemple, nous avons des serveurs web HTTPS génériques situés à la fois dans l'Ohio et dans l'Oregon. Avec une simple approche de type « round robin », nous devrions pouvoir voir le DNS global répondre aux requêtes concernant les mappages d'enregistrements de ressources A pour

www.wip.engineering.f5demo.net avec les deux adresses IP du serveur virtuel.

Un test simple peut être effectué avec des navigateurs web ou, dans le cas de S3 utilisant StorageGRID, éventuellement avec des outils graphiques comme S3Browser. Chaque requête DNS verra le prochain site de centre de données du pool utilisé comme cible pour le trafic suivant, en raison de notre choix de Round Robin au sein du pool.

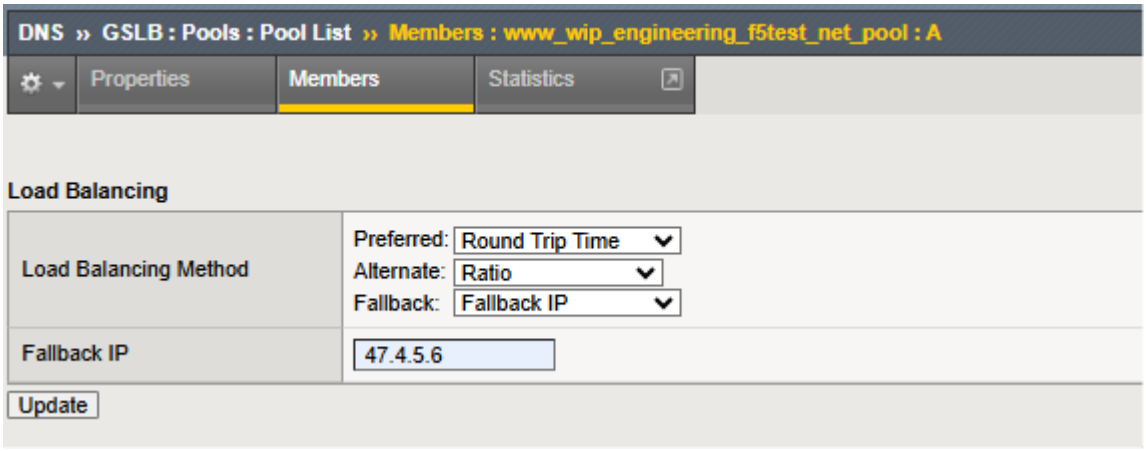
Dans notre exemple de configuration, nous pouvons utiliser dig ou nslookup pour générer rapidement une série de deux requêtes DNS et nous assurer que BIG-IP DNS effectue bien un équilibrage de charge round robin, ce qui permet aux deux sites de recevoir du trafic au fil du temps.



Exploration suggérée pour des techniques plus avancées

L'une des nombreuses approches possibles consisterait à utiliser le mode « Disponibilité globale » plutôt que le simple exemple de « Round Robin » donné ci-dessus. Avec la disponibilité globale, l'ordre séquentiel des pools, ou des serveurs virtuels au sein d'un seul pool, peut recevoir du trafic dirigé vers celui-ci. De cette manière, tout le trafic S3 pourrait, par défaut, être dirigé vers, par exemple, un site situé à New York.

Si les contrôles d'intégrité indiquent un problème de disponibilité des nœuds StorageGRID sur ce site, le trafic pourrait alors être redirigé vers Saint-Louis. Si Saint-Louis rencontrait des problèmes sanitaires, un site à Francfort pourrait alors commencer à recevoir des transactions de lecture ou d'écriture S3. Ainsi, la disponibilité globale est une approche de la résilience globale de la solution S3 StorageGRID . Une autre approche consiste à combiner différentes méthodes d'équilibrage de charge, en utilisant une approche par paliers.



Dans cet exemple, l'option « dynamique » est le premier choix d'équilibrage de charge pour les sites du pool configuré. Dans l'exemple présenté, une approche de mesure continue utilisant un sondage actif des performances du résolveur DNS local est maintenue et sert de catalyseur pour la sélection du site. Si cette approche n'est pas possible, les sites individuels peuvent être sélectionnés en fonction du ratio attribué à chacun. Grâce à ce ratio, les sites StorageGRID plus grands et à bande passante plus élevée peuvent recevoir plus de transactions S3 que les sites plus petits. Enfin, dans le cadre d'un scénario de reprise après sinistre, si tous les sites du pool deviennent défaillants, l'adresse IP de secours spécifiée est utilisée comme site de dernier recours. L'une des méthodes d'équilibrage de charge les plus intéressantes de BIG-IP DNS est la « topologie », selon laquelle la source entrante des requêtes DNS, le résolveur DNS local de l'utilisateur S3, est observée et, à l'aide des informations de topologie Internet, le site apparemment le plus « proche » est sélectionné dans le pool.

Enfin, si les sites sont répartis sur l'ensemble du globe, il peut être judicieux d'envisager l'utilisation de la technologie de « sonde » dynamique décrite en détail dans le manuel DNS F5 BIG-IP. Grâce aux sondes, il est possible de surveiller les sources fréquentes de requêtes DNS, par exemple un partenaire commercial dont le trafic utilise généralement le même résolveur DNS local. Les sondes DNS BIG-IP peuvent être lancées depuis le BIG-IP LTM dans chaque site du monde entier, afin de déterminer de manière générale quel site potentiel serait susceptible d'offrir la latence la plus faible pour les transactions S3. De ce fait, le trafic en provenance d'Asie pourrait être mieux pris en charge par les sites StorageGRID asiatiques que par les sites situés en Amérique du Nord ou en Europe.

Conclusion

L'intégration de F5 BIG-IP avec NetApp StorageGRID répond aux défis techniques liés à la disponibilité et à la cohérence des données sur plusieurs sites et à l'optimisation du routage des transactions S3. Le déploiement de cette solution améliore la résilience, les performances et la fiabilité du stockage, ce qui la rend idéale pour les entreprises à la recherche d'une infrastructure de stockage robuste, évolutive et flexible.

Pour en savoir plus, la documentation officielle F5 pour BIG-IP DNS est disponible ici : "lien". Un guide de style classe guidée, fournissant des instructions étape par étape sur un exemple de configuration, est également disponible. "ici".

Configuration SNMP Datalog

Par Aron Klein

Configurez Datalog pour collecter les mesures snmp et les traps StorageGRID.

Configurer Datalog

Datalog est une solution de surveillance qui fournit des mesures, des visualisations et des alertes. La configuration suivante a été implémentée avec l'agent linux version 7.43.1 sur un hôte Ubuntu 22.04.1 déployé localement sur le système StorageGRID.

Fichiers de profil Datadog et de déroutement générés à partir du fichier MIB StorageGRID

Datadog fournit une méthode de conversion des fichiers MIB de produit en fichiers de référence Datadog requis pour mapper les messages SNMP.

Ce fichier yaml StorageGRID pour le mappage de résolution des interruptions Datadog généré suivant l'instruction trouvée "ici". + placez ce fichier dans /etc/datadog-agent/conf.d/snmp.d/traps_db/ +

- "Téléchargez le fichier yaml d'interruption" +
  - **somme de contrôle md5** 42e27e4210719945a46172b98c379517 +
  - **sha256 checksum** d0fe5c8e6ca3c902d054f85f8554b70a85f928cba8b7c76391d356f05d2cf73b6887 +

Ce fichier yaml de profil StorageGRID pour le mappage de metrics Datadog généré suivant l'instruction trouvée "ici". + placez ce fichier dans /etc/datadog-agent/conf.d/snmp.d/profiles/ +

- "Téléchargez le fichier yaml de profil" +
  - **somme de contrôle md5** 72bb7784f4801adda4e0c3ea77df19aa +
  - **sha256 checksum** b6b7fadd33063422a8bb8e39b3ead8ab38349ee0229926eadc85f0087b8cee +

Configuration du datalog SNMP pour les métriques

La configuration de SNMP pour les mesures peut être gérée de deux manières. Vous pouvez configurer la détection automatique en fournissant une plage d'adresses réseau contenant le(s) système(s) StorageGRID ou en définissant les adresses IP des périphériques individuels. L'emplacement de la configuration est différent en fonction de la décision prise. La découverte automatique est définie dans le fichier yaml de l'agent de données. Les définitions explicites de périphériques sont configurées dans le fichier yaml de configuration snmp. Vous trouverez ci-dessous des exemples de chacun d'eux pour le même système StorageGRID.

Découverte automatique

configuration située dans /etc/datadog-agent/datadog.yaml

```
listeners:
  - name: snmp
snmp_listener:
```

```
  workers: 100  # number of workers used to discover devices concurrently
  discovery_interval: 3600  # interval between each autodiscovery in
seconds
  loader: core  # use core check implementation of SNMP integration.
recommended
  use_device_id_as_hostname: true  # recommended
  configs:
    - network_address: 10.0.0.0/24  # CIDR subnet
      snmp_version: 2
      port: 161
      community_string: 'st0r@gegrid'  # enclose with single quote
      profile: netapp-storagegrid
```

Périphériques individuels

/etc/datadog-agent/conf.d/snmp.d/conf.yaml

```
init_config:
  loader: core  # use core check implementation of SNMP integration.
recommended
  use_device_id_as_hostname: true  # recommended
instances:
- ip_address: '10.0.0.1'
  profile: netapp-storagegrid
  community_string: 'st0r@gegrid'  # enclose with single quote
- ip_address: '10.0.0.2'
  profile: netapp-storagegrid
  community_string: 'st0r@gegrid'
- ip_address: '10.0.0.3'
  profile: netapp-storagegrid
 community_string: 'st0r@gegrid'
- ip_address: '10.0.0.4'
  profile: netapp-storagegrid
  community_string: 'st0r@gegrid'
```

Configuration SNMP pour les interruptions

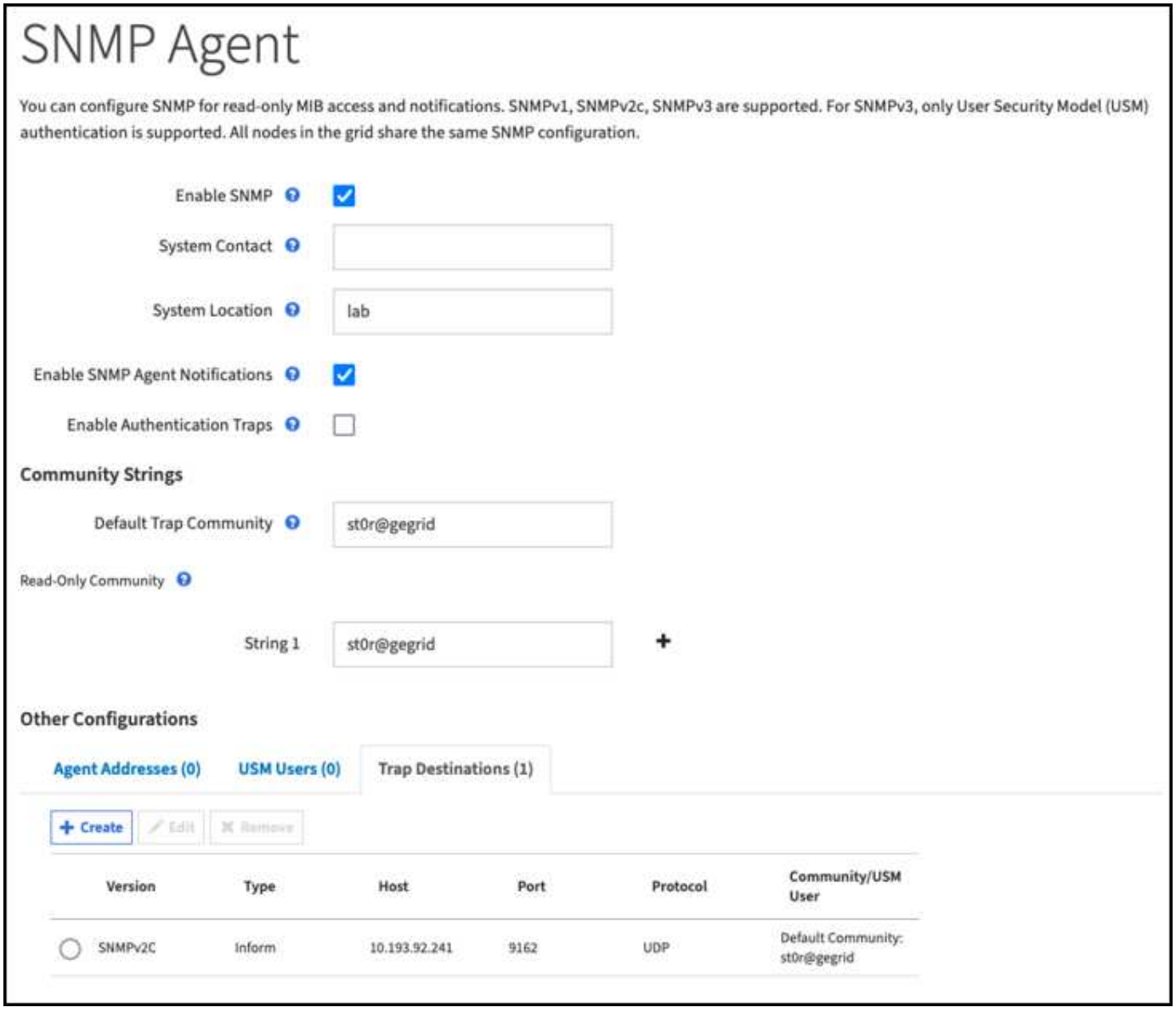
La configuration des traps SNMP est définie dans le fichier de configuration de datadog yaml /etc/datadog-agent/datadog.yaml

```
network_devices:
  namespace:  # optional, defaults to “default”.
  snmp_traps:
    enabled: true
    port: 9162 # on which ports to listen for traps
```

```
    community_strings: # which community strings to allow for v2 traps
      - st0r@gegrid
```

Exemple de configuration SNMP StorageGRID

L'agent SNMP de votre système StorageGRID se trouve sous l'onglet de configuration, colonne surveillance. Activez SNMP et entrez les informations souhaitées. Si vous souhaitez configurer des interruptions, sélectionnez « destinations des interruptions » et créez une destination pour l'hôte de l'agent Datadog contenant la configuration des interruptions.



Utilisez rclone pour migrer, DÉPLACER et SUPPRIMER des objets sur StorageGRID

Par Siegfried Hepp et Aron Klein

Rclone est un outil de ligne de commande et un client gratuits pour les opérations S3. Vous pouvez utiliser

rclone pour migrer, copier et supprimer des données d'objet sur StorageGRID. rclone permet de supprimer des compartiments même s'ils ne sont pas vides, grâce à la fonction de « purge » comme illustré ci-dessous.

Installer et configurer rclone

Pour installer rclone sur un poste de travail ou un serveur, téléchargez-le depuis "rclone.org".

Étapes de configuration initiale

1. Créez le fichier de configuration rclone en exécutant le script de configuration ou en créant manuellement le fichier.
2. Dans cet exemple, j'utilise sgdemo pour le nom du terminal StorageGRID S3 distant dans la configuration rclone.
   a. Créez le fichier de configuration ~/.config/rclone/rclone.conf

```
[sgdemo]
type = s3
provider = Other
access_key_id = ABCDEFGH123456789JKL
secret_access_key = 123456789ABCDEFGHIJKLMN0123456789PQRST+V
endpoint = sgdemo.netapp.com
```

   b. Exécutez la configuration rclone

rclone config

```
2023/04/13 14:22:45 NOTICE: Config file
"/root/.config/rclone/rclone.conf" not found - using defaults
No remotes found - make a new one
n) New remote
s) Set configuration password
q) Quit config
n/s/q> n
name> sgdemo
```

```
Option Storage.
Type of storage to configure.
Enter a string value. Press Enter for the default ("").
Choose a number from below, or type in your own value.
 1 / 1Fichier
   \ "fichier"
 2 / Alias for an existing remote
   \ "alias"
 3 / Amazon Drive
```

```
   \ "amazon cloud drive"
 4 / Amazon S3 Compliant Storage Providers including AWS,
Alibaba, Ceph, Digital Ocean, Dreamhost, IBM COS, Minio,
SeaweedFS, and Tencent COS
   \ "s3"
 5 / Backblaze B2
   \ "b2"
 6 / Better checksums for other remotes
   \ "hasher"
 7 / Box
   \ "box"
 8 / Cache a remote
   \ "cache"
 9 / Citrix Sharefile
   \ "sharefile"
10 / Compress a remote
   \ "compress"
11 / Dropbox
   \ "dropbox"
12 / Encrypt/Decrypt a remote
   \ "crypt"
13 / Enterprise File Fabric
   \ "filefabric"
14 / FTP Connection
   \ "ftp"
15 / Google Cloud Storage (this is not Google Drive)
   \ "google cloud storage"
16 / Google Drive
   \ "drive"
17 / Google Photos
   \ "google photos"
18 / Hadoop distributed file system
   \ "hdfs"
19 / Hubic
   \ "hubic"
20 / In memory object storage system.
   \ "memory"
21 / Jottacloud
   \ "jottacloud"
22 / Koofr
   \ "koofr"
23 / Local Disk
   \ "local"
24 / Mail.ru Cloud
   \ "mailru"
25 / Mega
```

```
   \ "mega"
26 / Microsoft Azure Blob Storage
   \ "azureblob"
27 / Microsoft OneDrive
   \ "onedrive"
28 / OpenDrive
   \ "opendrive"
29 / OpenStack Swift (Rackspace Cloud Files, Memset Memstore,
OVH)
   \ "swift"
30 / Pcloud
   \ "pcloud"
31 / Put.io
   \ "putio"
32 / QingCloud Object Storage
   \ "qingstor"
33 / SSH/SFTP Connection
   \ "sftp"
34 / Sia Decentralized Cloud
   \ "sia"
35 / Sugarsync
   \ "sugarsync"
36 / Tardigrade Decentralized Cloud Storage
   \ "tardigrade"
37 / Transparently chunk/split large files
   \ "chunker"
38 / Union merges the contents of several upstream fs
   \ "union"
39 / Uptobox
   \ "uptobox"
40 / Webdav
   \ "webdav"
41 / Yandex Disk
   \ "yandex"
42 / Zoho
   \ "zoho"
43 / http Connection
   \ "http"
44 / premiumize.me
   \ "premiumizeme"
45 / seafile
   \ "seafile"
```

```
Storage> 4
```

```
Option provider.
Choose your S3 provider.
Enter a string value. Press Enter for the default ("").
Choose a number from below, or type in your own value.
 1 / Amazon Web Services (AWS) S3
   \ "AWS"
 2 / Alibaba Cloud Object Storage System (OSS) formerly Aliyun
   \ "Alibaba"
 3 / Ceph Object Storage
   \ "Ceph"
 4 / Digital Ocean Spaces
   \ "DigitalOcean"
 5 / Dreamhost DreamObjects
   \ "Dreamhost"
 6 / IBM COS S3
   \ "IBMCOS"
 7 / Minio Object Storage
   \ "Minio"
 8 / Netease Object Storage (NOS)
   \ "Netease"
 9 / Scaleway Object Storage
   \ "Scaleway"
10 / SeaweedFS S3
   \ "SeaweedFS"
11 / StackPath Object Storage
   \ "StackPath"
12 / Tencent Cloud Object Storage (COS)
   \ "TencentCOS"
13 / Wasabi Object Storage
   \ "Wasabi"
14 / Any other S3 compatible provider
   \ "Other"
provider> 14
```

```
Option env_auth.
Get AWS credentials from runtime (environment variables or
EC2/ECS meta data if no env vars).
Only applies if access_key_id and secret_access_key is blank.
Enter a boolean value (true or false). Press Enter for the
default ("false").
Choose a number from below, or type in your own value.
 1 / Enter AWS credentials in the next step.
   \ "false"
 2 / Get AWS credentials from the environment (env vars or IAM).
```

```
   \ "true"
env_auth> 1
```

```
Option access_key_id.
AWS Access Key ID.
Leave blank for anonymous access or runtime credentials.
Enter a string value. Press Enter for the default ("").
access_key_id> ABCDEFGH123456789JKL
```

```
Option secret_access_key.
AWS Secret Access Key (password).
Leave blank for anonymous access or runtime credentials.
Enter a string value. Press Enter for the default ("").
secret_access_key> 123456789ABCDEFGHIJKLMN0123456789PQRST+V
```

```
Option region.
Region to connect to.
Leave blank if you are using an S3 clone and you don't have a
region.
Enter a string value. Press Enter for the default ("").
Choose a number from below, or type in your own value.
   / Use this if unsure.
 1 | Will use v4 signatures and an empty region.
   \ ""
   / Use this only if v4 signatures don't work.
 2 | E.g. pre Jewel/v10 CEPH.
   \ "other-v2-signature"
region> 1
```

```
Option endpoint.
Endpoint for S3 API.
Required when using an S3 clone.
Enter a string value. Press Enter for the default ("").
endpoint> sgdemo.netapp.com
```

```
Option location_constraint.
Location constraint - must be set to match the Region.
Leave blank if not sure. Used when creating buckets only.
Enter a string value. Press Enter for the default ("").
```

```
location_constraint>
```

```
Option acl.
Canned ACL used when creating buckets and storing or copying
objects.
This ACL is used for creating objects and if bucket_acl isn't
set, for creating buckets too.
For more info visit
https://docs.aws.amazon.com/AmazonS3/latest/dev/acl-
overview.html#canned-acl
Note that this ACL is applied when server-side copying objects as
S3
doesn't copy the ACL from the source but rather writes a fresh
one.
Enter a string value. Press Enter for the default ("").
Choose a number from below, or type in your own value.
   / Owner gets FULL_CONTROL.
 1 | No one else has access rights (default).
   \ "private"
   / Owner gets FULL_CONTROL.
 2 | The AllUsers group gets READ access.
   \ "public-read"
   / Owner gets FULL_CONTROL.
 3 | The AllUsers group gets READ and WRITE access.
   | Granting this on a bucket is generally not recommended.
   \ "public-read-write"
   / Owner gets FULL_CONTROL.
 4 | The AuthenticatedUsers group gets READ access.
   \ "authenticated-read"
   / Object owner gets FULL_CONTROL.
 5 | Bucket owner gets READ access.
   | If you specify this canned ACL when creating a bucket,
Amazon S3 ignores it.
   \ "bucket-owner-read"
   / Both the object owner and the bucket owner get FULL_CONTROL
over the object.
 6 | If you specify this canned ACL when creating a bucket,
Amazon S3 ignores it.
   \ "bucket-owner-full-control"
acl>
```

```
Edit advanced config?
y) Yes
n) No (default)
```

```
y/n> n
```

```
--------------------
[sgdemo]
type = s3
provider = Other
access_key_id = ABCDEFGH123456789JKL
secret_access_key = 123456789ABCDEFGHIJKLMN0123456789PQRST+V
endpoint = sgdemo.netapp.com:443
--------------------
y) Yes this is OK (default)
e) Edit this remote
d) Delete this remote
y/e/d>
```

```
Current remotes:
```

```
Name                 Type
====                 ====
sgdemo               s3
```

```
e) Edit existing remote
n) New remote
d) Delete remote
r) Rename remote
c) Copy remote
s) Set configuration password
q) Quit config
e/n/d/r/c/s/q> q
```

Exemples de commandes de base

- **Créer un compartiment :**

  `rclone mkdir remote:bucket`

  ```
  # rclone mkdir sgdemo:test01
  ```

  Utilisez --no-check-certificate si vous devez ignorer les certificats SSL.

- **Liste de tous les compartiments:**

  `rclone lsd remote:`

  # rclone lsd sgdemo :

- **Liste des objets dans un compartiment spécifique :**

  `rclone ls remote:bucket`

  # rclone ls sgdemo:test01

```
    65536 TestObject.0
    65536 TestObject.1
    65536 TestObject.10
    65536 TestObject.12
    65536 TestObject.13
    65536 TestObject.14
    65536 TestObject.15
    65536 TestObject.16
    65536 TestObject.17
    65536 TestObject.18
    65536 TestObject.2
    65536 TestObject.3
    65536 TestObject.5
    65536 TestObject.6
    65536 TestObject.7
    65536 TestObject.8
    65536 TestObject.9
  33554432 bigobj
      102 key.json
       47 locked01.txt
4294967296 sequential-read.0.0
       15 test.txt
      116 version.txt
```

- **Supprimer un compartiment :**

  `rclone rmdir remote:bucket`

  # rclone rmdir sgdemo:test02

- **Mettre un objet:**

```
rclone copy filename remote:bucket
```

```
# rclone copy ~/test/testfile.txt sgdemo:test01
```

- **Obtenir un objet:**

```
rclone copy remote:bucket/objectname filename
```

```
# Rclone copy sgdemo:test01/testfile.txt ~/test/testfileS3.txt
```

- **Supprimer un objet:**

```
rclone delete remote:bucket/objectname
```

```
# rclone delete sgdemo:test01/testfile.txt
```

- **Migrer des objets dans un compartiment**

```
rclone sync source:bucket destination:bucket --progress

rclone sync source_directory destination:bucket --progress
```

```
# rclone sync sgdemo:test01 sgdemo:clone01 --progress

Transferred:        4.032 GiB / 4.032 GiB, 100%, 95.484 KiB/s, ETA
0s
Transferred:           22 / 22, 100%
Elapsed time:       1m4.2s
```

Utilisez --Progress ou -P pour afficher la progression de la tâche. Sinon, il n'y a pas de sortie.

- **Supprimer un compartiment et tout le contenu de l'objet**

```
rclone purge remote:bucket --progress
```

```
# rclone purge sgdemo:test01 --progress

Transferred:              0 B / 0 B, -, 0 B/s, ETA -
Checks:                46 / 46, 100%
Deleted:               23 (files), 1 (dirs)
```

```
Elapsed time:        10.2s
```

rclone ls sgdemo:test01

```
2023/04/14 09:40:51 Failed to ls: directory not found
```

Bonnes pratiques de déploiement de StorageGRID avec Veeam Backup and Replication

Par Oliver Haensel et Aron Klein

Ce guide se concentre sur la configuration de NetApp StorageGRID et en partie de Veeam Backup and Replication. Ce livre blanc s'adresse aux administrateurs du stockage et du réseau qui connaissent bien les systèmes Linux et sont chargés de la maintenance ou de l'implémentation d'un système NetApp StorageGRID en association avec Veeam Backup and Replication.

Présentation

Les administrateurs du stockage cherchent à gérer la croissance de leurs données grâce à des solutions qui répondent à leurs besoins en termes de disponibilité, de restauration rapide, d'évolutivité et d'automatisation des règles de conservation des données à long terme. Ces solutions doivent également offrir une protection contre les pertes et les attaques malveillantes. Ensemble, Veeam et NetApp ont créé une solution de protection des données combinant Veeam Backup & Recovery avec NetApp StorageGRID pour le stockage objet sur site.

Veeam et NetApp StorageGRID proposent une solution simple d'utilisation qui s'associent pour répondre aux exigences liées à la croissance rapide des données et à l'augmentation des réglementations à travers le monde. Le stockage objet basé dans le cloud est réputé pour sa résilience, son évolutivité, ses fonctionnalités opérationnelles et sa rentabilité, qui en font un choix naturel comme cible pour vos sauvegardes. Ce document fournit des conseils et des recommandations pour la configuration de votre solution de sauvegarde Veeam et de votre système StorageGRID.

La charge de travail d'objets de Veeam crée un grand nombre d'opérations simultanées de PUT, DELETE et LIST pour les petits objets. L'activation de l'immuabilité ajoute au nombre de demandes dans le magasin d'objets pour définir la conservation et répertorier les versions. Le processus d'une tâche de sauvegarde comprend l'écriture d'objets pour la modification quotidienne. Une fois les nouvelles écritures terminées, la tâche supprime tous les objets basés sur la stratégie de rétention de la sauvegarde. La planification des tâches de sauvegarde se chevauchera presque toujours. Ce chevauchement entraînera une grande partie de la fenêtre de sauvegarde comprenant une charge de travail PUT/DELETE 50/50 sur le magasin d'objets. Ajuster dans Veeam le nombre d'opérations simultanées avec le paramètre de slot de tâche, augmenter la taille de l'objet en augmentant la taille du bloc de tâche de sauvegarde, réduire le nombre d'objets dans les demandes de suppression multi-objets, et le choix de la fenêtre de temps maximum pour les tâches à effectuer optimisera la solution en termes de performances et de coûts.

Assurez-vous de lire la documentation du produit pour "Sauvegarde et réplication Veeam" et "StorageGRID" avant de commencer. Veeam fournit des calculateurs permettant de comprendre le dimensionnement de l'infrastructure Veeam et les exigences de capacité qui doivent être utilisées avant de dimensionner votre solution StorageGRID . Veuillez toujours vérifier les configurations validées par Veeam- NetApp sur le site Web du programme Veeam Ready pour "Objets compatibles Veeam, immuabilité d'objet et référentiel" .

Configuration Veeam

Version recommandée

Il est toujours recommandé de rester à jour et d'appliquer les derniers correctifs pour votre système Veeam Backup & Replication 12 ou 12.1. Nous recommandons actuellement d'installer au moins le correctif P20230718 de Veeam 12.

Configuration du référentiel S3

Un référentiel de sauvegarde scale-out (SOBR) est le Tier de capacité du stockage objet S3. Le Tier de capacité est une extension du référentiel principal, qui permet de prolonger les périodes de conservation des données et de réduire le coût de la solution de stockage. Veeam a la possibilité d'immuabilité avec l'API S3 Object Lock. Veeam 12 peut utiliser plusieurs compartiments dans un référentiel scale-out. StorageGRID n'a pas de limite pour le nombre d'objets ou la capacité d'un compartiment unique. L'utilisation de plusieurs compartiments peut améliorer les performances lors de la sauvegarde de datasets très volumineux où les données de sauvegarde peuvent atteindre plusieurs pétaoctets dans des objets.

La limitation des tâches simultanées peut être nécessaire en fonction du dimensionnement de la solution et des besoins spécifiques. Les paramètres par défaut spécifient un emplacement de tâche de référentiel pour chaque cœur de processeur et pour chaque emplacement de tâche une limite d'emplacement de tâche simultanée de 64. Par exemple, si votre serveur dispose de 2 cœurs de processeur, 128 threads simultanés au total seront utilisés pour le magasin d'objets. Cela inclut les COMMANDES PUT, GET et batch Delete. Il est recommandé de sélectionner une limite conservatrice pour les créneaux de tâches à commencer par et d'ajuster cette valeur une fois que les sauvegardes Veeam ont atteint l'état stable de nouvelles sauvegardes et que les données de sauvegarde expirent. Veuillez vous adresser à votre équipe de gestion de compte NetApp pour dimensionner le système StorageGRID en fonction des délais et des performances souhaités. Il peut être nécessaire de régler le nombre d'emplacements de tâches et la limite des tâches par emplacement pour obtenir la solution optimale.

Configuration de la procédure de sauvegarde

Les tâches de sauvegarde Veeam peuvent être configurées avec plusieurs options de taille de bloc qui doivent être prises en compte avec attention. La taille de bloc par défaut est de 1 Mo. Grâce à l'efficacité du stockage, Veeam assure la compression et la déduplication, ce qui permet de créer des tailles d'objet d'environ 500 Ko pour la sauvegarde complète initiale et des objets de 100 à 200 Ko pour les tâches incrémentielles. Nous pouvons considérablement améliorer les performances et réduire les besoins en matière de magasin d'objets en choisissant une taille de bloc de sauvegarde plus importante. Si la taille de bloc supérieure améliore considérablement les performances du magasin d'objets, elle implique toutefois une augmentation potentielle des besoins en capacité de stockage primaire en raison de la réduction des performances du stockage. Il est recommandé de configurer les tâches de sauvegarde avec une taille de bloc de 4 Mo, ce qui crée des objets d'environ 2 Mo pour les sauvegardes complètes et des objets de 700 Ko à 1 Mo pour les sauvegardes incrémentielles. Les clients peuvent même envisager de configurer des tâches de sauvegarde à l'aide d'une taille de bloc de 8 Mo, qui peut être activée avec l'aide du support Veeam.

La mise en œuvre des sauvegardes immuables utilise le verrouillage objet S3 dans le magasin d'objets. L'option immuabilité génère un nombre accru de requêtes auprès du magasin d'objets pour obtenir des mises à jour de listes et de conservation des objets.

Lorsque les rétentions de sauvegarde expirent, les procédures de sauvegarde traitent la suppression des objets. Veeam envoie les demandes de suppression au magasin d'objets dans le cadre de requêtes de suppression de plusieurs objets de 1000 objets par demande. Pour les petites solutions, il peut être nécessaire de l'ajuster afin de réduire le nombre d'objets par demande. En outre, si cette valeur est moindre, les demandes de suppression seront réparties de manière plus homogène entre les nœuds du système StorageGRID. Il est recommandé d'utiliser les valeurs du tableau ci-dessous comme point de départ pour la

configuration de la limite de suppression de plusieurs objets. Multipliez la valeur du tableau par le nombre de nœuds pour le type d'appliance choisi pour obtenir la valeur du paramètre dans Veeam. Si cette valeur est égale ou supérieure à 1000, il n'est pas nécessaire d'ajuster la valeur par défaut. Si cette valeur doit être ajustée, contactez le support Veeam pour effectuer cette modification.

Modèle de type appliance	S3MultiObjectDeleteLimit par nœud
SG5712	34
SG5760	75
SG6060	200

Pour en savoir plus sur la configuration recommandée en fonction de vos besoins, contactez l'équipe NetApp en charge de votre compte. Les recommandations concernant les paramètres de configuration Veeam incluent :

- Taille du bloc de la tâche de sauvegarde = 4 Mo
- Limite d'emplacement de tâche SOBR = 2-16
- Limite de suppression de plusieurs objets = 34-1000

Configuration StorageGRID

Version recommandée

NetApp StorageGRID 11.9 ou 12.0 avec le dernier correctif sont les versions recommandées pour les déploiements Veeam. Il est toujours recommandé de rester à jour et d'appliquer les derniers correctifs pour votre système StorageGRID .

Configuration de l'équilibreur de charge et du terminal S3

Dans Veeam, le terminal doit être connecté via HTTPS uniquement. Veeam ne prend pas en charge les connexions non chiffrées. Le certificat SSL peut être un certificat auto-signé, une autorité de certification privée de confiance ou une autorité de certification publique de confiance. Pour assurer un accès continu au référentiel S3, il est recommandé d'utiliser au moins deux équilibreurs de charge dans une configuration haute disponibilité. Les équilibreurs de charge peuvent être un service d'équilibrage de charge intégré fourni par StorageGRID, situé sur chaque nœud d'administration et nœud de passerelle ou sur une solution tierce telle que F5, Kemp, HASProxy, Loadbalancer.org, etc L'utilisation d'un équilibreur de charge StorageGRID permet de définir des classificateurs du trafic (règles de QoS) capables de hiérarchiser le workload Veeam ou de limiter Veeam à ne pas affecter les workloads prioritaires sur le système StorageGRID.

Compartiment S3

StorageGRID est un système de stockage multi-locataire sécurisé. Il est recommandé de créer un locataire dédié pour la charge de travail Veeam. Un quota de stockage peut être éventuellement attribué. En tant que bonne pratique, activez « Utiliser sa propre source d'identité ». Sécurisez l'utilisateur de gestion racine du locataire avec un mot de passe approprié. Veeam Backup 12 nécessite une forte cohérence pour les buckets S3. StorageGRID propose plusieurs options de cohérence configurées au niveau du bucket. Pour les déploiements multisites avec Veeam accédant aux données à partir de plusieurs emplacements, sélectionnez « strong-global ». Si les sauvegardes et restaurations Veeam s'effectuent sur un seul site, le niveau de cohérence doit être défini sur « site fort ». Pour plus d'informations sur les niveaux de cohérence des buckets, veuillez consulter le "documentation" . Pour utiliser StorageGRID pour les sauvegardes d'immuabilité Veeam, S3 Object Lock doit être activé globalement et configuré sur le bucket lors de la création du bucket.

Gestion du cycle de vie

StorageGRID prend en charge la réplication et le code d'effacement pour la protection au niveau objet sur l'ensemble des nœuds et sites StorageGRID. Le codage d'effacement requiert une taille d'objet d'au moins 200 Ko. La taille de bloc par défaut de Veeam de 1 Mo produit des tailles d'objet qui peuvent souvent être inférieures à cette taille minimale recommandée de 200 Ko après les fonctionnalités d'efficacité du stockage de Veeam. Pour les performances de la solution, il est déconseillé d'utiliser un profil de code d'effacement sur plusieurs sites, sauf si la connectivité entre les sites suffit pour ne pas augmenter la latence ou restreindre la bande passante du système StorageGRID. Dans un système StorageGRID multisite, la règle ILM peut être configurée pour stocker une copie unique sur chaque site. Pour une durabilité ultime, une règle pourrait être configurée de manière à stocker une copie codée en effacement sur chaque site. L'implémentation la plus recommandée pour cette charge de travail est l'utilisation de deux copies en local sur les serveurs Veeam Backup.

Supprimer les performances

Veeam fournit un réglage du taux de demande de suppression et une planification du processus de suppression de sauvegarde. Pour optimiser davantage les performances de suppression, vous pouvez désactiver les suppressions synchrones et laisser le scanner ILM gérer la suppression éventuelle des objets.

Étapes pour désactiver les suppressions synchrones

1. Ouvrez le gestionnaire de grille StorageGRID .
2. Dans le coin supérieur droit, sélectionnez le point d'interrogation puis Documentation API.
3. Dans le coin supérieur droit, cliquez sur le lien de la page de documentation de l'API privée.
4. Développer ilm-advanced.
5. Sélectionnez OBTENIR ilm-avancé.
6. Sélectionnez Essayer, puis Exécuter.
7. Vérifiez le résultat de la réponse.

    a. Si les valeurs sont nulles, cela signifie que les valeurs ilm-advanced par défaut sont utilisées.

    b. Si les valeurs ne sont pas nulles, cela signifie que des valeurs avancées ILM personnalisées sont utilisées. Copiez toutes les sorties après « données » :, en commençant par le { jusqu'à l'avant-dernier }.

        i. Enregistrez-le dans un éditeur de texte.

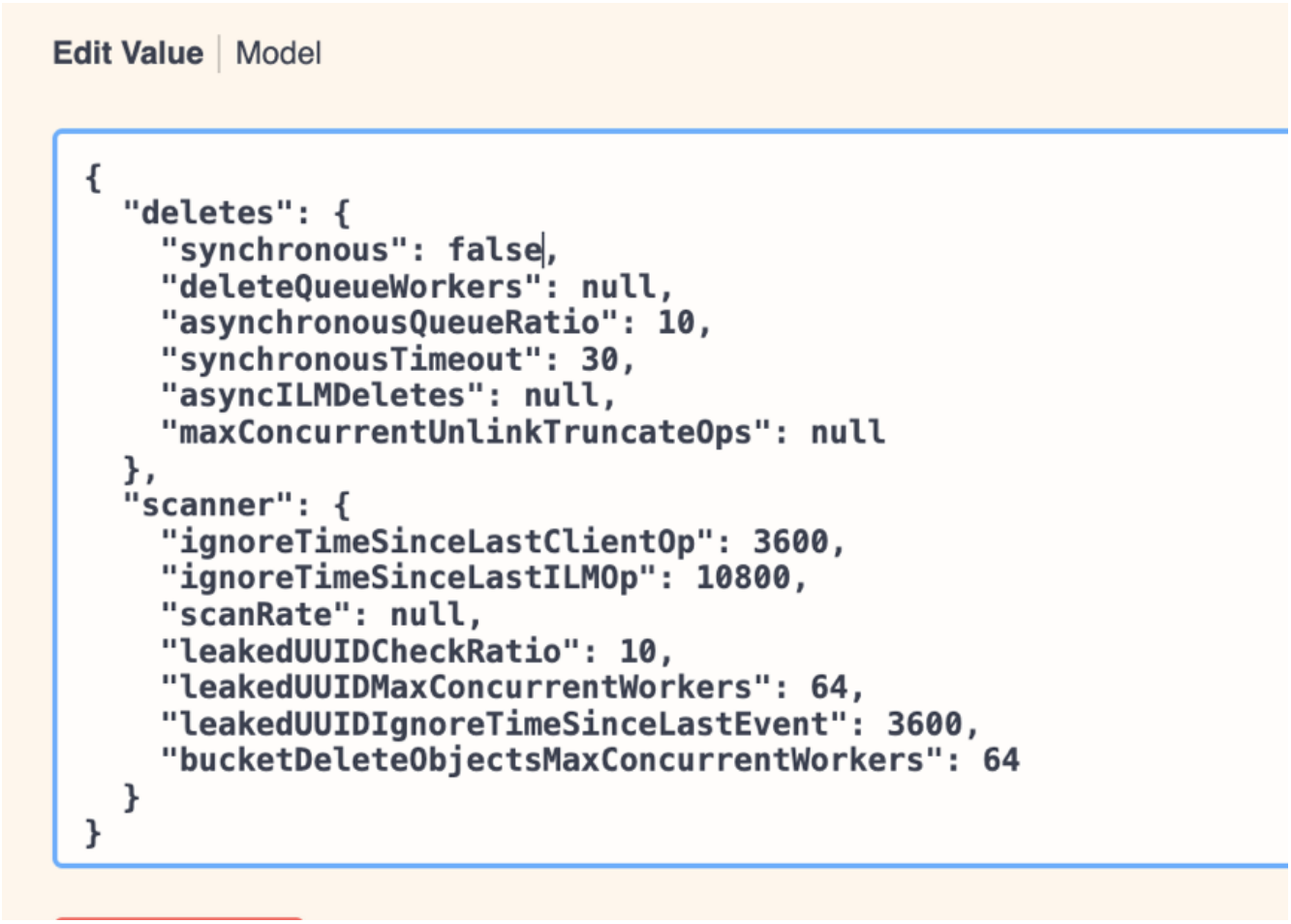
        Exemple de réponse :

Response body


```
{
  "responseTime": "2025-09-19T15:01:28.142Z",
  "status": "success",
  "apiVersion": "4.2",
  "data": {
    "deletes": {
      "synchronous": null,
      "deleteQueueWorkers": null,
      "asynchronousQueueRatio": null,
      "synchronousTimeout": null,
      "asyncILMDeletes": null,
      "maxConcurrentUnlinkTruncateOps": null
    },
    "scanner": {
      "ignoreTimeSinceLastClientOp": null,
      "ignoreTimeSinceLastILMOp": null,
      "scanRate": null,
      "leakedUUIDCheckRatio": null,
      "leakedUUIDMaxConcurrentWorkers": null,
      "leakedUUIDIgnoreTimeSinceLastEvent": null,
      "bucketDeleteObjectsMaxConcurrentWorkers": null
    }
  }
}
```


8. Sélectionnez PUT ilm-advanced.
9. Sélectionnez Essayer pour commencer à modifier le corps de l'API.
    a. Par défaut, le corps de l'API contiendra des valeurs par défaut et non des valeurs personnalisées précédemment configurées. C'est la raison pour laquelle il est TRÈS important d'exécuter les étapes 5 à 7.
10. Si des valeurs non par défaut sont trouvées à l'étape 5 à 7, remplacez le corps de l'API par la sortie enregistrée à l'étape 7. . Sinon, si les valeurs étaient nulles à l'étape 5-7, laissez le corps de l'API tel quel.
11. Ajustez les paramètres suivants dans la zone de corps de l'API :
    a. Définissez la valeur synchrone sur faux.

       Exemple de texte du corps de l'API :

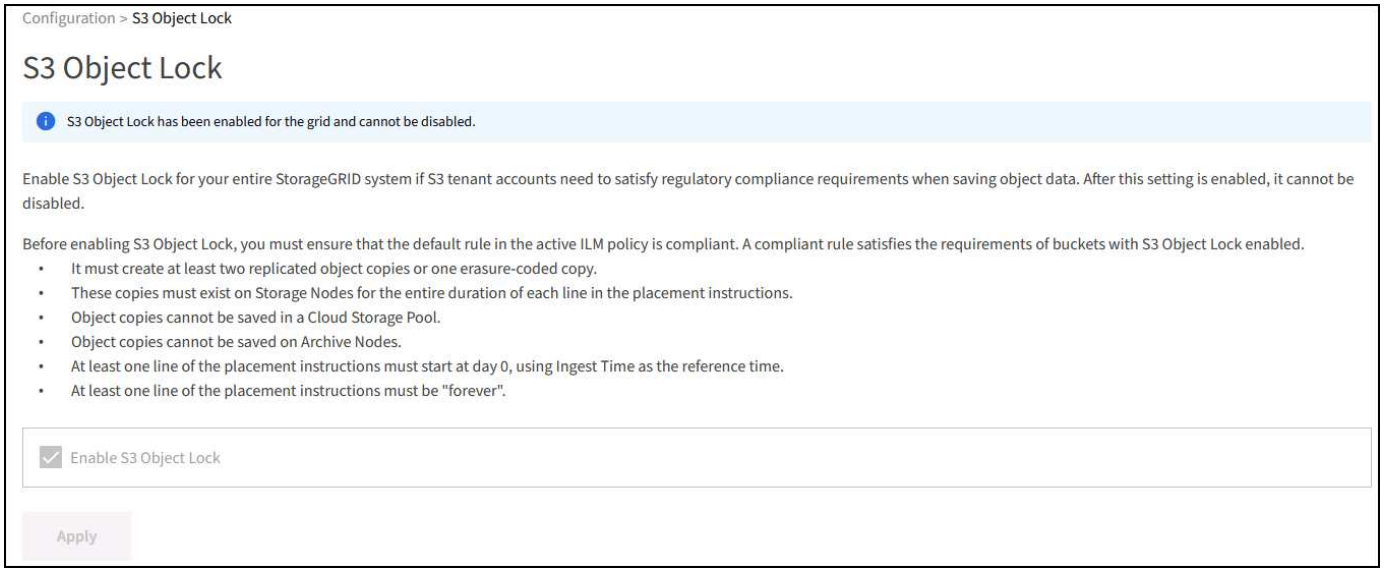


12. Une fois terminé, sélectionnez Exécuter

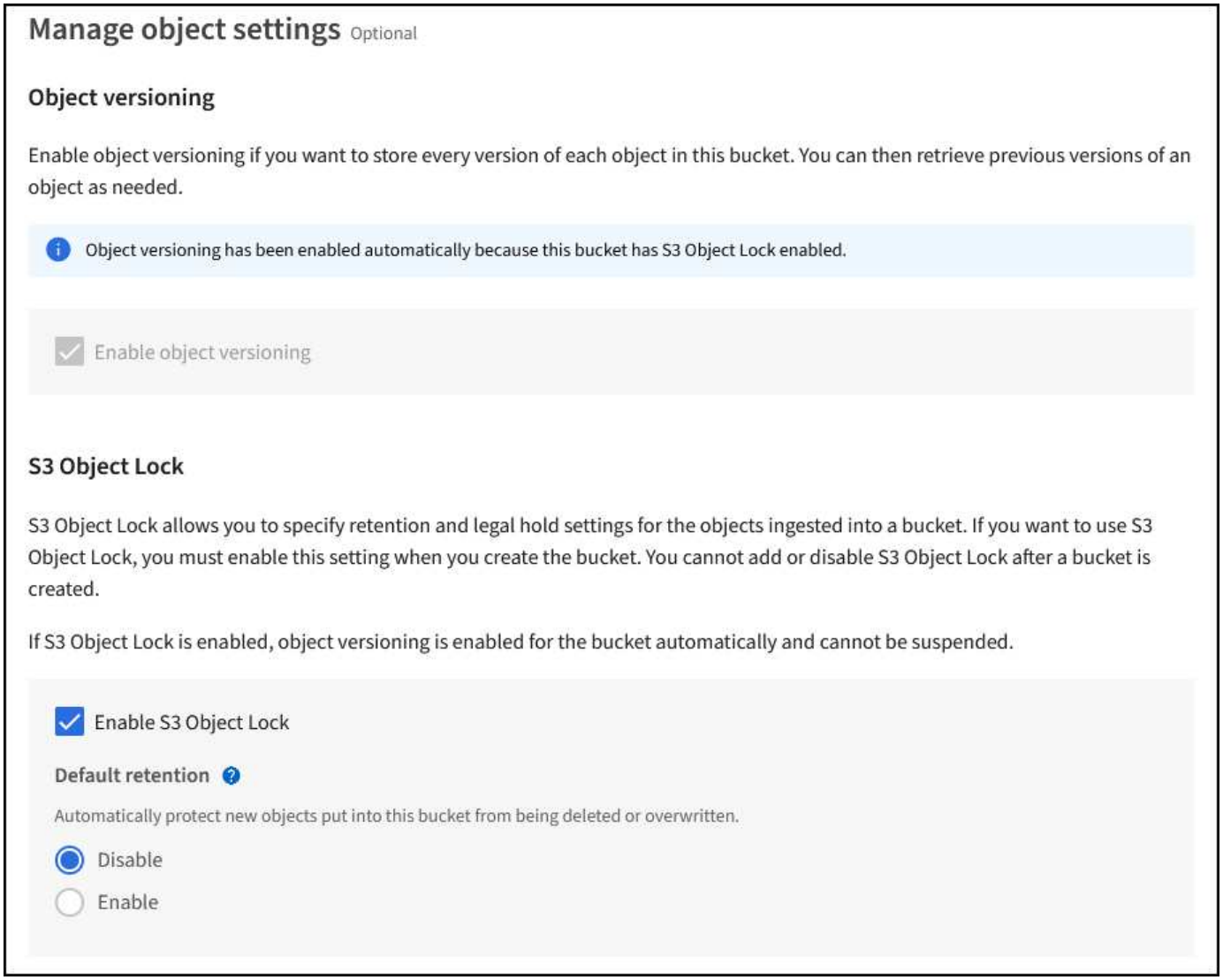
Points clés de la mise en œuvre

StorageGRID

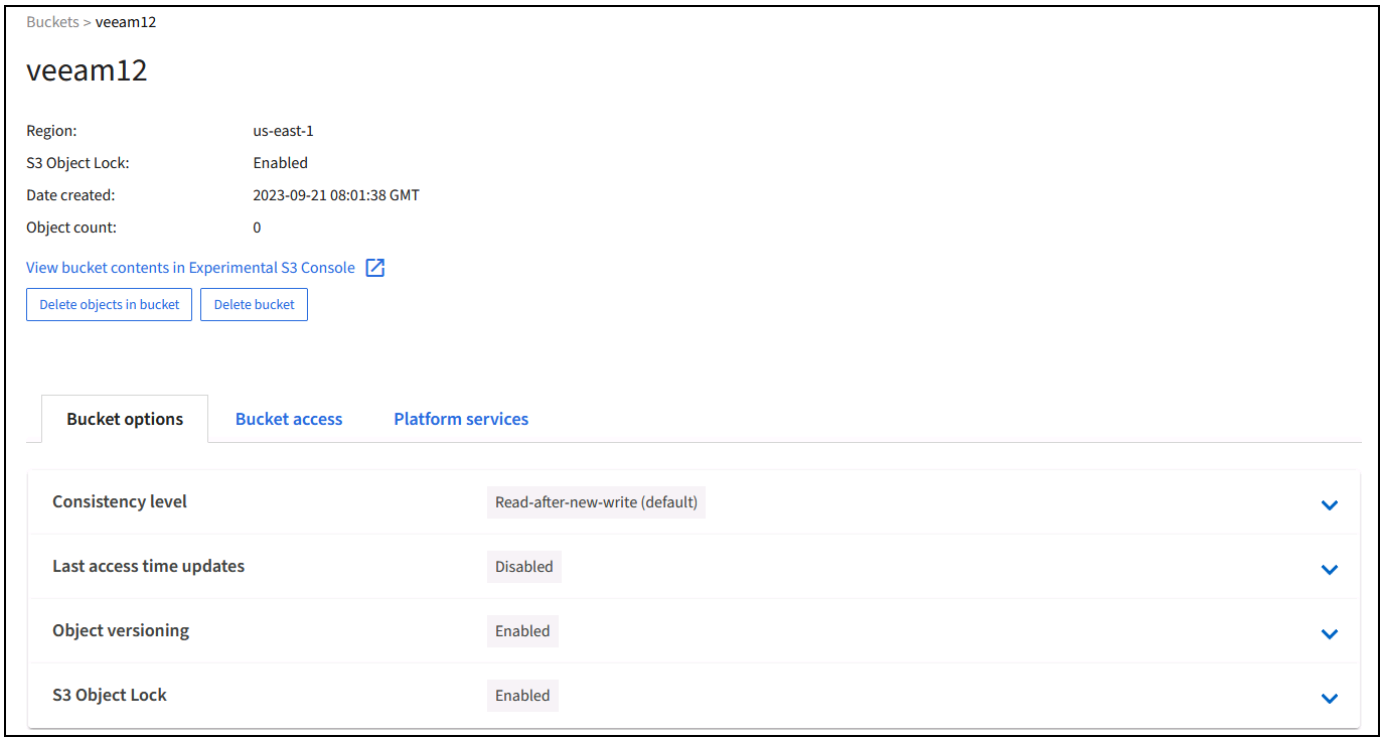
Assurez-vous que le verrouillage des objets est activé sur le système StorageGRID si l'immuabilité est requise. Recherchez l'option dans l'interface de gestion sous Configuration/S3 Object Lock.



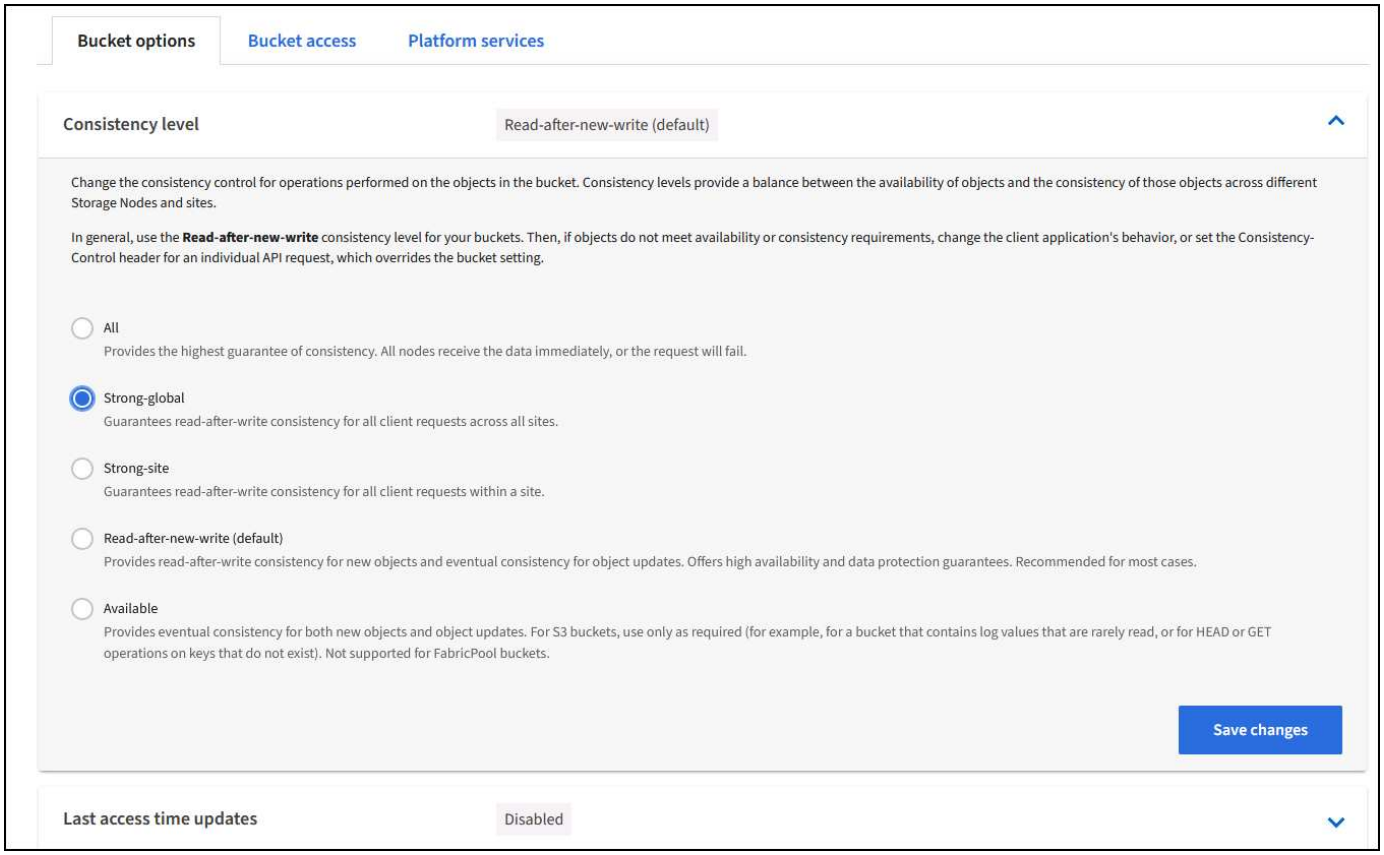
Lors de la création du compartiment, sélectionnez Activer le verrouillage des objets S3 si ce compartiment doit être utilisé pour les sauvegardes sans altération. La gestion des versions de compartiment est alors automatiquement activée. Laissez la conservation par défaut désactivée, car Veeam définit la conservation d'objet de manière explicite. La gestion des versions et le verrouillage objet S3 ne doivent pas être sélectionnés si Veeam ne crée pas de sauvegardes immuables.



Une fois le compartiment créé, accédez à la page de détails du compartiment créé. Sélectionnez le niveau de cohérence.



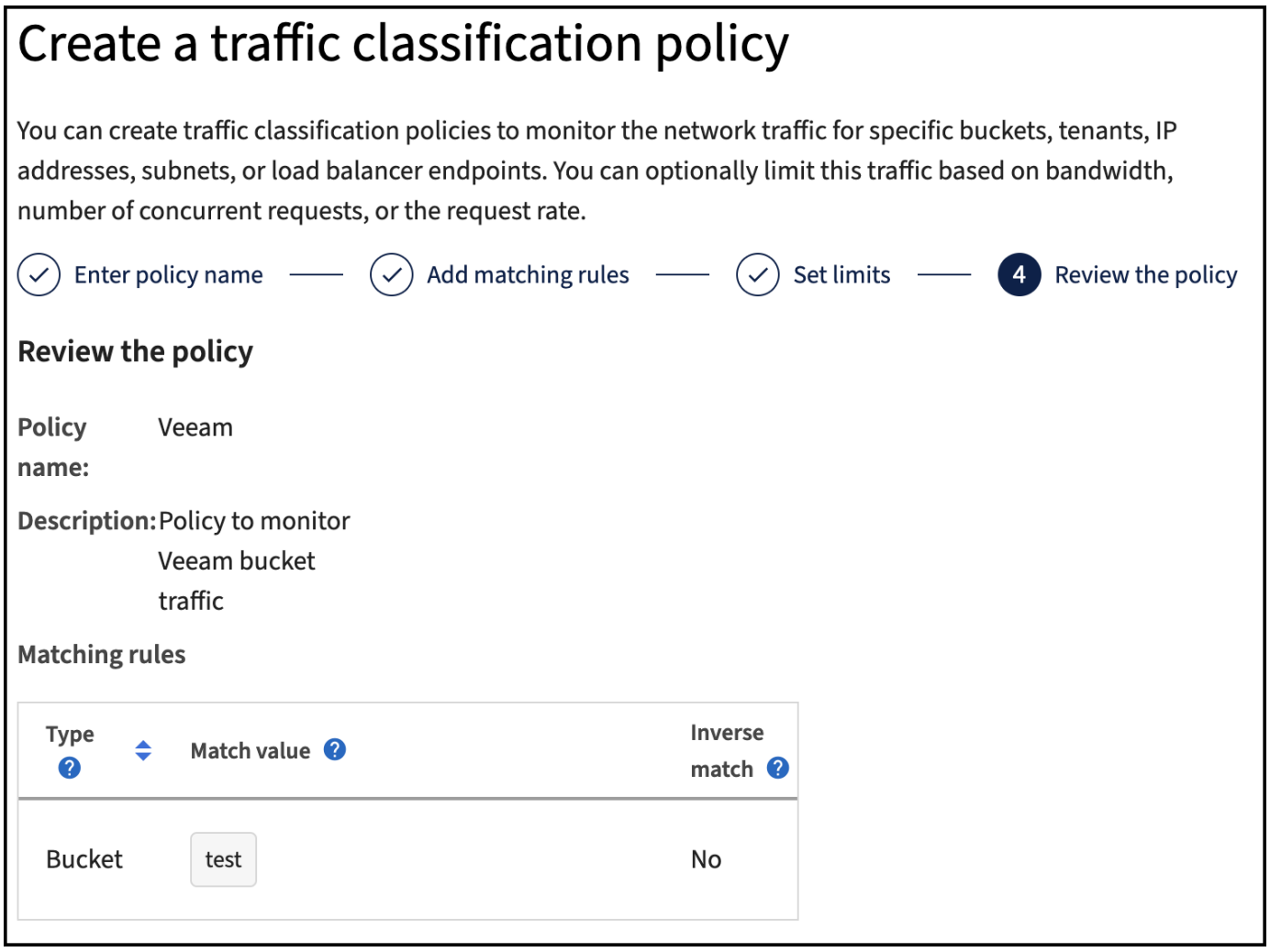
Veeam requiert une cohérence renforcée pour les compartiments S3. Pour les déploiements multi-sites avec Veeam qui accèdent aux données depuis plusieurs sites, sélectionnez « strong-global ». Si les sauvegardes et les restaurations Veeam ont lieu sur un seul site, le niveau de cohérence doit être défini sur « site à forte intensité ». Enregistrez les modifications.



StorageGRID propose un service d’équilibrage de la charge intégré sur chaque nœud d’administration et sur

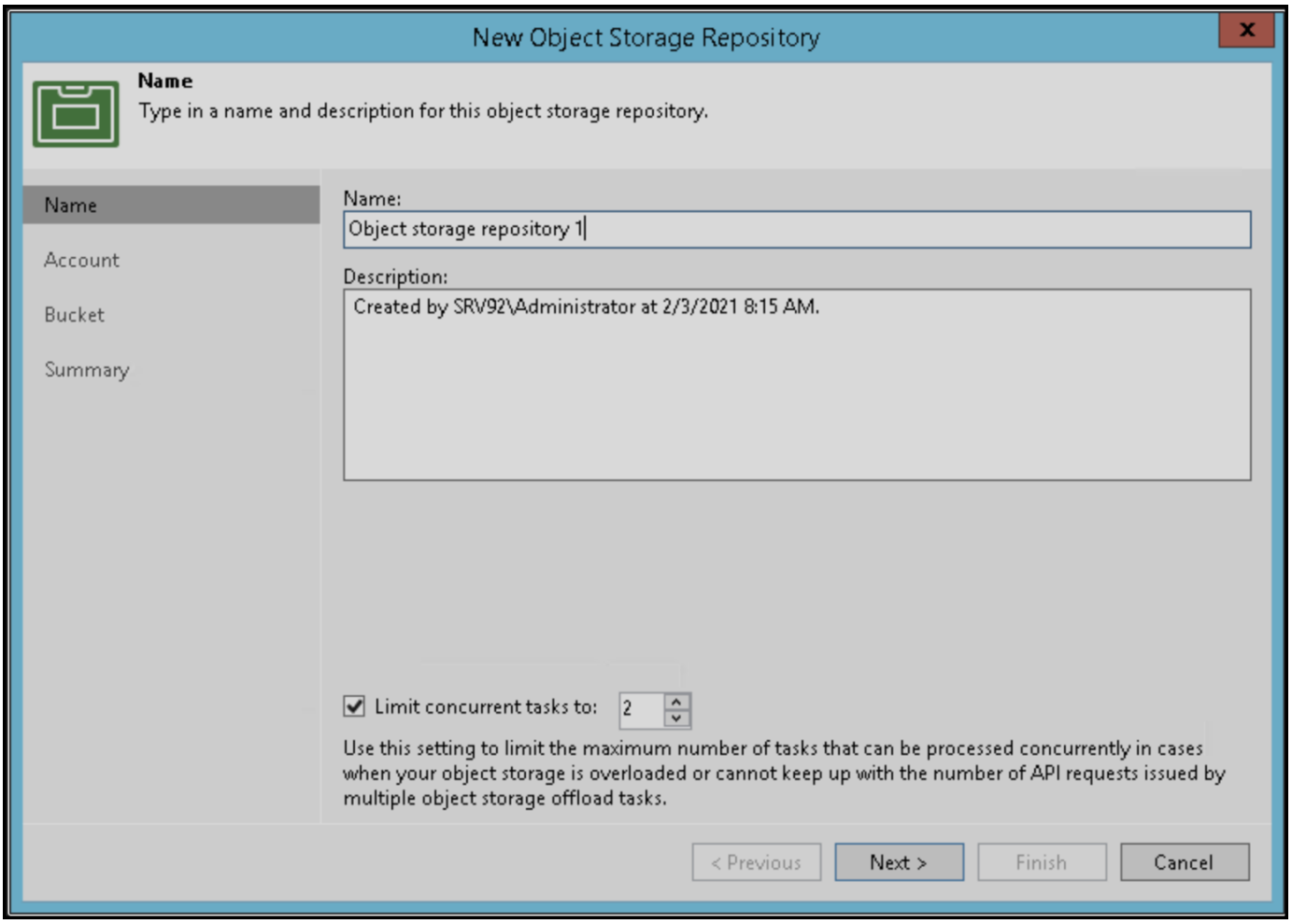
tous les nœuds de passerelle dédiés. L'un des nombreux avantages de l'utilisation de cet équilibreur de charge est la possibilité de configurer des règles de classification du trafic (QoS). Bien qu'elles soient principalement utilisées pour limiter l'impact des applications sur les autres charges de travail client ou pour hiérarchiser une charge de travail sur d'autres, elles fournissent également un bonus de collecte de metrics supplémentaires pour faciliter le contrôle.

Dans l'onglet de configuration, sélectionnez "classification du trafic" et créez une nouvelle stratégie. Attribuez un nom à la règle et sélectionnez le ou les compartiments ou le tenant comme type. Entrez le(s) nom(s) du ou des compartiments ou du tenant. Si la qualité de service est requise, définissez une limite, mais pour la plupart des implémentations, il convient d'ajouter les avantages en termes de surveillance, afin de ne pas fixer de limite.

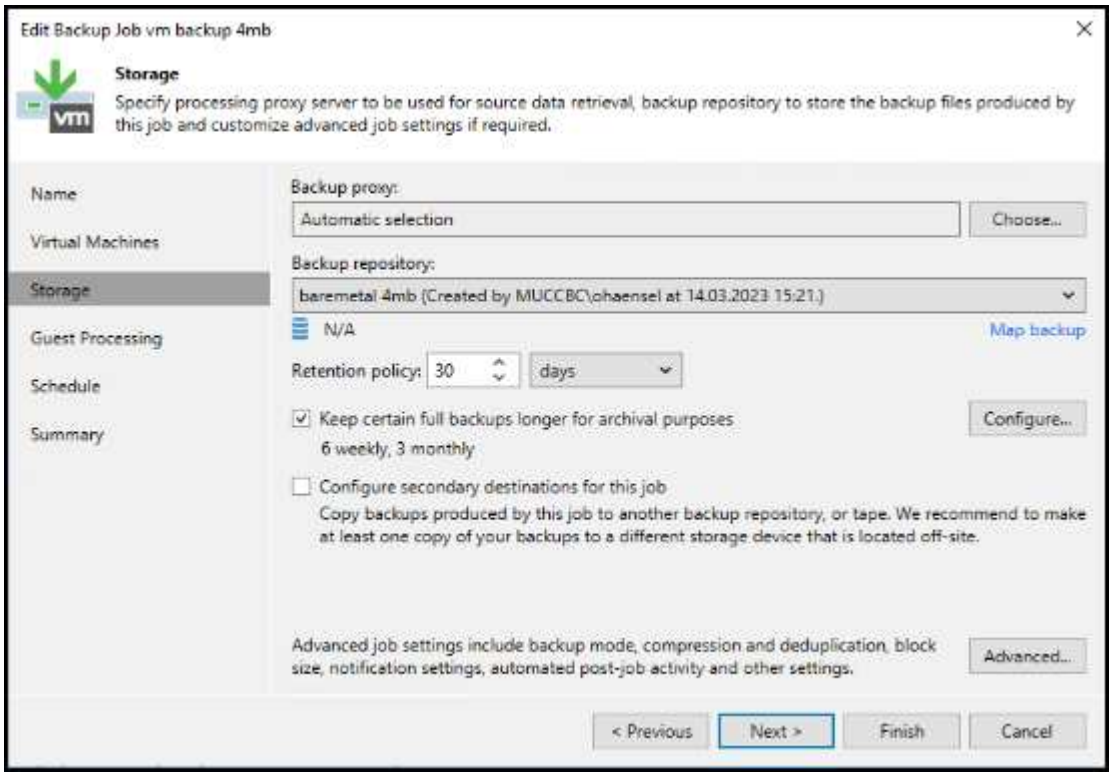


Veeam

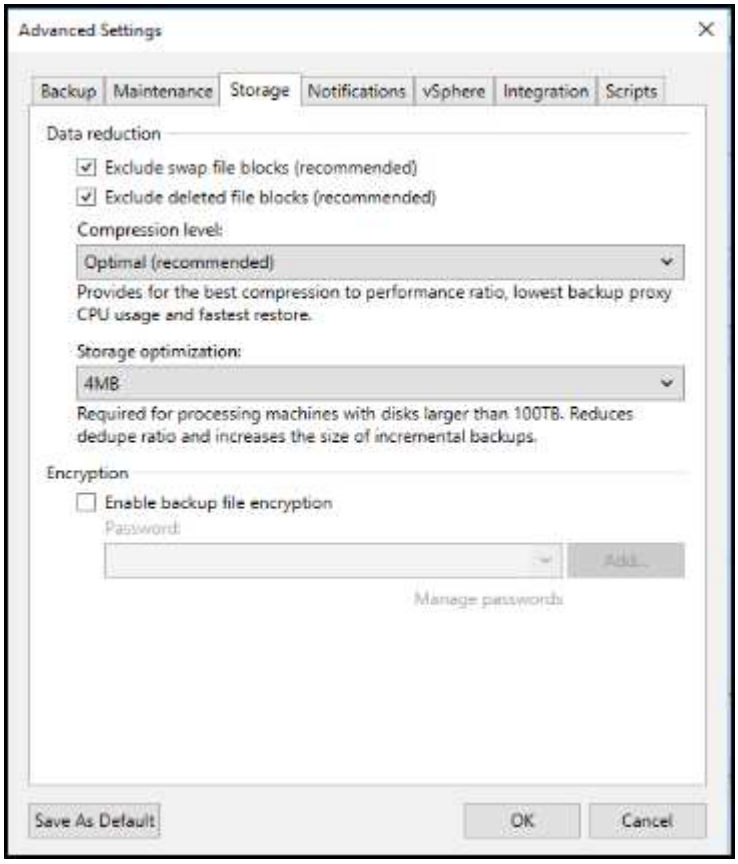
Selon le modèle et la quantité d'appliances StorageGRID, il peut être nécessaire de sélectionner et de configurer une limite au nombre d'opérations simultanées sur le compartiment.



Pour démarrer l'assistant, suivez la documentation Veeam sur la configuration des tâches de sauvegarde dans la console Veeam. Après avoir ajouté des machines virtuelles, sélectionnez le référentiel SOBR.



Cliquez sur Paramètres avancés et définissez les paramètres d'optimisation du stockage sur 4 Mo ou plus. La compression et la déduplication doivent être activées. Modifiez les paramètres invités en fonction de vos besoins et configurez la planification des tâches de sauvegarde.



Surveillance StorageGRID

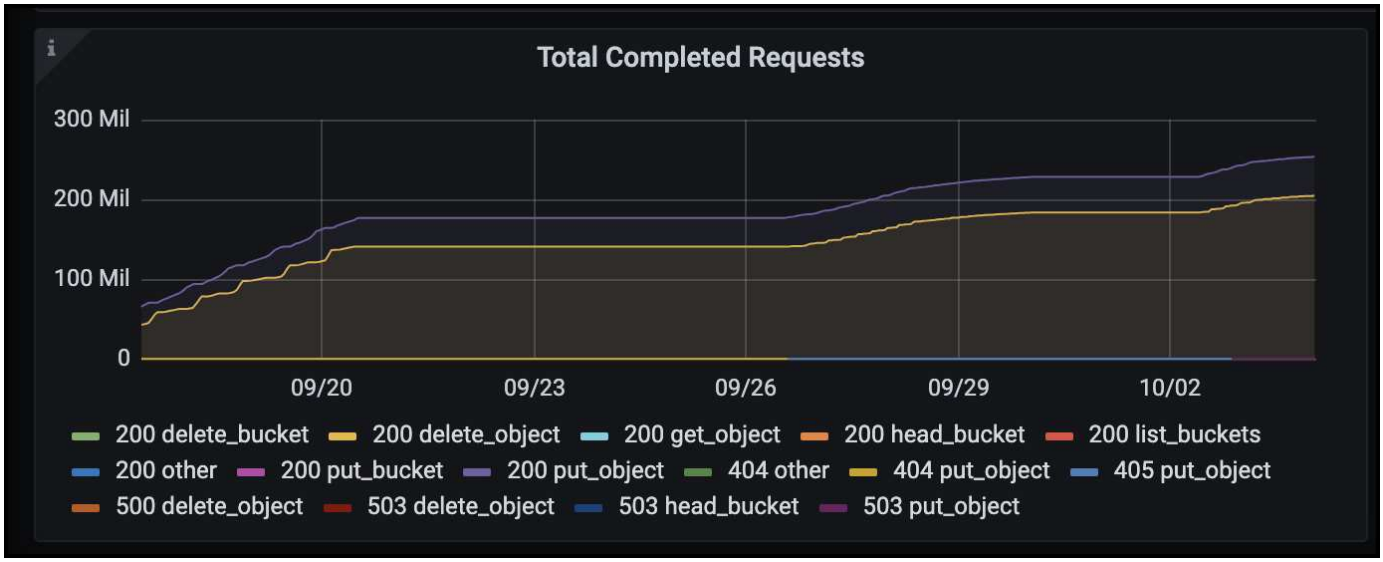
Pour obtenir une vue d'ensemble des performances de Veeam et StorageGRID, vous devez attendre l'expiration du délai de conservation des premières sauvegardes. Jusqu'à présent, la charge de travail Veeam se compose principalement d'opérations PUT et aucune suppression n'a eu lieu. Une fois que les données de sauvegarde arrivent à expiration et que les nettoyages sont en cours, vous pouvez voir l'utilisation cohérente complète du magasin d'objets et ajuster les paramètres dans Veeam, si nécessaire.

StorageGRID fournit des graphiques pratiques pour contrôler le fonctionnement du système, disponibles dans l'onglet support, page Metrics. Les principaux tableaux de bord à examiner seront la vue d'ensemble S3, ILM et la règle de classification du trafic si une règle a été créée. Vous trouverez dans le tableau de bord S3 des informations sur les taux d'opération S3, les latences et les réponses aux demandes.

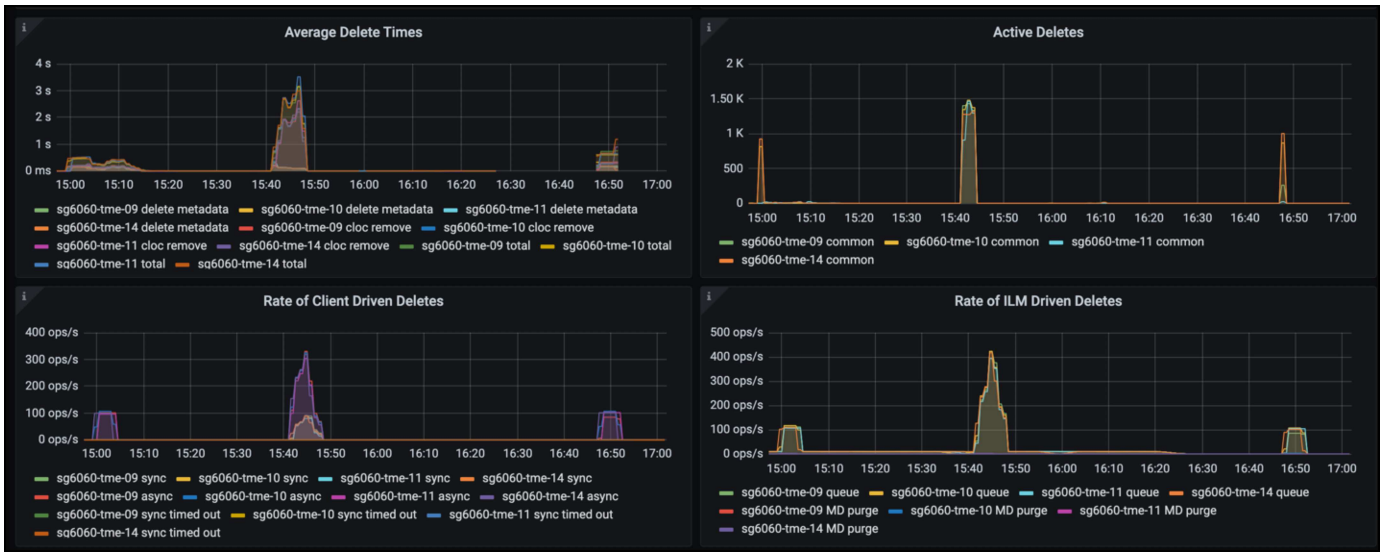
Les taux S3 et les requêtes actives vous permettent de voir la charge que chaque nœud gère et le nombre total de requêtes par type.

Le graphique durée moyenne indique la durée moyenne de chaque nœud pour chaque type de demande. Il s'agit de la latence moyenne de la demande et peut être un bon indicateur qu'un réglage supplémentaire peut être nécessaire ou que le système StorageGRID peut prendre plus de charge.

Dans le tableau nombre total de demandes terminées, vous pouvez voir les demandes par type et par code de réponse. Si vous voyez des réponses autres que 200 (OK), cela peut indiquer un problème comme le système StorageGRID est fortement chargé et envoie 503 réponses (ralentissement) et un réglage supplémentaire peut être nécessaire, ou le temps est venu d'étendre le système pour augmenter la charge.



Le tableau de bord ILM vous permet de contrôler les performances de suppression de votre système StorageGRID. StorageGRID combine les suppressions synchrones et asynchrones sur chaque nœud afin d'essayer d'optimiser la performance globale de toutes les requêtes.



Dans le cadre d'une règle de classification du trafic, nous pouvons afficher des metrics sur le débit de la demande d'équilibrage de charge, les taux, la durée, ainsi que la taille des objets envoyés et reçus par Veeam.

Où trouver des informations complémentaires

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

- "Documentation du produit NetApp StorageGRID"
- "Sauvegarde et réplication Veeam"

Configurez la source de données Dremio avec StorageGRID

Par Angela Cheng

Dremio prend en charge la rareté des sources de données, y compris le stockage objet dans le cloud ou sur site. Vous pouvez configurer Dremio pour qu'il utilise StorageGRID comme source de données de stockage objet.

Configurer la source de données Dremio

Prérequis

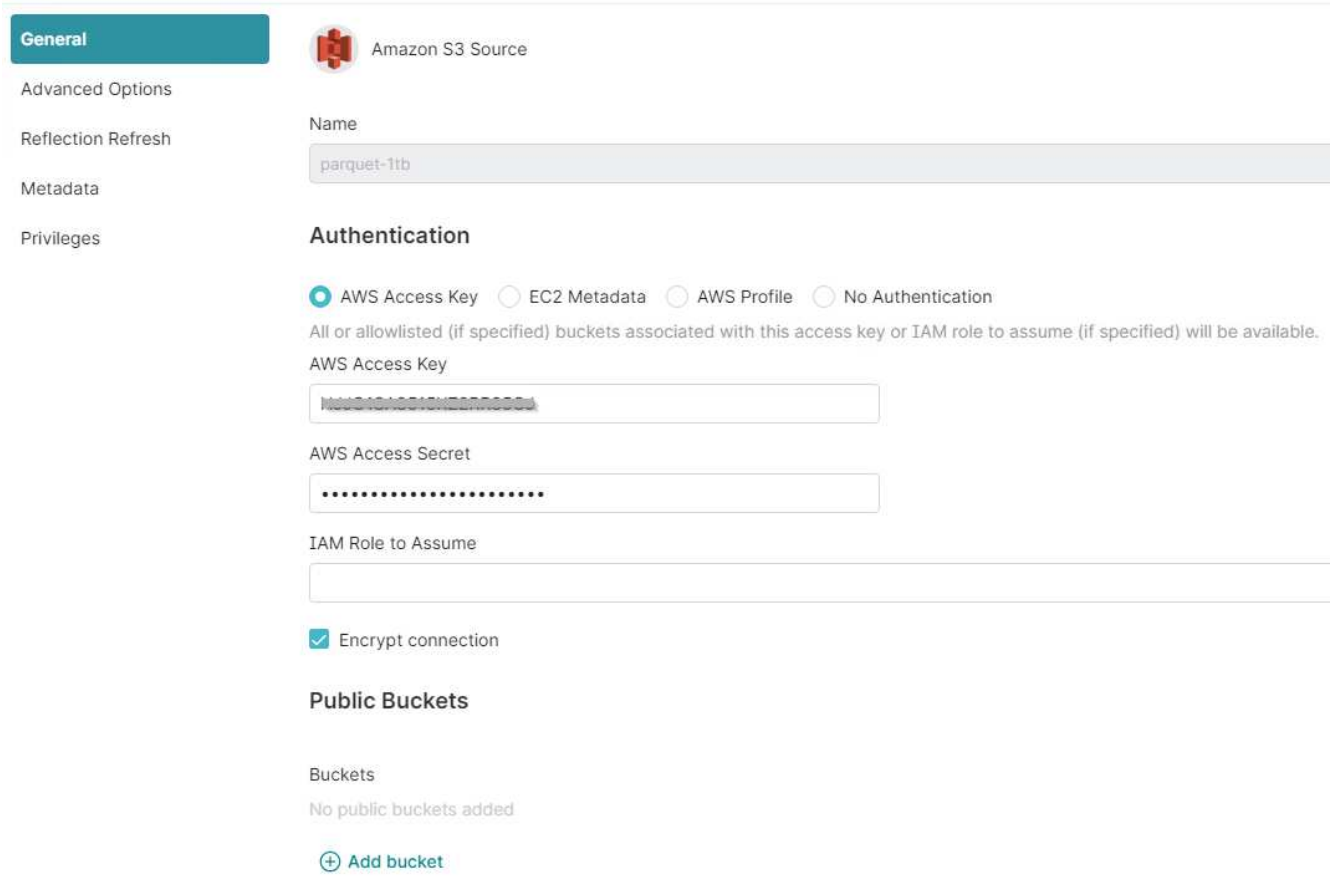
- URL de terminal StorageGRID S3, ID de clé d'accès s3 du locataire et clé d'accès secrète.
- Recommandation de configuration StorageGRID : désactivez la compression (désactivée par défaut). Dremio utilise la plage d'octets GET pour extraire simultanément différentes plages d'octets à partir du même objet pendant la requête. La taille type des demandes de plage d'octets est de 1 Mo. Les objets compressés dégradent les performances GET au niveau de la plage d'octets.

Guide Dremio

"Connexion à Amazon S3 : Configuration du stockage compatible avec S3".

Instructions

1. Sur la page Datasets Dremio, cliquez sur le signe + pour ajouter une source, sélectionnez 'Amazon S3'.
2. Entrez le nom de cette nouvelle source de données : ID de clé d'accès du locataire StorageGRID S3 et clé d'accès secrète.
3. Cochez la case « crypter la connexion » si vous utilisez https pour la connexion au terminal StorageGRID S3.
   Si vous utilisez un certificat CA auto-signé pour ce noeud final s3, suivez l'instructions du guide Dremio pour ajouter ce certificat CA dans <JAVA_HOME>/jre/lib/Security + du serveur Dremio
   Exemple de capture d'écran

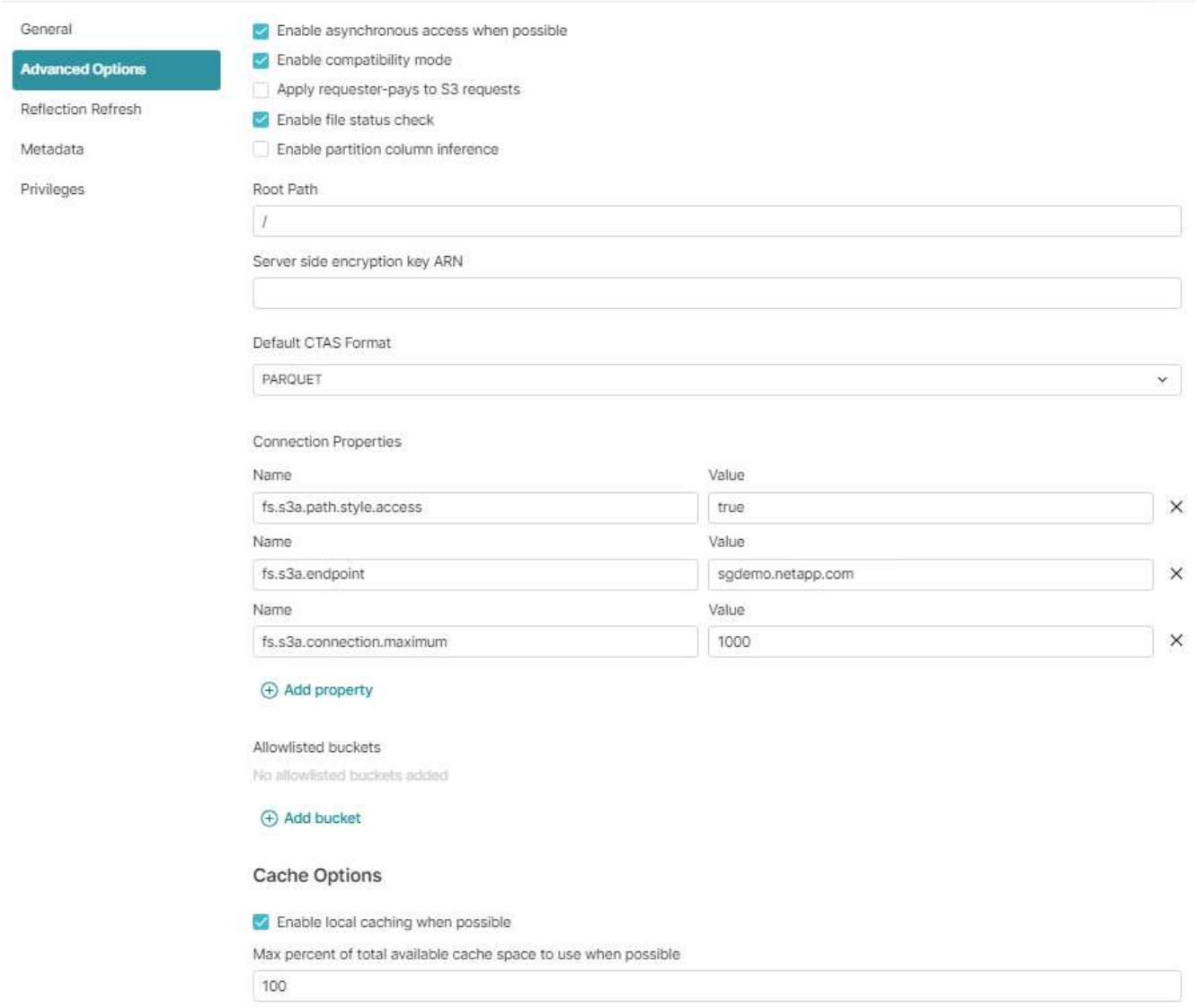


4. Cliquez sur « Options avancées », cochez « Activer le mode de compatibilité ».
5. Sous Propriétés de connexion, cliquez sur + Ajouter des propriétés et ajoutez ces propriétés s3a.

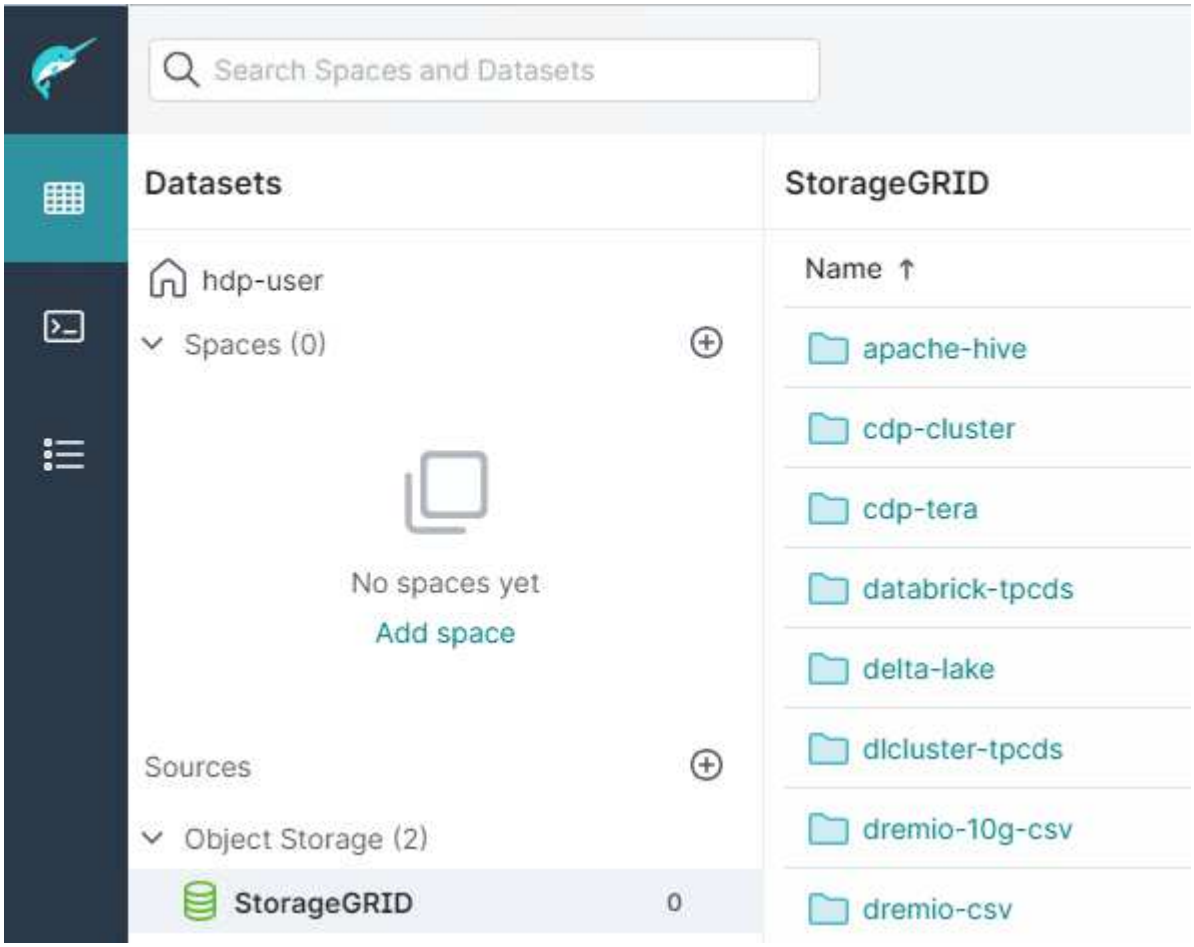
6. fs.s3a.connection.la valeur par défaut maximale est 100. Si vos datasets s3 incluent des fichiers de parquet volumineux comportant au moins 100 colonnes, vous devez entrer une valeur supérieure à 100. Reportez-vous au guide Dremio pour ce réglage.

Nom	Valeur
fs.s3a.endpoint	*<noeud final StorageGRID S3:port>*
fs.s3a.path.style.access	vrai
fs.s3a.connexion.maximum	*<une valeur supérieure à 100>*

Exemple de capture d'écran



7. Configurez les autres options de Dremio en fonction des besoins de votre organisation ou de vos applications.
8. Cliquez sur le bouton Enregistrer pour créer cette nouvelle source de données.
9. Une fois la source de données StorageGRID ajoutée, une liste de rubriques s'affiche dans le panneau de gauche.
   Exemple de capture d'écran



NetApp StorageGRID avec GitLab

Par Angela Cheng

NetApp a testé StorageGRID avec GitLab. Voir l'exemple de configuration GitLab ci-dessous. Reportez-vous à la section "Guide de configuration du stockage objet GitLab" pour plus d'informations.

Exemple de connexion de stockage objet

Pour les installations de package Linux, voici un exemple de `connection` configuration dans le formulaire consolidé. Modifier `/etc/gitlab/gitlab.rb` et ajoutez les lignes suivantes en remplaçant les valeurs souhaitées :

```
# Workaround for unexpected EOF errors with strict OpenSSL 3 / external
services
gitlab_rails['env'] = { 'SSL_IGNORE_UNEXPECTED_EOF' => '1' }

# Consolidated object storage configuration
gitlab_rails['object_store']['enabled'] = true
gitlab_rails['object_store']['proxy_download'] = true
gitlab_rails['object_store']['connection'] = {
  'provider' => 'AWS',
```

```
  'region' => 'us-east-1',
  'endpoint' => 'https://<storagegrid-s3-endpoint:port>',
  'path_stype' => 'true',
  'aws_access_key_id' => '<AWS_ACCESS_KEY_ID>',
  'aws_secret_access_key' => '<AWS_SECRET_ACCESS_KEY>'
}
# OPTIONAL: The following lines are only needed if server side encryption
is required
gitlab_rails['object_store']['storage_options'] = {
  'server_side_encryption' => 'AES256'
}
gitlab_rails['object_store']['objects']['artifacts']['bucket'] = 'gitlab-
artifacts'
gitlab_rails['object_store']['objects']['external_diffs']['bucket'] =
'gitlab-mr-diffs'
gitlab_rails['object_store']['objects']['lfs']['bucket'] = 'gitlab-lfs'
gitlab_rails['object_store']['objects']['uploads']['bucket'] = 'gitlab-
uploads'
gitlab_rails['object_store']['objects']['packages']['bucket'] = 'gitlab-
packages'
gitlab_rails['object_store']['objects']['dependency_proxy']['bucket'] =
'gitlab-dependency-proxy'
gitlab_rails['object_store']['objects']['terraform_state']['bucket'] =
'gitlab-terraform-state'
gitlab_rails['object_store']['objects']['pages']['bucket'] = 'gitlab-
pages'
```

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.