Guides des fonctionnalités des produits

How to enable StorageGRID in your environment

NetApp
April 26, 2024

Sommaire

Guides des fonctionnalités des produits

Création d'un pool de stockage cloud pour AWS ou Google Cloud

Vous pouvez utiliser un pool de stockage cloud pour déplacer des objets StorageGRID vers un compartiment S3 externe. Le compartiment externe peut appartenir à Amazon S3 (AWS) ou à Google Cloud.

Ce dont vous avez besoin

- StorageGRID 11.6 a été configuré.
- Vous avez déjà configuré un compartiment S3 externe sur AWS ou Google Cloud.

Étapes

1. Dans Grid Manager, accédez à **ILM** > **Storage pools**.
2. Dans la section Cloud Storage pools de la page, sélectionnez **Create**.

   La fenêtre contextuelle Créer un pool de stockage cloud s'affiche.

3. Entrez un nom d'affichage.
4. Sélectionnez **Amazon S3** dans la liste déroulante Type de fournisseur.

   Ce type de fournisseur fonctionne pour AWS S3 ou Google Cloud.

5. Entrez l'URI du compartiment S3 à utiliser pour le pool de stockage cloud.

   Deux formats sont autorisés :

   ```
   https://host:port
   ```

   ```
   http://host:port
   ```

6. Entrez le nom du compartiment S3.

   Le nom que vous spécifiez doit correspondre exactement au nom du compartiment S3. Sinon, la création du pool de stockage cloud échoue. Vous ne pouvez pas modifier cette valeur après l'enregistrement du pool de stockage cloud.

7. Vous pouvez également saisir l'ID de clé d'accès et la clé d'accès secrète.
8. Sélectionnez **ne pas vérifier le certificat** dans la liste déroulante.
9. Cliquez sur **Enregistrer**.

Résultat attendu

Assurez-vous qu'un pool de stockage cloud a été créé pour Amazon S3 ou Google Cloud.

Par Jonathan Wong

Création d’un pool de stockage cloud pour le stockage Azure Blob

Vous pouvez utiliser un pool de stockage cloud pour déplacer des objets StorageGRID vers un conteneur Azure externe.

Ce dont vous avez besoin

- StorageGRID 11.6 a été configuré.
- Vous avez déjà configuré un conteneur Azure externe.

Étapes

1. Dans Grid Manager, accédez à **ILM** > **Storage pools**.
2. Dans la section Cloud Storage pools de la page, sélectionnez **Create**.

   La fenêtre contextuelle Créer un pool de stockage cloud s’affiche.

3. Entrez un nom d’affichage.
4. Sélectionnez **Azure Blob Storage** dans la liste déroulante Type de fournisseur.
5. Entrez l’URI du compartiment S3 à utiliser pour le pool de stockage cloud.

   Deux formats sont autorisés :

   ```
   https://host:port
   ```

   ```
   http://host:port
   ```

6. Entrez le nom du conteneur Azure.

   Le nom que vous spécifiez doit correspondre exactement au nom du conteneur Azure. Sinon, la création du pool de stockage cloud échoue. Vous ne pouvez pas modifier cette valeur après l’enregistrement du pool de stockage cloud.

7. Vous pouvez également saisir le nom de compte et la clé de compte associés du conteneur Azure pour l’authentification.
8. Sélectionnez **ne pas vérifier le certificat** dans la liste déroulante.
9. Cliquez sur **Enregistrer**.

Résultat attendu

Confirmation de la création d’un pool de stockage cloud pour Azure Blob Storage

Par Jonathan Wong

Utilisation d’un pool de stockage cloud pour la sauvegarde

Vous pouvez créer une règle ILM pour déplacer des objets dans Cloud Storage Pool à des fins de sauvegarde.

Ce dont vous avez besoin

- StorageGRID 11.6 a été configuré.
- Vous avez déjà configuré un conteneur Azure externe.

Étapes

1. Dans Grid Manager, accédez à **ILM** > **règles** > **Créer**.
2. Entrez une description.
3. Entrez un critère pour déclencher la règle.
4. Cliquez sur **Suivant**.
5. Répliquez l'objet dans les nœuds de stockage.
6. Ajoutez une règle de placement.
7. Réplication de l'objet vers le pool de stockage cloud
8. Cliquez sur **Suivant**.
9. Cliquez sur **Enregistrer**.

Résultat attendu

Vérifiez que le diagramme de conservation affiche les objets stockés localement dans StorageGRID et dans un Cloud Storage Pool pour la sauvegarde.

Confirmez que, lorsque la règle ILM est déclenchée, une copie existe dans le pool de stockage cloud et vous pouvez récupérer l'objet localement sans effectuer de restauration d'objet.

Par Jonathan Wong

Configurez le service d'intégration de recherche StorageGRID

Ce guide fournit des instructions détaillées sur la configuration du service d'intégration de recherche NetApp StorageGRID 11.6 avec Amazon OpenSearch Service ou avec Elasticsearch sur site.

Introduction

StorageGRID prend en charge trois types de services de plateforme.

- **Réplication StorageGRID CloudMirror**. Mettre en miroir des objets spécifiques d'un compartiment StorageGRID vers une destination externe spécifiée.
- **Notifications**. Notifications d'événements par compartiment pour envoyer des notifications sur des actions spécifiques réalisées sur des objets vers un Amazon simple notification Service (Amazon SNS) externe spécifié.
- **Service d'intégration de recherche**. Envoyez les métadonnées d'objet S3 (simple Storage Service) à un index Elasticsearch spécifique où vous pouvez rechercher ou analyser les métadonnées à l'aide du service externe.

Les services de plateforme sont configurés par le locataire S3 via l'interface du gestionnaire des locataires. Pour plus d'informations, voir "Considérations relatives à l'utilisation des services de plate-forme".

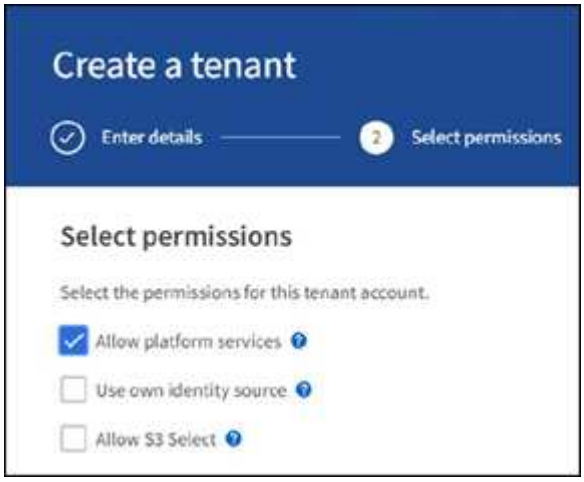
Ce document est un supplément au "Guide des locataires StorageGRID 11.6" et fournit des instructions

détaillées et des exemples de configuration du terminal et des compartiments pour les services d'intégration de la recherche. Les instructions d'installation d'Amazon Web Services (AWS) ou de Elasticsearch sur site indiquées ici sont fournies à des fins de test ou de démonstration uniquement.

Les participants doivent maîtriser Grid Manager et le Gestionnaire de locataires, et avoir accès au navigateur S3 pour effectuer des opérations de chargement (PUT) et de téléchargement (GET) de base pour les tests d'intégration de la recherche StorageGRID.

Créez des locataires et activez les services de plateforme

1. Créez un locataire S3 à l'aide de Grid Manager, entrez un nom d'affichage et sélectionnez le protocole S3.
2. Sur la page d'autorisation, sélectionnez l'option Autoriser les services de plate-forme. Vous pouvez également sélectionner d'autres autorisations, si nécessaire.



3. Configurez le mot de passe initial de l'utilisateur root du locataire ou, si la fédération identifier est activée sur la grille, sélectionnez le groupe fédéré disposant d'une autorisation d'accès racine pour configurer le compte du locataire.
4. Cliquez sur se connecter en tant que racine et sélectionnez godet : créer et gérer des godets.

   Vous accédez alors à la page Gestionnaire de locataires.

5. Dans le Gestionnaire des locataires, sélectionnez Mes clés d'accès pour créer et télécharger la clé d'accès S3 pour des tests ultérieurs.

Services d'intégration de recherche avec Amazon OpenSearch

Configuration du service Amazon OpenSearch (anciennement Elasticsearch

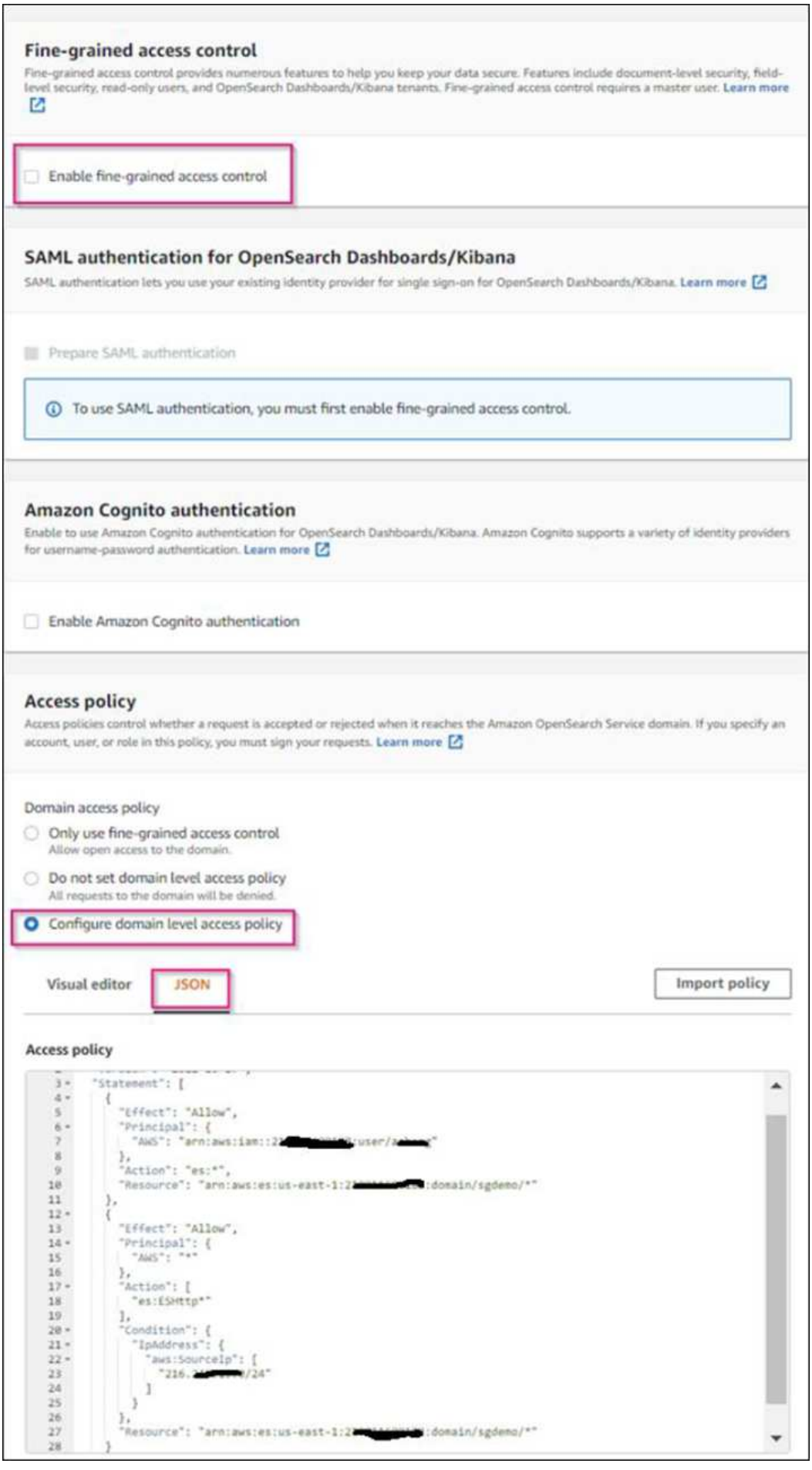
Utilisez cette procédure pour une configuration rapide et simple du service OpenSearch à des fins de test/démonstration uniquement. Si vous utilisez Elasticsearch sur site pour des services d'intégration de la recherche, consultez la section Services d'intégration de recherche avec Elasticsearch sur site.

Vous devez disposer d'un identifiant de console AWS valide, d'une clé d'accès, d'une clé d'accès secrète et d'une autorisation pour vous abonner au service OpenSearch.

1. Créez un nouveau domaine à l'aide des instructions de "Mise en route du service OpenSearch d'AWS", à l'exception de ce qui suit :

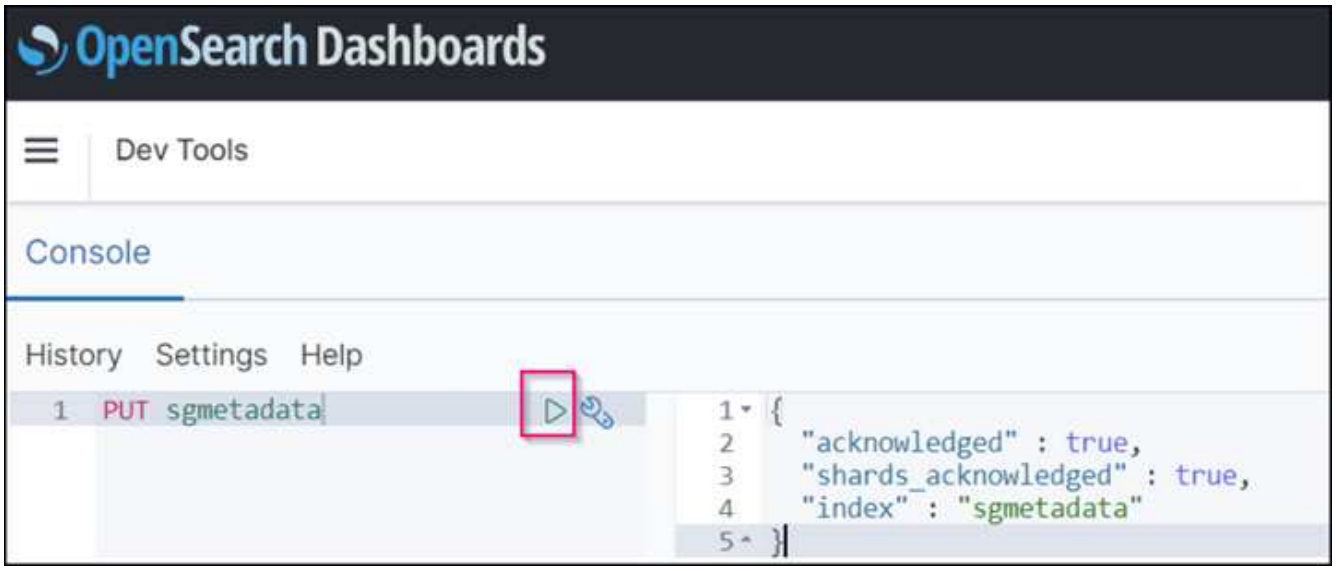
- Étape 4. Nom de domaine : sgdemo
- Étape 10. Contrôle d'accès de grain fin : désélectionnez l'option Activer le contrôle d'accès de grain fin.
- Étape 12. Règle d'accès : sélectionnez configurer la stratégie d'accès de niveau, sélectionnez l'onglet JSON pour modifier la stratégie d'accès en utilisant l'exemple suivant :
  - Remplacez le texte surligné par votre propre ID et nom d'utilisateur AWS Identity and Access Management (IAM).
  - Remplacez le texte en surbrillance (adresse IP) par l'adresse IP publique de votre ordinateur local utilisé pour accéder à la console AWS.
  - Ouvrez un onglet de navigateur pour "https://checkip.amazonaws.com" Pour trouver votre IP publique.

```
{

    "Version": "2012-10-17",
    "Statement": [
        {
        "Effect": "Allow",
        "Principal":
        {"AWS": "arn:aws:iam:: nnnnnn:user/xyzabc"},
        "Action": "es:*",
        "Resource": "arn:aws:es:us-east-1:nnnnnn:domain/sgdemo/*"
        },
        {
        "Effect": "Allow",
        "Principal": {"AWS": "*"},
        "Action": [
        "es:ESHttp*"
                ],
        "Condition": {
            "IpAddress": {
                "aws:SourceIp": [ "nnn.nnn.nn.n/nn"
                    ]
                }
        },
        "Resource": "arn:aws:es:us-east-1:nnnnnn:domain/sgdemo/*"
        }
    ]
}
```

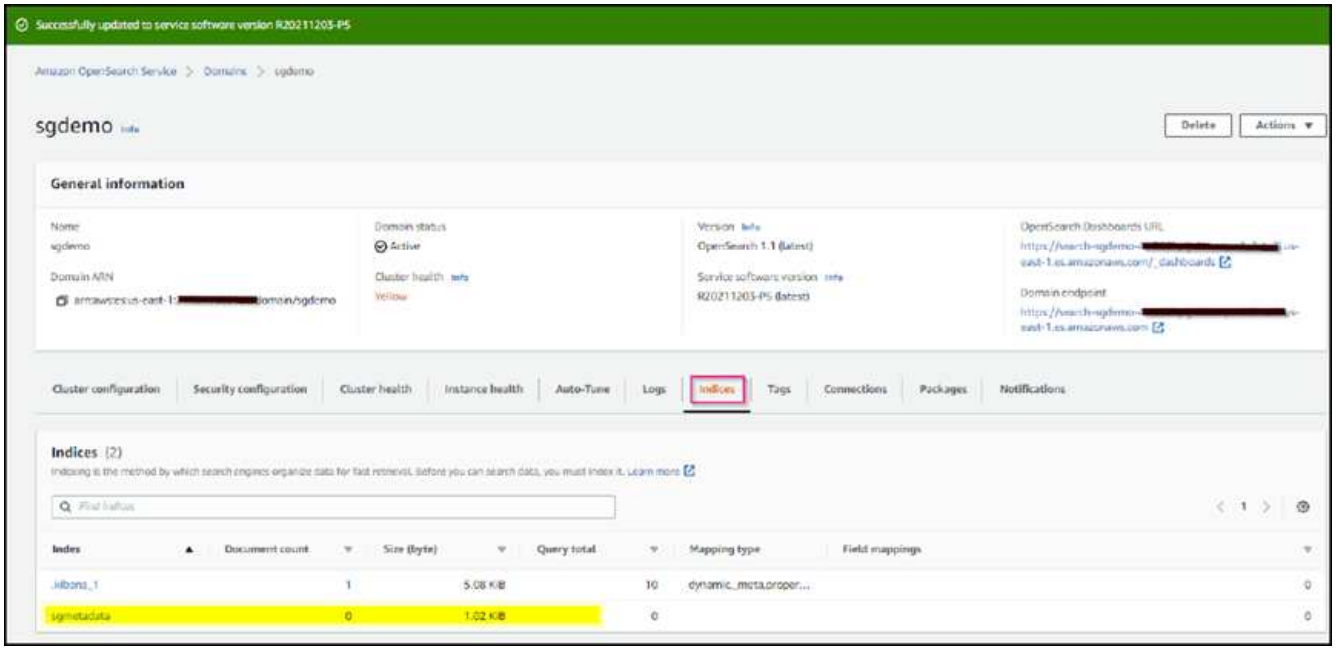

Fine-grained access control
Fine-grained access control provides numerous features to help you keep your data secure. Features include document-level security, field-level security, read-only users, and OpenSearch Dashboards/Kibana tenants. Fine-grained access control requires a master user. Learn more
Enable fine-grained access control
SAML authentication for OpenSearch Dashboards/Kibana
SAML authentication lets you use your existing identity provider for single sign-on for OpenSearch Dashboards/Kibana. Learn more
Prepare SAML authentication
To use SAML authentication, you must first enable fine-grained access control.
Amazon Cognito authentication
Enable to use Amazon Cognito authentication for OpenSearch Dashboards/Kibana. Amazon Cognito supports a variety of identity providers for username-password authentication. Learn more
Enable Amazon Cognito authentication
Access policy
Access policies control whether a request is accepted or rejected when it reaches the Amazon OpenSearch Service domain. If you specify an account, user, or role in this policy, you must sign your requests. Learn more
Domain access policy
Only use fine-grained access control
Allow open access to the domain.
Do not set domain level access policy
All requests to the domain will be denied.
Configure domain level access policy
Visual editor
JSON
Import policy
Access policy
"Statement": [
{
"Effect": "Allow",
"Principal": {
"AWS": "arn:aws:iam::2[redacted]:user/A[redacted]"
},
"Action": "es:*",
"Resource": "arn:aws:es:us-east-1:2[redacted]:domain/sgdemo/*"
},
{
"Effect": "Allow",
"Principal": {
"AWS": "*"
},
"Action": [
"es:ESHttp*"
],
"Condition": {
"IpAddress": {
"aws:SourceIp": [
"216.[redacted]/24"
]
}
},
"Resource": "arn:aws:es:us-east-1:2[redacted]:domain/sgdemo/*"
}

2. Attendez 15 à 20 minutes pour que le domaine devienne actif.

3. Cliquez sur OpenSearch tableaux de bord URL pour ouvrir le domaine dans un nouvel onglet pour accéder au tableau de bord. Si vous obtenez une erreur d'accès refusé, vérifiez que l'adresse IP source de la stratégie d'accès est correctement définie sur l'adresse IP publique de votre ordinateur pour autoriser l'accès au tableau de bord du domaine.
4. Sur la page d'accueil du tableau de bord, sélectionnez Explorer de votre choix. Dans le menu, accédez à Management → Dev Tools
5. Sous Outils de développement → Console , entrez `PUT <index>` Où vous utilisez l'index pour le stockage des métadonnées d'objet StorageGRID. Nous utilisons le nom d'index 'gmetadatas' dans l'exemple suivant. Cliquez sur le petit symbole de triangle pour exécuter la commande PUT. Le résultat attendu s'affiche dans le panneau de droite comme indiqué dans l'exemple d'écran suivant.



6. Vérifiez que l'index est visible depuis l'interface utilisateur Amazon OpenSearch sous sgdomain > indices.

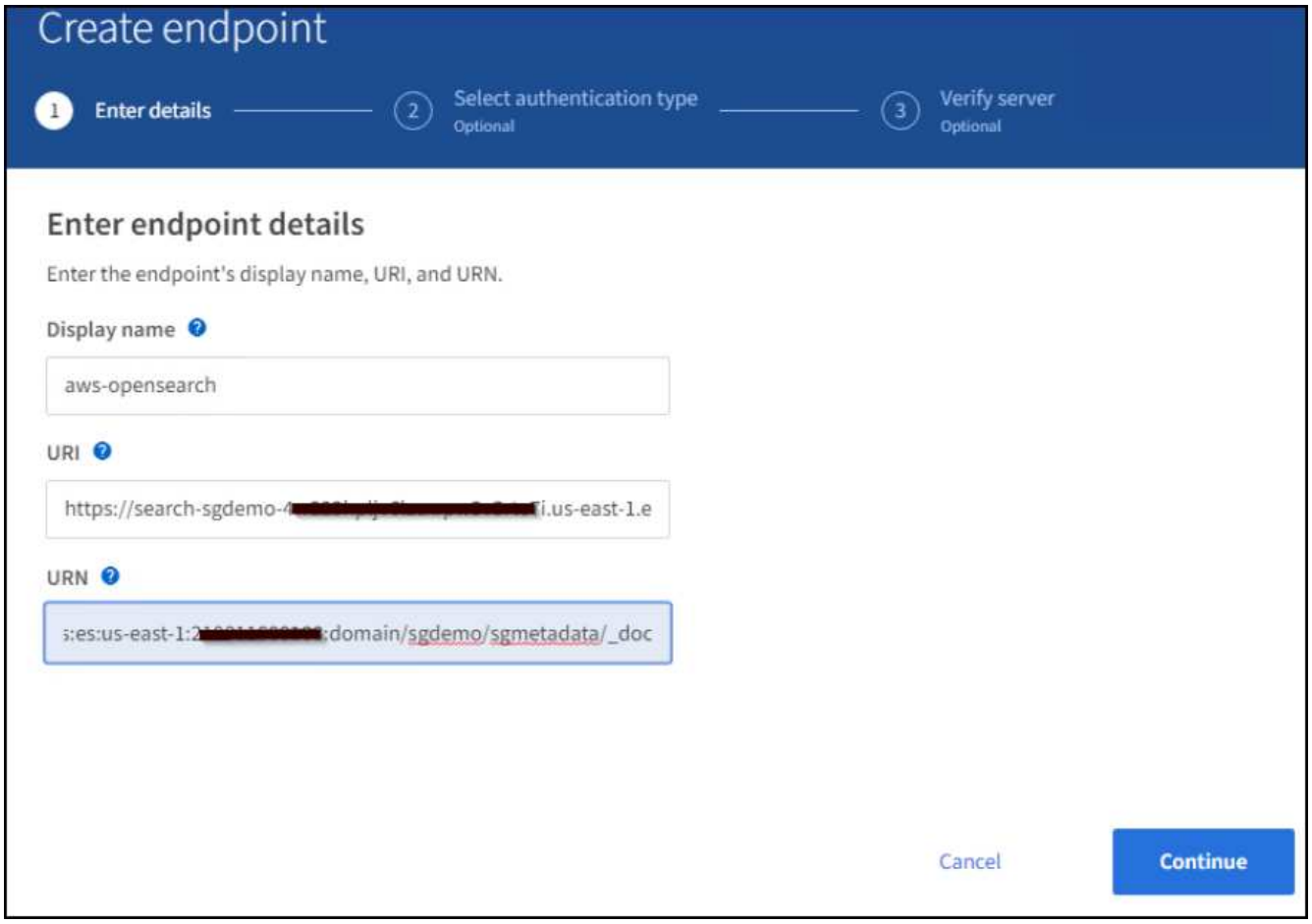


Configuration du terminal des services de plate-forme

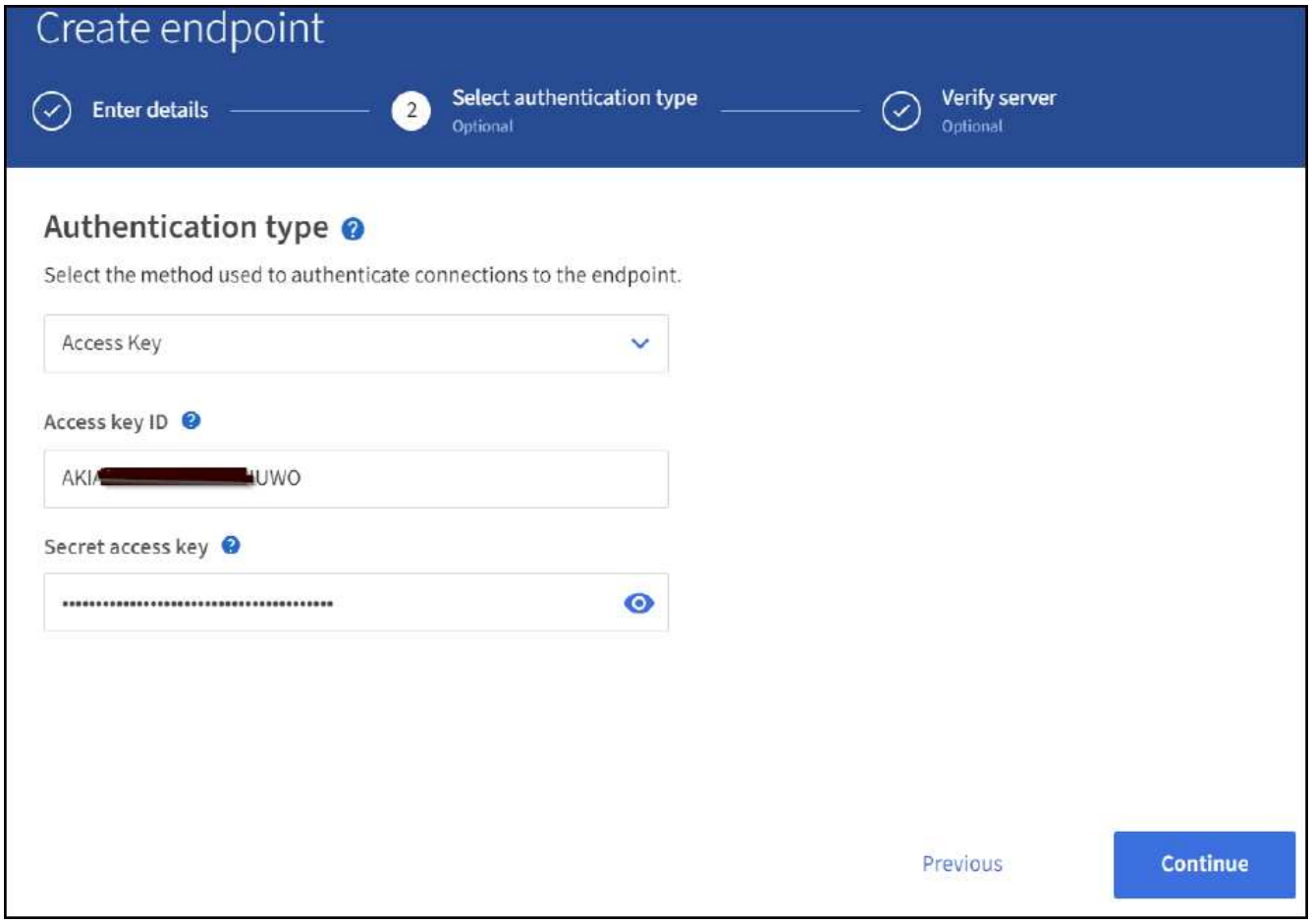
Pour configurer les terminaux des services de plate-forme, procédez comme suit :

1. Dans tenant Manager, accédez à STORAGE(S3) > terminaux des services de plateforme.
2. Cliquez sur Créer un point final, entrez les informations suivantes, puis cliquez sur Continuer :
   - Exemple de nom d'affichage `aws-opensearch`
   - Le noeud final du domaine dans la capture d'écran de l'exemple sous l'étape 2 de la procédure précédente dans le champ URI.
   - Le domaine ARN utilisé à l'étape 2 de la procédure précédente dans le champ URN et ajouter `/<index>/_doc` Jusqu'à la fin de l'ARN.

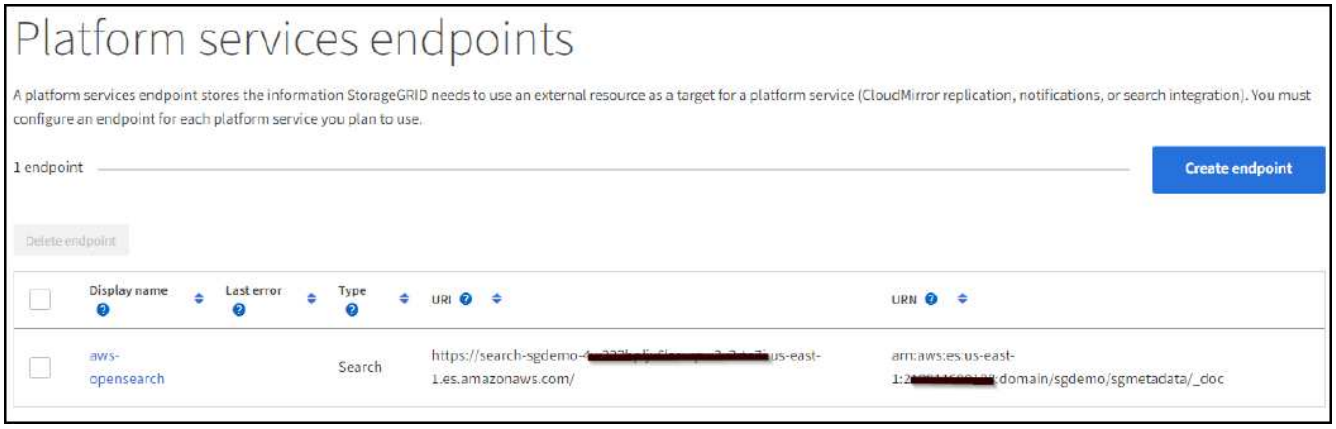
     Dans cet exemple, l'URN devient `arn:aws:es:us-east-1:211234567890:domain/sgdemo/sgmedata/_doc`.



3. Pour accéder au domaine Amazon OpenSearch sgdomain, choisissez Access Key comme type d'authentification, puis entrez la clé d'accès Amazon S3 et la clé secrète. Pour passer à la page suivante, cliquez sur Continuer.



4. Pour vérifier le noeud final, sélectionnez utiliser le certificat CA du système d'exploitation et tester et Créer un noeud final. Si la vérification réussit, un écran de point final similaire à la figure suivante s'affiche. En cas d'échec de la vérification, vérifiez que l'URN inclut `/<index>/_doc` À l'issue du chemin, la clé d'accès AWS et la clé secrète sont correctes.



Services d'intégration de recherche avec Elasticsearch sur site

Configuration Elasticsearch sur site

Cette procédure permet une configuration rapide des données sur site Elasticsearch et Kibana utilisant docker uniquement à des fins de test. Si le serveur Elasticsearch et Kibana existent déjà, passez à l'étape 5.

1. Suivez ceci "Procédure d'installation de Docker" pour installer docker. Nous utilisons le "Procédure d'installation de CentOS Docker" dans cette configuration.

```
sudo yum install -y yum-utils
sudo yum-config-manager --add-repo
https://download.docker.com/linux/centos/docker-ce.repo
sudo yum install docker-ce docker-ce-cli containerd.io
sudo systemctl start docker
```

   - Pour démarrer docker après le redémarrage, entrez les informations suivantes :

```
sudo systemctl enable docker
```

   - Réglez le `vm.max_map_count` valeur jusqu'à 262144 :

```
sysctl -w vm.max_map_count=262144
```

   - Pour conserver le paramètre après le redémarrage, saisissez les informations suivantes :

```
echo 'vm.max_map_count=262144' >> /etc/sysctl.conf
```

2. Suivez le "Guide de démarrage rapide d'Elasticsearch" Section auto-gérée pour installer et exécuter Elasticsearch et Kibana docker. Dans cet exemple, nous avons installé la version 8.1.

Notez le nom d'utilisateur/mot de passe et le jeton créés par Elasticsearch, vous devez utiliser ces éléments pour démarrer l'interface utilisateur Kibana et l'authentification du terminal de la plateforme StorageGRID.

Elasticsearch Service | Self-managed

Install and run Elasticsearch

1. Install and start Docker Desktop.
2. Run:

```
docker network create elastic
docker pull docker.elastic.co/elasticsearch/elasticsearch:8.1.0
docker run --name es-node01 --net elastic -p 9200:9200 -p 9300:9300 -it
```

When you start Elasticsearch for the first time, the following security configuration occurs automatically:

- Certificates and keys are generated for the transport and HTTP layers.
- The Transport Layer Security (TLS) configuration settings are written to `elasticsearch.yml`.
- A password is generated for the `elastic` user.
- An enrollment token is generated for Kibana.

NOTE You might need to scroll back a bit in the terminal to view the password and enrollment token.

3. Copy the generated password and enrollment token and save them in a secure location. These values are shown only when you start Elasticsearch for the first time. You'll use these to enroll Kibana with your Elasticsearch cluster and log in.

NOTE If you need to reset the password for the `elastic` user or other built-in users, run the `elasticsearch-reset-password` tool. To generate new enrollment tokens for Kibana or Elasticsearch nodes, run the `elasticsearch-create-enrollment-token` tool. These tools are available in the Elasticsearch `bin` directory.

Install and run Kibana

To analyze, visualize, and manage Elasticsearch data using an intuitive UI, install Kibana.

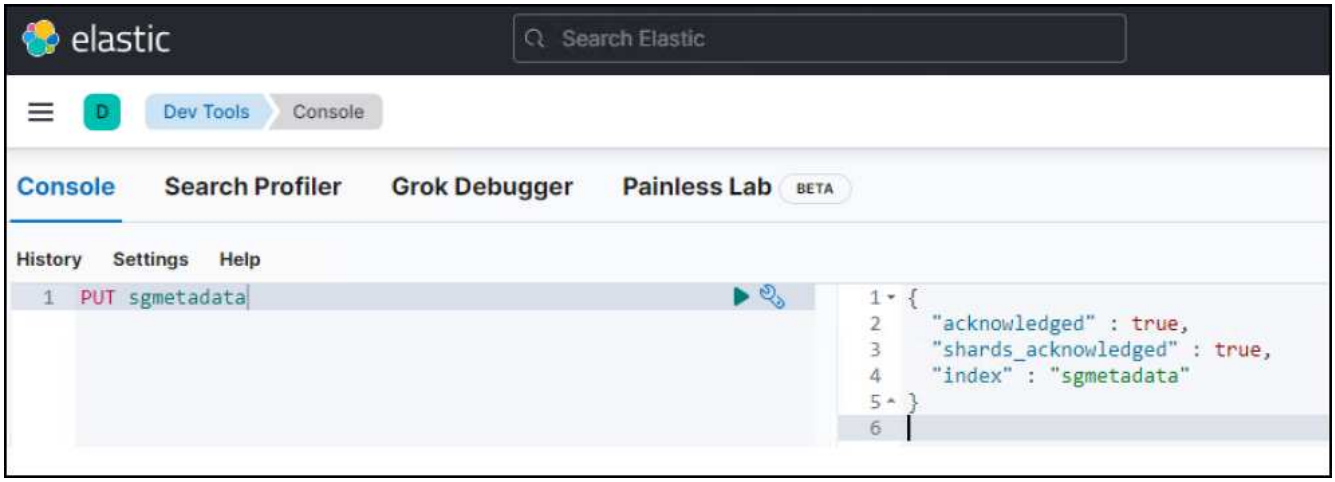
1. In a new terminal session, run:

```
docker pull docker.elastic.co/kibana/kibana:8.1.0
docker run --name kib-01 --net elastic -p 5601:5601 docker.elastic.co/ki
```

When you start Kibana, a unique link is output to your terminal.

2. To access Kibana, click the generated link in your terminal.
   a. In your browser, paste the enrollment token that you copied and click the button to connect your Kibana instance with Elasticsearch.
   b. Log in to Kibana as the `elastic` user with the password that was generated when you started Elasticsearch.

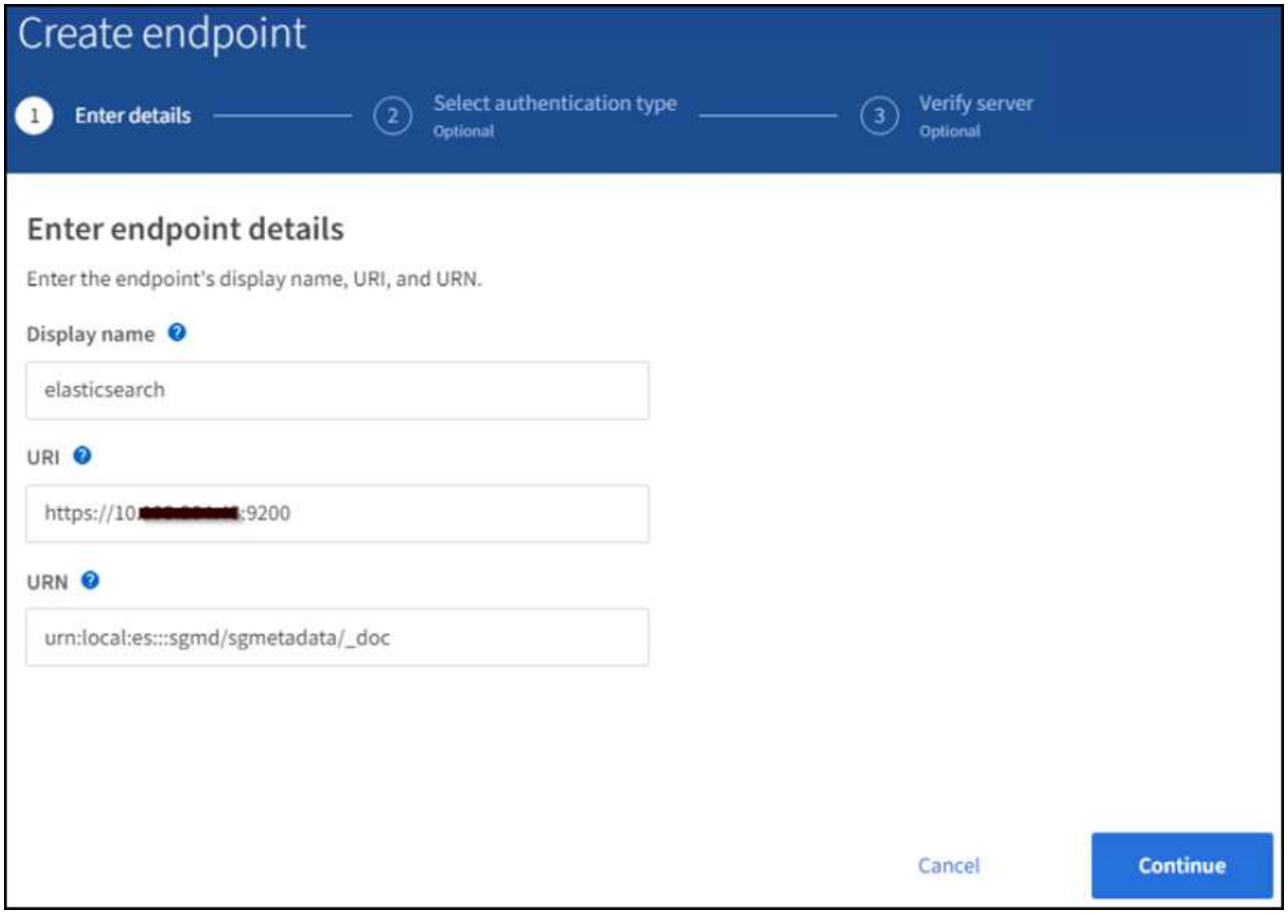
3. Après le démarrage du conteneur kibana docker, le lien URL `https://0.0.0.0:5601` s'affiche dans la console. Remplacez 0.0.0.0 par l'adresse IP du serveur dans l'URL.
4. Connectez-vous à l'interface utilisateur Kibana en utilisant le nom d'utilisateur `elastic` Et le mot de passe généré par Elastic dans l'étape précédente.
5. Pour la première connexion, sur la page d'accueil du tableau de bord, sélectionnez Explorer par vous-même. Dans le menu, sélectionnez gestion > Outils de développement.
6. Sur l'écran Console des outils de développement, entrez `PUT <index>` Où vous utilisez cet index pour stocker les métadonnées des objets StorageGRID. Nous utilisons le nom de l'index `sgmetadata` dans cet exemple. Cliquez sur le petit symbole de triangle pour exécuter la commande PUT. Le résultat attendu s'affiche dans le panneau de droite comme indiqué dans l'exemple d'écran suivant.



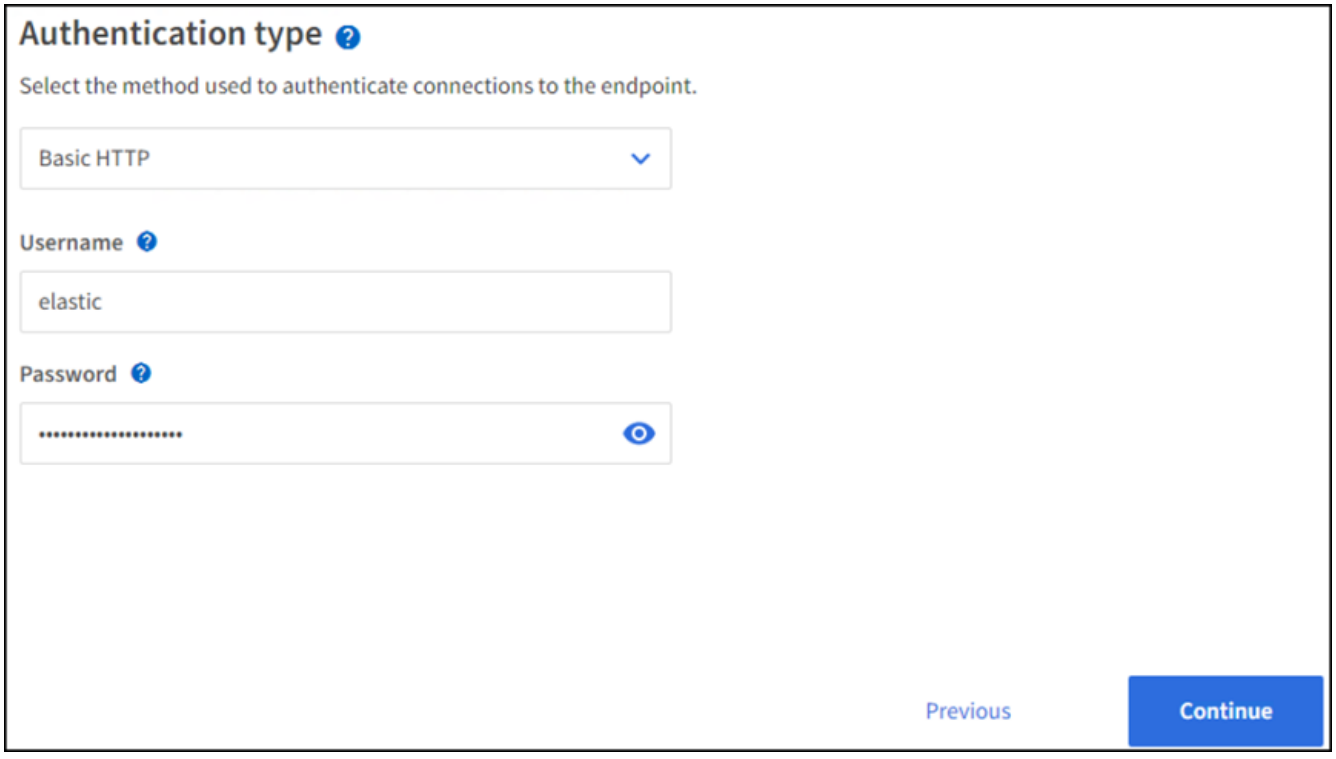
Configuration du terminal des services de plate-forme

Pour configurer les terminaux pour les services de plate-forme, procédez comme suit :

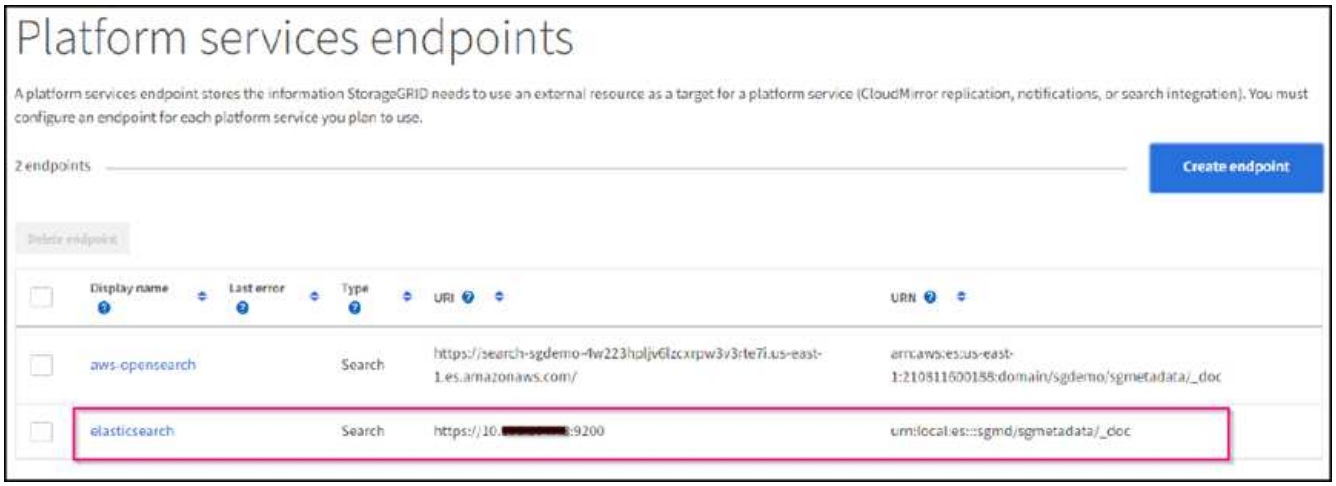
1. Dans tenant Manager, accédez à STORAGE(S3) > terminaux des services de plateforme
2. Cliquez sur Créer un point final, entrez les informations suivantes, puis cliquez sur Continuer :
   - Exemple de nom d'affichage : `elasticsearch`
   - URI : `https://<elasticsearch-server-ip or hostname>:9200`
   - URN : `urn:<something>:es:::<some-unique-text>/<index-name>/_doc` Où l'index-name est le nom que vous avez utilisé sur la console Kibana. Exemple : `urn:local:es:::sgmd/sgmetadata/_doc`



3. Sélectionnez Basic HTTP comme type d'authentification, saisissez le nom d'utilisateur `elastic` Et le mot de passe généré par le processus d'installation Elasticsearch. Pour passer à la page suivante, cliquez sur Continuer.



4. Sélectionnez ne pas vérifier le certificat et le test et Créer un noeud final pour vérifier le noeud final. Si la vérification est réussie, un écran de point final similaire à la capture d'écran suivante s'affiche. Si la vérification échoue, vérifiez que les entrées URN, URI et nom d'utilisateur/mot de passe sont correctes.



Configuration du service d'intégration de la recherche de compartiments

Une fois le terminal du service de plateforme créé, l'étape suivante consiste à configurer ce service au niveau du compartiment pour envoyer les métadonnées d'objet au terminal défini lors de la création ou de la suppression d'un objet, ou encore lors de la mise à jour de ses métadonnées ou balises.

Vous pouvez configurer l'intégration de la recherche à l'aide du Gestionnaire de locataires afin d'appliquer un code XML de configuration StorageGRID personnalisé à un compartiment comme suit :

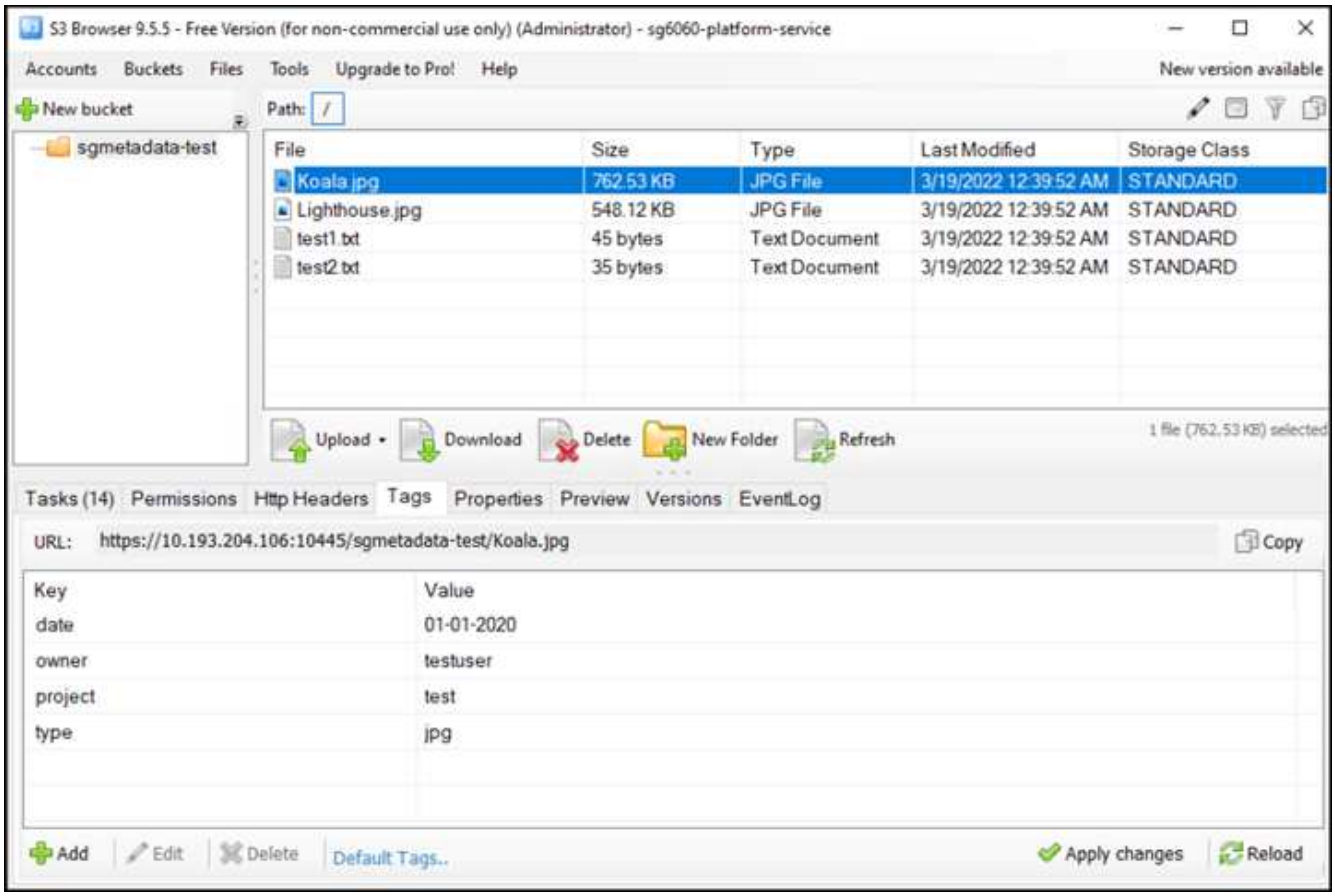
1. Dans le Gestionnaire des locataires, accédez à STORAGE(S3) > compartiments
2. Cliquez sur Créer un compartiment, entrez le nom du compartiment (par exemple, `sgmetadata-test`) et acceptez la valeur par défaut `us-east-1` région.
3. Cliquez sur Continuer > Créer un compartiment.
4. Pour afficher la page de présentation du compartiment, cliquez sur le nom du compartiment, puis sélectionnez Platform Services.
5. Sélectionnez la boîte de dialogue Activer l'intégration de la recherche. Dans la zone XML fournie, entrez le XML de configuration à l'aide de cette syntaxe.

   L'URN mis en surbrillance doit correspondre au terminal des services de plateforme que vous avez défini. Vous pouvez ouvrir un autre onglet du navigateur pour accéder au Gestionnaire de locataires et copier l'URN à partir du noeud final de services de plateforme défini.

   Dans cet exemple, nous n'avons utilisé aucun préfixe, ce qui signifie que les métadonnées de chaque objet de ce compartiment sont envoyées au terminal Elasticsearch précédemment défini.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
            <Urn> urn:local:es:::sgmd/sgmetadata/_doc</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

6. Utilisez le navigateur S3 pour vous connecter à StorageGRID avec la clé secrète/d'accès par locataire, et téléchargez les objets de test vers `sgmetadata-test` et ajoutez des balises ou des métadonnées personnalisées aux objets.



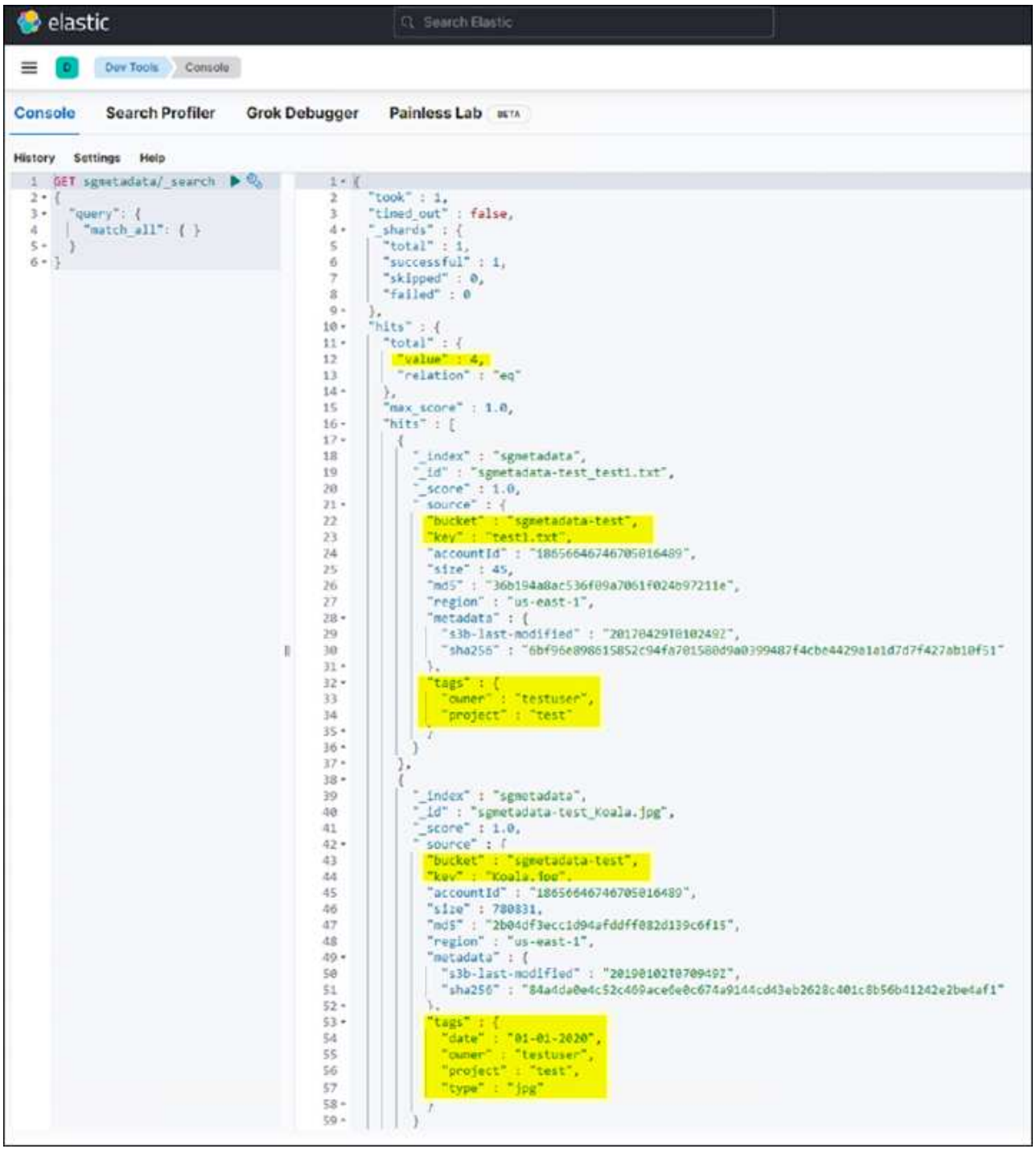
7. Utilisez l'interface utilisateur Kibana pour vérifier que les métadonnées de l'objet ont été chargées dans l'index des métadonnées sgmetadata.

   a. Dans le menu, sélectionnez gestion > Outils de développement.

   b. Collez l'exemple de requête dans le panneau de la console à gauche et cliquez sur le symbole du triangle pour l'exécuter.

      L'exemple de résultat de la requête 1 dans la capture d'écran suivante montre quatre enregistrements. Ceci correspond au nombre d'objets dans le godet.

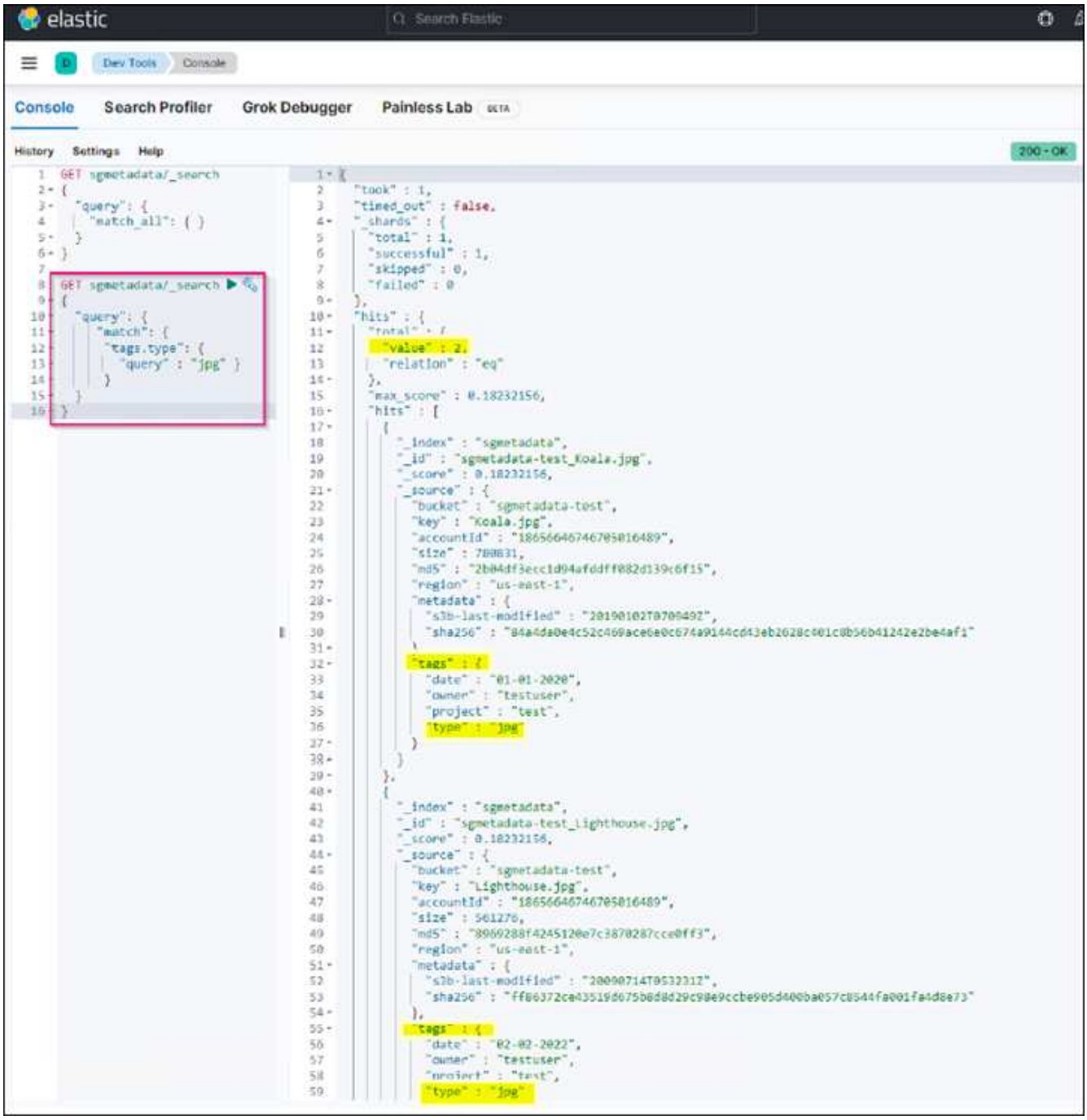
```
GET sgmetadata/_search
{
    "query": {
        "match_all": { }
}
}
```



Le résultat de l'exemple de requête 2 dans la capture d'écran suivante montre deux enregistrements de type de balise jpg.

```
GET sgmetadata/_search
{
    "query": {
        "match": {
            "tags.type": {
                "query" : "jpg" }
                }
            }
}
```

+



Où trouver des informations complémentaires

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

- "Qu'est-ce que les services de plateforme"
- "Documentation StorageGRID 11.6"

Par Angela Cheng

Clone de nœud

Considérations et performances sur le clonage des nœuds.

Considérations relatives au clonage de nœuds

Le clone de nœud peut être une méthode plus rapide pour remplacer les nœuds d'appliance existants dans le cadre d'une mise à jour technologique, d'une augmentation de la capacité ou d'une augmentation de la performance du système StorageGRID. Le clone de nœud peut également être utile pour la conversion en chiffrement de nœud avec un KMS ou pour le remplacement d'un nœud de stockage DDP8 par DDP16.

- La capacité utilisée du nœud source n'est pas pertinente pour le temps nécessaire à la fin du processus de clonage. Le clone de nœud est une copie complète du nœud, y compris l'espace libre dans le nœud.
- Les appareils source et cible doivent avoir la même version PGE
- La capacité du nœud de destination doit toujours être supérieure à la source
  - Assurez-vous que la nouvelle appliance de destination possède un lecteur plus grand que la source
  - Si l'appliance de destination possède des lecteurs de même taille et est configurée pour DDP8, vous pouvez configurer la destination pour DDP16. Si la source est déjà configurée pour DDP16, le clone de nœud ne sera pas possible.
  - Lorsque vous utilisez des appliances SG5660 ou SG5760 pour des appliances SG6060, sachez que les SG6060 disposent de 60 disques de capacité lorsque le SG6060 ne présente que 58.
- Le processus de clonage de nœud nécessite que le nœud source soit hors ligne de la grille pendant toute la durée du processus de clonage. Si un nœud supplémentaire se déconnecte pendant ce temps, les services client peuvent être affectés.
- Un nœud de stockage ne peut être hors ligne que pendant 15 jours. Si l'estimation du processus de clonage est proche de 15 jours ou supérieure à 15 jours, utilisez les procédures d'extension et de désaffectation.
- Pour un SG6060 avec tiroirs d'extension, vous devez ajouter la durée nécessaire à la taille de tiroir correcte au moment de l'appliance de base pour obtenir la durée totale du clone.
- Le nombre de volumes d'une appliance de stockage cible doit être supérieur ou égal au nombre de volumes du nœud source. Vous ne pouvez pas cloner un nœud source avec 16 volumes de magasin d'objets (rangedb) vers une appliance de stockage cible avec 12 volumes de magasin d'objets, même si l'appliance cible a une capacité supérieure au nœud source. La plupart des appliances de stockage disposent de 16 volumes de stockage objet, à l'exception de l'appliance SGF6112 qui ne dispose que de 12 volumes de stockage objet. Par exemple, vous ne pouvez pas cloner à partir d'un SG5760 vers un SGF6112.

Estimations des performances des clones de nœuds

Les tableaux suivants contiennent des estimations calculées pour la durée du clone de nœud. Les conditions varient donc, les entrées dans **BOLD** peuvent risquer de dépasser la limite de 15 jours pour un nœud en panne.

DDP8

SG5612 → tous

Vitesse de l'interface réseau	Taille de disque de 4 To	Taille de disque de 8 To	Taille de disque de 10 To	Taille des disques de 12 To	Taille de disque de 16 To	Taille des disques de 18 To
10 GBIT/S.	1 jour	2 jours	2.5 jours	3 jours	4 jours	4.5 jours
25 GO	1 jour	2 jours	2.5 jours	3 jours	4 jours	4.5 jours

SG5712 → tout

Vitesse de l'interface réseau	Taille de disque de 4 To	Taille de disque de 8 To	Taille de disque de 10 To	Taille des disques de 12 To	Taille de disque de 16 To	Taille des disques de 18 To
10 GBIT/S.	1 jour	2 jours	2.5 jours	3 jours	4 jours	4.5 jours
25 GO	1 jour	2 jours	2.5 jours	3 jours	4 jours	4.5 jours

SG5660 → SG5760

Vitesse de l'interface réseau	Taille de disque de 4 To	Taille de disque de 8 To	Taille de disque de 10 To	Taille des disques de 12 To	Taille de disque de 16 To	Taille des disques de 18 To
10 GBIT/S.	3 jours	6 jours	7 jours	8.5 jours	11.5 jours	**13 jours**
25 GO	3 jours	6 jours	7 jours	8.5 jours	11.5 jours	**13 jours**

SG5660 → SG6060

Vitesse de l'interface réseau	Taille de disque de 4 To	Taille de disque de 8 To	Taille de disque de 10 To	Taille des disques de 12 To	Taille de disque de 16 To	Taille des disques de 18 To
10 GBIT/S.	2.5 jours	4.5 jours	5.5 jours	6.5 jours	9 jours	10 jours
25 GO	2 jours	4 jours	5 jours	6 jours	8 jours	9 jours

SG5760 → SG5760

Vitesse de l'interface réseau	Taille de disque de 4 To	Taille de disque de 8 To	Taille de disque de 10 To	Taille des disques de 12 To	Taille de disque de 16 To	Taille des disques de 18 To
10 GBIT/S.	3 jours	6 jours	7 jours	8.5 jours	11.5 jours	**13 jours**
25 GO	3 jours	6 jours	7 jours	8.5 jours	11.5 jours	**13 jours**

SG5760 → SG6060

Vitesse de l'interface réseau	Taille de disque de 4 To	Taille de disque de 8 To	Taille de disque de 10 To	Taille des disques de 12 To	Taille de disque de 16 To	Taille des disques de 18 To
10 GBIT/S.	2.5 jours	4.5 jours	5.5 jours	6.5 jours	9 jours	10 jours
25 GO	1.5 jours	3 jours	3.5 jours	4.5 jours	6 jours	6.5 jours

SG6060 → SG6060

Vitesse de l'interface réseau	Taille de disque de 4 To	Taille de disque de 8 To	Taille de disque de 10 To	Taille des disques de 12 To	Taille de disque de 16 To	Taille des disques de 18 To
10 GBIT/S.	2.5 jours	4.5 jours	5.5 jours	6.5 jours	8.5 jours	9.5 jours
25 GO	1.5 jours	3 jours	3.5 jours	4 jours	5.5 jours	6 jours

DDP16

SG5760 → SG5760

Vitesse de l'interface réseau	Taille de disque de 4 To	Taille de disque de 8 To	Taille de disque de 10 To	Taille des disques de 12 To	Taille de disque de 16 To	Taille des disques de 18 To
10 GBIT/S.	3.5 jours	6.5 jours	8 jours	9.5 jours	12.5 jours	**14 jours**
25 GO	3.5 jours	6.5 jours	8 jours	9.5 jours	12.5 jours	**14 jours**

SG5760 → SG6060

Vitesse de l'interface réseau	Taille de disque de 4 To	Taille de disque de 8 To	Taille de disque de 10 To	Taille des disques de 12 To	Taille de disque de 16 To	Taille des disques de 18 To
10 GBIT/S.	2.5 jours	5 jours	6 jours	7.5 jours	10 jours	11 jours

Vitesse de l'interface réseau	Taille de disque de 4 To	Taille de disque de 8 To	Taille de disque de 10 To	Taille des disques de 12 To	Taille de disque de 16 To	Taille des disques de 18 To
25 GO	2 jours	3.5 jours	4 jours	5 jours	6.5 jours	7 jours

SG6060 → SG6060

Vitesse de l'interface réseau	Taille de disque de 4 To	Taille de disque de 8 To	Taille de disque de 10 To	Taille des disques de 12 To	Taille de disque de 16 To	Taille des disques de 18 To
10 GBIT/S.	3.5 jours	5 jours	6 jours	7 jours	9.5 jours	10.5 jours
25 GO	2 jours	3 jours	4 jours	4.5 jours	6 jours	7 jours

Tiroir d'extension (à ajouter au-dessus des SG6060 pour chaque tiroir de l'appliance source)

Vitesse de l'interface réseau	Taille de disque de 4 To	Taille de disque de 8 To	Taille de disque de 10 To	Taille des disques de 12 To	Taille de disque de 16 To	Taille des disques de 18 To
10 GBIT/S.	3.5 jours	5 jours	6 jours	7 jours	9.5 jours	10.5 jours
25 GO	2 jours	3 jours	4 jours	4.5 jours	6 jours	7 jours

Par Aron Klein

Comment utiliser le remap de port

Vous devrez peut-être remmapper un port entrant ou sortant pour plusieurs raisons. Vous pouvez passer du service d'équilibrage de la charge CLB existant au point de terminaison actuel de l'équilibreur de charge des services nginx et maintenir le même port pour réduire l'impact sur les clients, utiliser le port 443 pour le client S3 sur un réseau client de nœud d'administration ou pour les restrictions de pare-feu.

Migration des clients S3 de CLB à NGINX avec le remap du port

Dans les versions antérieures à StorageGRID 11.3, le service Load Balancer inclus sur les nœuds de passerelle est le composant Connection Load Balancer (CLB). Dans StorageGRID 11.3, NetApp présente le service NGINX en tant que solution intégrée riche en fonctionnalités pour l'équilibrage de la charge du trafic HTTP(s). Étant donné que le service CLB reste disponible dans la version actuelle de StorageGRID, vous ne pouvez pas réutiliser le port 8082 dans la nouvelle configuration de noeud final d'équilibreur de charge. Pour contourner ce problème, le port entrant 8082 est remappé sur 10443. Toutes les requêtes HTTPS arrivant sur le port 8082 de la passerelle sont alors redirigées vers le port 10443, en contournant le service CLB et en se connectant au service NGINX. Bien que les instructions suivantes soient pour VMware, LA fonctionnalité PORT_REMAP existe pour toutes les méthodes d'installation et vous pouvez utiliser un processus similaire pour les déploiements et les appliances sans système d'exploitation.

Déploiement du nœud de passerelle de machine virtuelle VMware

Les étapes suivantes concernent un déploiement StorageGRID dans lequel le ou les nœuds de passerelle sont déployés dans VMware vSphere 7 en tant que machines virtuelles utilisant le format OVF (Open Virtualization format) de StorageGRID. Le processus implique la suppression destructive de la machine virtuelle et le redéploiement de la machine virtuelle avec le même nom et la même configuration. Avant de mettre la machine virtuelle sous tension, modifiez la propriété vApp pour remmapper le port, puis mettez la machine virtuelle sous tension et suivez le processus de restauration du nœud.

Prérequis

- Vous exécutez StorageGRID 11.3 ou une version ultérieure
- Vous avez téléchargé les fichiers d'installation VMware de la version StorageGRID installée et y avez accès.
- Vous disposez d'un compte vCenter avec les autorisations d'allumer/d'éteindre les machines virtuelles, de modifier les paramètres des machines virtuelles et des vApps, de supprimer les machines virtuelles de vCenter et de déployer les machines virtuelles via OVF.
- Vous avez créé un terminal d'équilibrage de charge
  - Le port est configuré sur le port de redirection souhaité
  - Le certificat SSL du noeud final est identique à celui installé pour le service CLB dans le certificat de serveur Configuration/certificats de serveur/noeuds finaux du service API de stockage objet ou le client peut accepter une modification du certificat.

> ⓘ
>
> ```
> If your existing certificate is self-signed, you cannot reuse it
> in the new endpoint. You must generate a new self-signed
> certificate when creating the endpoint and configure the clients
> to accept the new certificate.
> ```

Détruisez le premier nœud de passerelle

Pour détruire le premier nœud de passerelle, procédez comme suit :

1. Choisissez le nœud de passerelle à utiliser si la grille en contient plusieurs.
2. Le cas échéant, supprimez les adresses IP de nœud de toutes les entités DNS Round Robin ou de tous les pools d'équilibrage de charge.
3. Attendez que le délai de mise en service (TTL) et les sessions ouvertes expirent.
4. Mettez le nœud VM hors tension.
5. Retirez le nœud VM du disque.

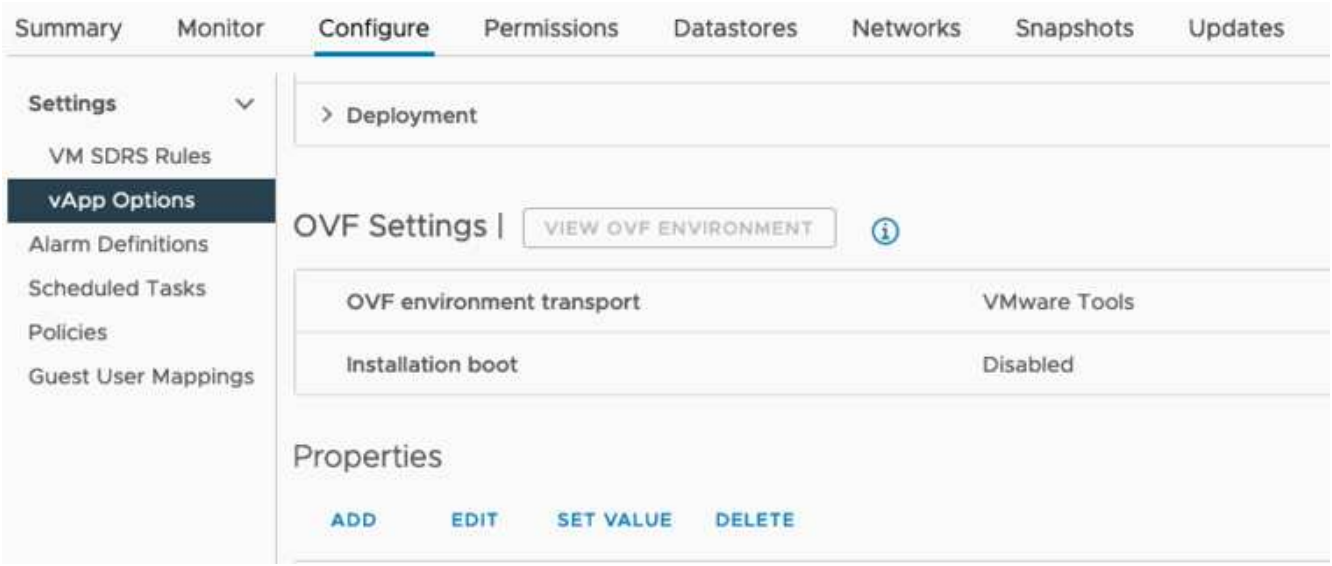
Déployez le nœud de passerelle de remplacement

Pour déployer le nœud de passerelle de remplacement, procédez comme suit :

1. Déployer la nouvelle machine virtuelle à partir d'OVF, en sélectionnant les fichiers .ovf, .mf et .vmdk à partir du package d'installation téléchargé à partir du site de support :
   - vsphere-gateway.mf
   - vsphere-gateway.ovf

◦ NetApp-SG-11.4.0-20200721.1338.d3969b3.vmdk

2. Une fois la machine virtuelle déployée, sélectionnez-la dans la liste des machines virtuelles, puis cliquez sur l'onglet configurer Options vApp.



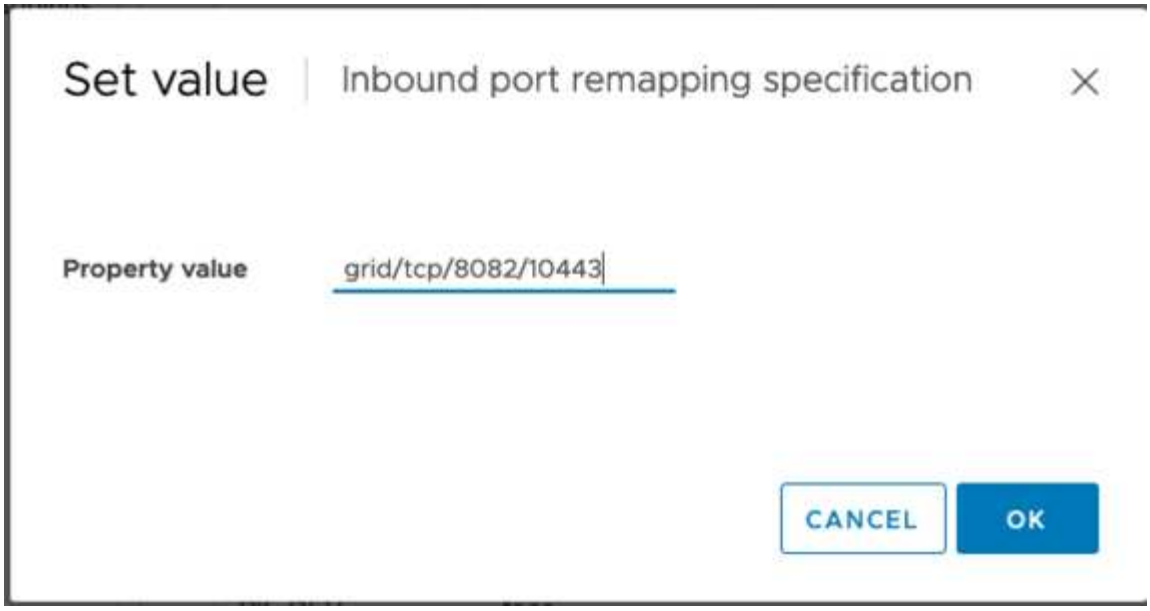
3. Faites défiler jusqu'à la section Propriétés et sélectionnez LA propriété PORT_REMAP_INBOUND

4. Faites défiler jusqu'en haut de la liste Propriétés et cliquez sur Modifier

5. Sélectionnez l'onglet Type, vérifiez que la case configurable par l'utilisateur est cochée, puis cliquez sur Enregistrer.

6. En haut de la liste Propriétés, la propriété "PORT_REMAP_INBOUND" étant toujours sélectionnée, cliquez sur définir la valeur.

7. Dans le champ valeur de la propriété, entrez le réseau (grille, admin ou client), TCP, le port d'origine (8082) et le nouveau port (10443) avec "/" entre chaque valeur, comme illustré ci-dessous.

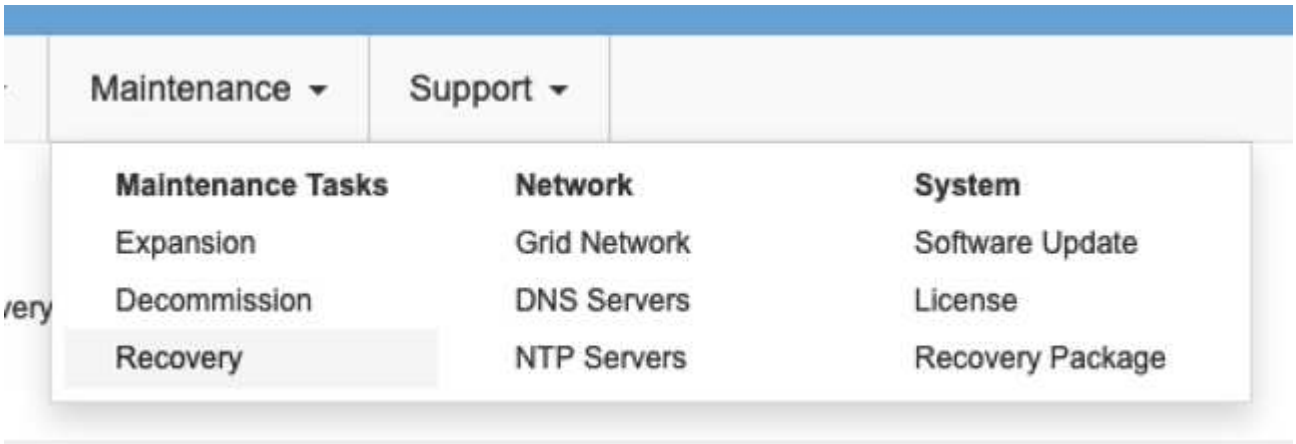


8. Si vous utilisez plusieurs réseaux, utilisez une virgule (,) pour séparer les chaînes réseau, par exemple GRID/tcp/8082/10443,admin/tcp/8082/10443,client/tcp/8082/10443

Restaurez le nœud de passerelle

Pour restaurer le nœud de passerelle, procédez comme suit :

1. Accédez à la section Maintenance/récupération de l'interface utilisateur de gestion du grid.



2. Mettez le nœud de la machine virtuelle sous tension et attendez que le nœud apparaisse dans la section Maintenance/Recovery Pending Nodes de l'interface utilisateur Grid Management.

> For information and directions for node recovery, see the https://docs.netapp.com/sgws-114/topic/com.netapp.doc.sg-maint/GUID-7E22B1B9-4169-4800-8727-75F25FC0FFB1.html[Recovery and Maintenance guide]

3. Une fois le nœud restauré, l'IP peut être incluse dans toutes les entités DNS round-Robin ou dans les pools d'équilibrage de charge, le cas échéant.

   Maintenant, toutes les sessions HTTPS sur le port 8082 sont sur le port 10443

Remadez le port 443 pour l'accès du client S3 sur un nœud d'administration

La configuration par défaut dans le système StorageGRID d'un nœud d'administration ou d'un groupe haute disponibilité contenant un nœud d'administration permet de réserver les ports 443 et 80 pour l'interface du gestionnaire de locataires et de gestion. Elle ne peut pas être utilisée pour les terminaux d'équilibrage de charge. La solution consiste à utiliser la fonction de remap de port et à rediriger le port entrant 443 vers un nouveau port qui sera configuré comme point final d'équilibrage de charge. Une fois cette opération terminée, le trafic client S3 pourra utiliser le port 443, l'interface de gestion Grid sera uniquement accessible via le port 8443 et l'interface de gestion des locataires sera uniquement accessible sur le port 9443. La fonction de remap port ne peut être configurée qu'au moment de l'installation du nœud. Pour mettre en œuvre un remap de port d'un nœud actif dans la grille, celui-ci doit être réinitialisé à l'état préinstallé. Il s'agit d'une procédure destructive qui inclut une restauration de nœud une fois la modification de configuration effectuée.

Sauvegarde des journaux et des bases de données

Les nœuds d'administration contiennent des journaux d'audit, des metrics prometheus, ainsi que des informations historiques sur les attributs, les alarmes et les alertes. La présence de plusieurs nœuds d'administration signifie que vous avez plusieurs copies de ces données. Si vous ne disposez pas de plusieurs nœuds d'administration dans votre grid, veillez à conserver ces données à restaurer une fois le nœud restauré à la fin de ce processus. Si vous disposez d'un autre nœud d'administration dans votre grid, vous pouvez copier les données à partir de ce nœud pendant le processus de restauration. Si vous ne disposez pas d'un autre nœud d'administration dans la grille, vous pouvez suivre ces instructions pour copier les données avant de détruire le nœud.

Copie des journaux d'audit

1. Connectez-vous au nœud d'administration :
   a. Saisissez la commande suivante : `ssh admin@grid_node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

c. Entrez la commande suivante pour passer à la racine : `su -`

d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

e. Ajoutez la clé privée SSH à l'agent SSH. Entrez : `ssh-add`

f. Entrez le mot de passe d'accès SSH répertorié dans le `Passwords.txt` fichier.

```
When you are logged in as root, the prompt changes from `$` to `#`.
```

2. Créer le répertoire pour copier tous les fichiers journaux d'audit dans un emplacement temporaire sur un nœud de grille distinct, nous allons utiliser *Storage_node_01*:

a. `ssh admin@storage_node_01_IP`

b. `mkdir -p /var/local/tmp/saved-audit-logs`

3. De retour sur le nœud admin, arrêtez le service AMS pour l'empêcher de créer un nouveau fichier journal : `service ams stop`

4. Renommez le fichier audit.log de sorte qu'il ne remplace pas le fichier existant lorsque vous le copiez sur le nœud d'administration restauré.

a. Renommez audit.log en un nom de fichier numéroté unique tel que aaaa-mm-jj.txt.1. Par exemple, vous pouvez renommer le fichier journal d'audit 2015-10-25.txt.1

```
cd /var/local/audit/export
ls -l
mv audit.log 2015-10-25.txt.1
```

5. Redémarrez le service AMS : `service ams start`

6. Copier tous les fichiers journaux d'audit : `scp * admin@storage_node_01_IP:/var/local/tmp/saved-audit-logs`

Copiez les données Prometheus

La copie de la base de données Prometheus peut prendre une heure ou plus. Certaines fonctionnalités de Grid Manager ne seront pas disponibles tant que les services seront arrêtés sur le nœud d'administration.

1. Créez le répertoire pour copier les données prometheus vers un emplacement temporaire sur un nœud de grille distinct. Là encore, nous allons utiliser *Storage_node_01*:

a. Connectez-vous au nœud de stockage :

i. Saisissez la commande suivante : `ssh admin@storage_node_01_IP`

ii. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

iii. mkdir -p /var/local/tmp/prometheus`

2. Connectez-vous au nœud d'administration :

a. Saisissez la commande suivante : `ssh admin@admin_node_IP`

b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

c. Entrez la commande suivante pour passer à la racine : `su -`

d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

e. Ajoutez la clé privée SSH à l'agent SSH. Entrez : `ssh-add`

f. Entrez le mot de passe d'accès SSH répertorié dans le `Passwords.txt` fichier.

```
When you are logged in as root, the prompt changes from `$` to `#`.
```

3. Depuis le nœud d'administration, arrêtez le service Prometheus : `service prometheus stop`

   a. Copiez la base de données Prometheus du nœud d'administration source vers le nœud d'emplacement de sauvegarde du nœud de stockage : `/rsync -azh --stats "/var/local/mysql_ibdata/prometheus/data" " storage_node_01_IP:/var/local/tmp/prometheus/"`

4. Redémarrez le service Prometheus sur le nœud d'administration source.`service prometheus start`

Sauvegarder les informations historiques

Les informations historiques sont stockées dans une base de données mysql. Pour vider une copie de la base de données, vous aurez besoin de l'utilisateur et du mot de passe de NetApp. Si vous avez un autre nœud d'administration dans la grille, cette étape n'est pas nécessaire et la base de données peut être clonée à partir d'un nœud d'administration restant pendant le processus de restauration.

1. Connectez-vous au nœud d'administration :

   a. Saisissez la commande suivante : `ssh admin@admin_node_IP`

   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   c. Entrez la commande suivante pour passer à la racine : `su -`

   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   e. Ajoutez la clé privée SSH à l'agent SSH. Entrez : `ssh-add`

   f. Entrez le mot de passe d'accès SSH répertorié dans le `Passwords.txt` fichier.

```
When you are logged in as root, the prompt changes from `$` to `#`.
```

2. Arrêtez les services StorageGRID sur le noeud d'administration et démarrez ntp et mysql

   a. Arrêter tous les services : `service servermanager stop`

   b. redémarrez le service ntp : `service ntp start`..restart mysql service: `service mysql start`

3. Vider la base de données mi dans /var/local/tmp

   a. entrez la commande suivante : `mysqldump -u username -p password mi > /var/local/tmp/mysql-mi.sql`

4. Copiez le fichier de vidage mysql sur un autre noeud, nous utiliserons *Storage_node_01: scp /var/local/tmp/mysql-mi.sql _storage_node_01_IP:/var/local/tmp/mysql-mi.sql*

a. Lorsque vous n'avez plus besoin d'un accès sans mot de passe à d'autres serveurs, supprimez la clé privée de l'agent SSH. Entrez : `ssh-add -D`

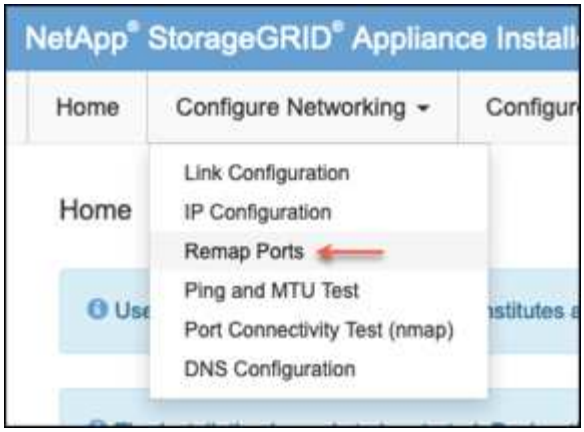
Reconstruire le nœud d'administration

Maintenant que vous disposez d'une copie de sauvegarde de toutes les données et journaux souhaités sur un autre nœud d'administration de la grille ou stockées dans un emplacement temporaire, il est temps de réinitialiser l'appliance afin que le remap des ports puisse être configuré.

1. La réinitialisation d'une appliance la ramène à l'état pré-installé, où elle conserve uniquement le nom d'hôte, les adresses IP et les configurations réseau. Toutes les données seront perdues, c'est pourquoi nous nous sommes assurés de disposer d'une sauvegarde de toute information importante.
   a. entrez la commande suivante : `sgareinstall`

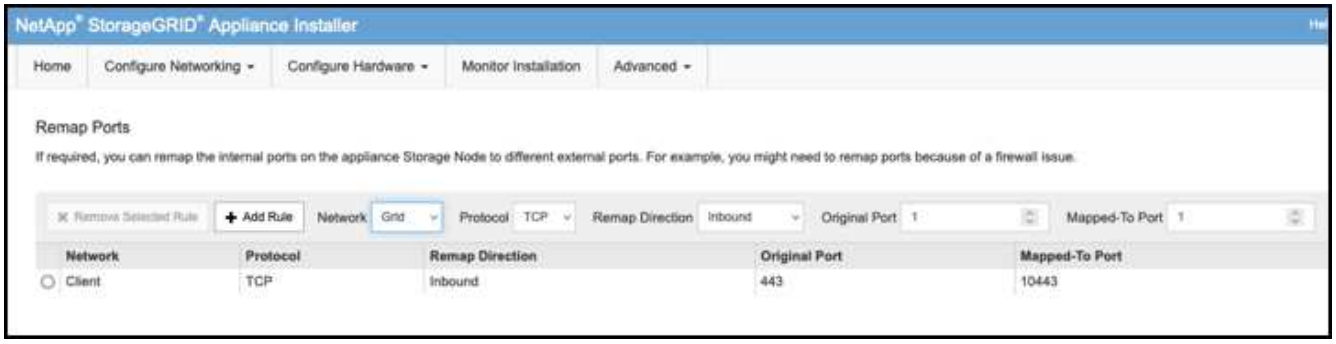
```
root@sg100-01:~ # sgareinstall
WARNING: All StorageGRID Webscale services on this node will be shut
down.
WARNING: Data stored on this node may be lost.
WARNING: You will have to reinstall StorageGRID Webscale to this
node.

After running this command and waiting a few minutes for the node to
reboot,
browse to one of the following URLs to reinstall StorageGRID Webscale
on
this node:

    https://10.193.174.192:8443
    https://10.193.204.192:8443
    https://169.254.0.1:8443

Are you sure you want to continue (y/n)? y
Renaming SG installation flag file.
Initiating a reboot to trigger the StorageGRID Webscale appliance
installation wizard.
```

2. Après un certain temps, l'appliance redémarre et vous pouvez accéder à l'interface utilisateur PGE du nœud.
3. Accédez à la page configurer la mise en réseau



4. Sélectionnez le réseau, le protocole, la direction et les ports souhaités, puis cliquez sur le bouton Ajouter une règle.

> Le remap du port entrant 443 sur le RÉSEAU DE LA GRILLE interrompt les procédures d'installation et d'extension. Il n'est pas recommandé de remapper le port 443 sur le réseau DE LA GRILLE.



5. L'un des mappages de port souhaités a été ajouté, vous pouvez revenir à l'onglet Home et cliquer sur le bouton Start installation.

Vous pouvez maintenant suivre les procédures de restauration du nœud Admin dans le "documentation produit"

Restaurer les bases de données et les journaux

Maintenant que le nœud d'administration a été restauré, vous pouvez restaurer les metrics, les journaux et les informations d'historique. Si vous avez un autre nœud d'administration dans la grille, suivez la procédure "documentation produit" en utilisant les scripts *prometheus-clone-db.sh* et *mi-clone-db.sh*. S'il s'agit de votre seul nœud d'administration et que vous avez choisi de sauvegarder ces données, vous pouvez suivre les étapes ci-dessous pour restaurer les informations.

Copiez à nouveau les journaux d'audit

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

d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

e. Ajoutez la clé privée SSH à l'agent SSH. Entrez : `ssh-add`

f. Entrez le mot de passe d'accès SSH répertorié dans le `Passwords.txt` fichier.

```
When you are logged in as root, the prompt changes from `$` to `#`.
```

2. Copiez les fichiers journaux d'audit conservés sur le nœud d'administration restauré : `scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY* .`
3. Pour plus de sécurité, supprimez les journaux d'audit du nœud de grille défaillant après avoir vérifié qu'ils ont bien été copiés sur le nœud d'administration restauré.
4. Mettez à jour les paramètres utilisateur et groupe des fichiers journaux d'audit sur le nœud d'administration restauré : `chown ams-user:bycast *`

Vous devez également restaurer tout accès client existant au partage d'audit. Pour plus d'informations, reportez-vous aux instructions d'administration de StorageGRID.

Restaurez des metrics Prometheus

> La copie de la base de données Prometheus peut prendre une heure ou plus. Certaines fonctionnalités de Grid Manager ne seront pas disponibles tant que les services seront arrêtés sur le nœud d'administration.

1. Connectez-vous au nœud d'administration :
   a. Saisissez la commande suivante : `ssh admin@grid_node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   e. Ajoutez la clé privée SSH à l'agent SSH. Entrez : `ssh-add`
   f. Entrez le mot de passe d'accès SSH répertorié dans le `Passwords.txt` fichier.

```
When you are logged in as root, the prompt changes from `$` to `#`.
```

2. Depuis le nœud d'administration, arrêtez le service Prometheus : `service prometheus stop`
   a. Copiez la base de données Prometheus depuis l'emplacement de sauvegarde temporaire vers le nœud d'administration : `/rsync -azh --stats "backup_node:/var/local/tmp/prometheus/" "/var/local/mysql_ibdata/prometheus/"`
   b. vérifiez que les données se trouvent dans le chemin approprié et qu'elles sont complètes `ls /var/local/mysql_ibdata/prometheus/data/`
3. Redémarrez le service Prometheus sur le nœud d'administration source.`service prometheus start`

Restaurer les informations historiques

1. Connectez-vous au nœud d'administration :
   a. Saisissez la commande suivante : `ssh admin@grid_node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   e. Ajoutez la clé privée SSH à l'agent SSH. Entrez : `ssh-add`
   f. Entrez le mot de passe d'accès SSH répertorié dans le `Passwords.txt` fichier.

   ```
   When you are logged in as root, the prompt changes from `$` to `#`.
   ```

2. Copiez le fichier de vidage mysql à partir du nœud alternatif : `scp grid_node_IP_:/var/local/tmp/mysql-mi.sql /var/local/tmp/mysql-mi.sql`
3. Arrêtez les services StorageGRID sur le noeud d'administration et démarrez ntp et mysql
   a. Arrêter tous les services : `service servermanager stop`
   b. redémarrez le service ntp : `service ntp start`..restart mysql service: `service mysql start`
4. Supprimez la base de données mi et créez une nouvelle base de données vide : `mysql -u username -p password -A mi -e "drop database mi; create database mi;"`
5. restaurez la base de données mysql à partir du vidage de la base de données : `mysql -u username -p password -A mi < /var/local/tmp/mysql-mi.sql`
6. Redémarrez tous les autres services `service servermanager start`

Par Aron Klein

Procédure de relocalisation du site dans le grid et de modification du réseau à l'échelle du site

Ce guide décrit la préparation et la procédure à suivre pour déplacer un site StorageGRID dans une grille multi-sites. Vous devez avoir une compréhension complète de cette procédure et prévoir à l'avance pour assurer un processus sans heurt et minimiser l'interruption pour les clients.

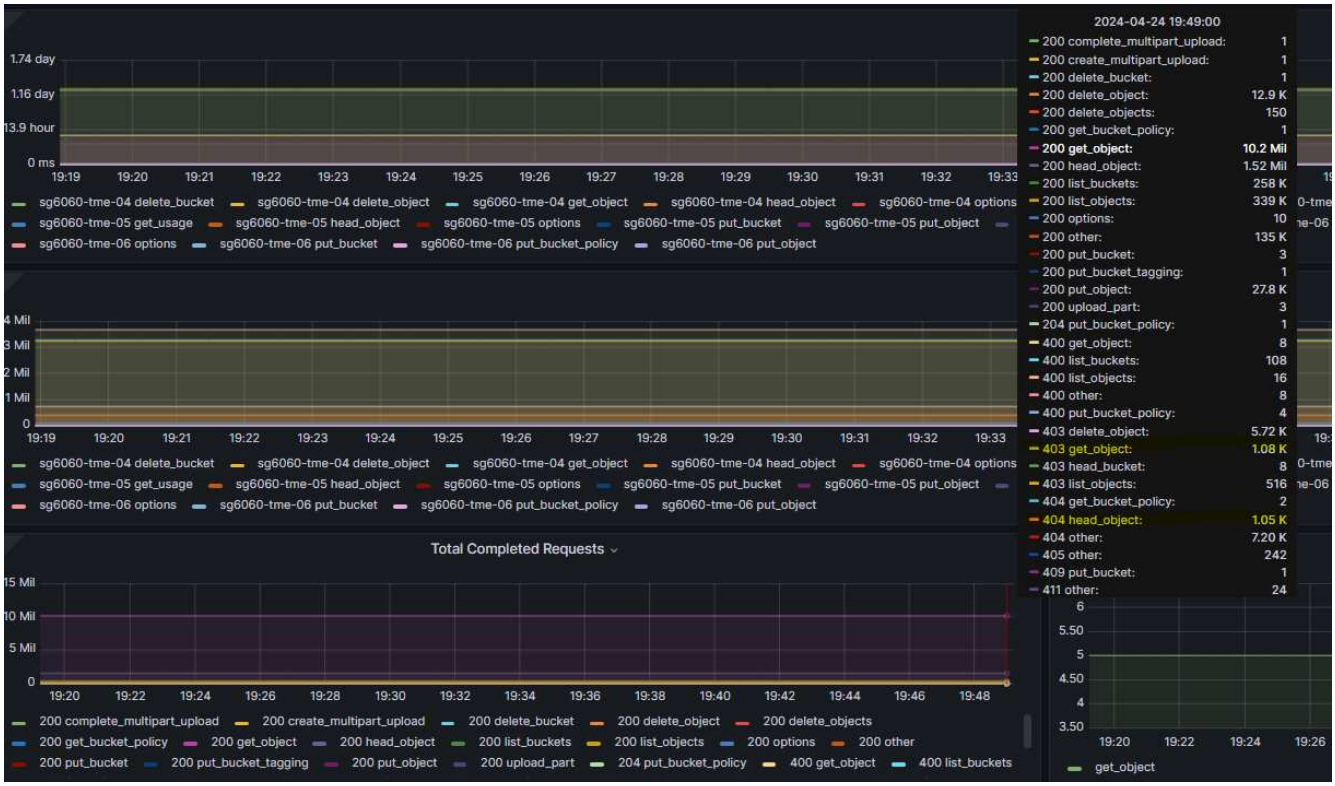
Si vous devez modifier le réseau grille de la grille entière, reportez-vous à la section "Modifiez les adresses IP de tous les nœuds de la grille".

Considérations avant la relocalisation du site

- Le déplacement du site doit être terminé et tous les nœuds doivent être en ligne dans les 15 jours pour éviter la reconstruction de la base de données Cassandra.
  "Panne d'un nœud de stockage de plus de 15 jours"
- Si une règle ILM de la règle active utilise un comportement d'ingestion strict, envisagez de la modifier en vue de l'équilibrer ou de la double allocation si le client souhaite continuer à PLACER les objets dans la

grille pendant la relocalisation du site.

- Pour les appliances de stockage de 60 disques ou plus, ne déplacez jamais le tiroir avec des disques installés. Étiquetez chaque lecteur de disque et retirez-le du boîtier de stockage avant de le emballer/déplacer.
- Changement d'appliance StorageGRID le réseau local virtuel du réseau de la grille peut être effectué à distance sur le réseau d'administration ou le réseau client. Sinon, prévoyez d'être sur site pour effectuer la modification avant ou après la mutation.
- Vérifiez si l'application client utilise la TÊTE ou si l'objet de non-existence est utilisé avant la MISE. Si oui, remplacez la cohérence du compartiment par site fort pour éviter les erreurs HTTP 500. Si vous n'êtes pas sûr, consultez la présentation S3 graphiques Grafana **Gestionnaire de grille > support > métriques**, placez le curseur de la souris sur le graphique « demande totale terminée ». S'il y a un nombre très élevé de 404 objets GET ou 404 objets Head, une ou plusieurs applications utilisent probablement l'objet Head ou Get nonexistence. Le compte est cumulatif, passez la souris sur différents chronologies pour voir la différence.



Procédure de modification de l'adresse IP de la grille avant le déplacement du site

Étapes

1. Si un nouveau sous-réseau de réseau Grid sera utilisé au nouvel emplacement, "Ajoutez le sous-réseau à la liste de sous-réseau du réseau Grid"
2. Connectez-vous au nœud d'administration principal, utilisez change-ip pour effectuer une modification de l'adresse IP de la grille. **Stage** doit être effectué avant d'arrêter le nœud pour le déplacement.
   a. Sélectionnez 2 puis 1 pour modification de l'adresse IP de la grille

```
Editing: Node IP/subnet and gateway

Use up arrow to recall a previously typed value, which you can then edit
Use d or 0.0.0.0/0 as the IP/mask to delete the network from the node
Use q to complete the editing session early and return to the previous menu
Press <enter> to use the value shown in square brackets

================================================================================
Site: LONDON
================================================================================
LONDON-ADM1 Grid    IP/mask [     10.45.74.14/26 ]: 10.45.74.24/26
LONDON-S1   Grid    IP/mask [     10.45.74.16/26 ]: 10.45.74.26/26
LONDON-S2   Grid    IP/mask [     10.45.74.17/26 ]: 10.45.74.27/26
LONDON-S3   Grid    IP/mask [     10.45.74.18/26 ]: 10.45.74.28/26
================================================================================
LONDON-ADM1 Grid    Gateway [         10.45.74.1 ]:
LONDON-S1   Grid    Gateway [         10.45.74.1 ]:
LONDON-S2   Grid    Gateway [         10.45.74.1 ]:
LONDON-S3   Grid    Gateway [         10.45.74.1 ]:
================================================================================
================================================================================
Site: OXFORD
================================================================================
OXFORD-ADM1 Grid    IP/mask [     10.45.75.14/26 ]:
OXFORD-S1   Grid    IP/mask [     10.45.75.16/26 ]:
OXFORD-S2   Grid    IP/mask [     10.45.75.17/26 ]:
OXFORD-S3   Grid    IP/mask [     10.45.75.18/26 ]:
================================================================================
OXFORD-ADM1 Grid    Gateway [         10.45.75.1 ]:
OXFORD-S1   Grid    Gateway [         10.45.75.1 ]:
OXFORD-S2   Grid    Gateway [         10.45.75.1 ]:
OXFORD-S3   Grid    Gateway [         10.45.75.1 ]:
================================================================================
Finished editing. Press Enter to return to menu.
```

b. sélectionnez 5 pour afficher les modifications

```
================================================================================
Site: LONDON
================================================================================
LONDON-ADM1 Grid    IP      [     10.45.74.14/26 ]: 10.45.74.24/26
LONDON-S1   Grid    IP      [     10.45.74.16/26 ]: 10.45.74.26/26
LONDON-S2   Grid    IP      [     10.45.74.17/26 ]: 10.45.74.27/26
LONDON-S3   Grid    IP      [     10.45.74.18/26 ]: 10.45.74.28/26
Press Enter to continue
```

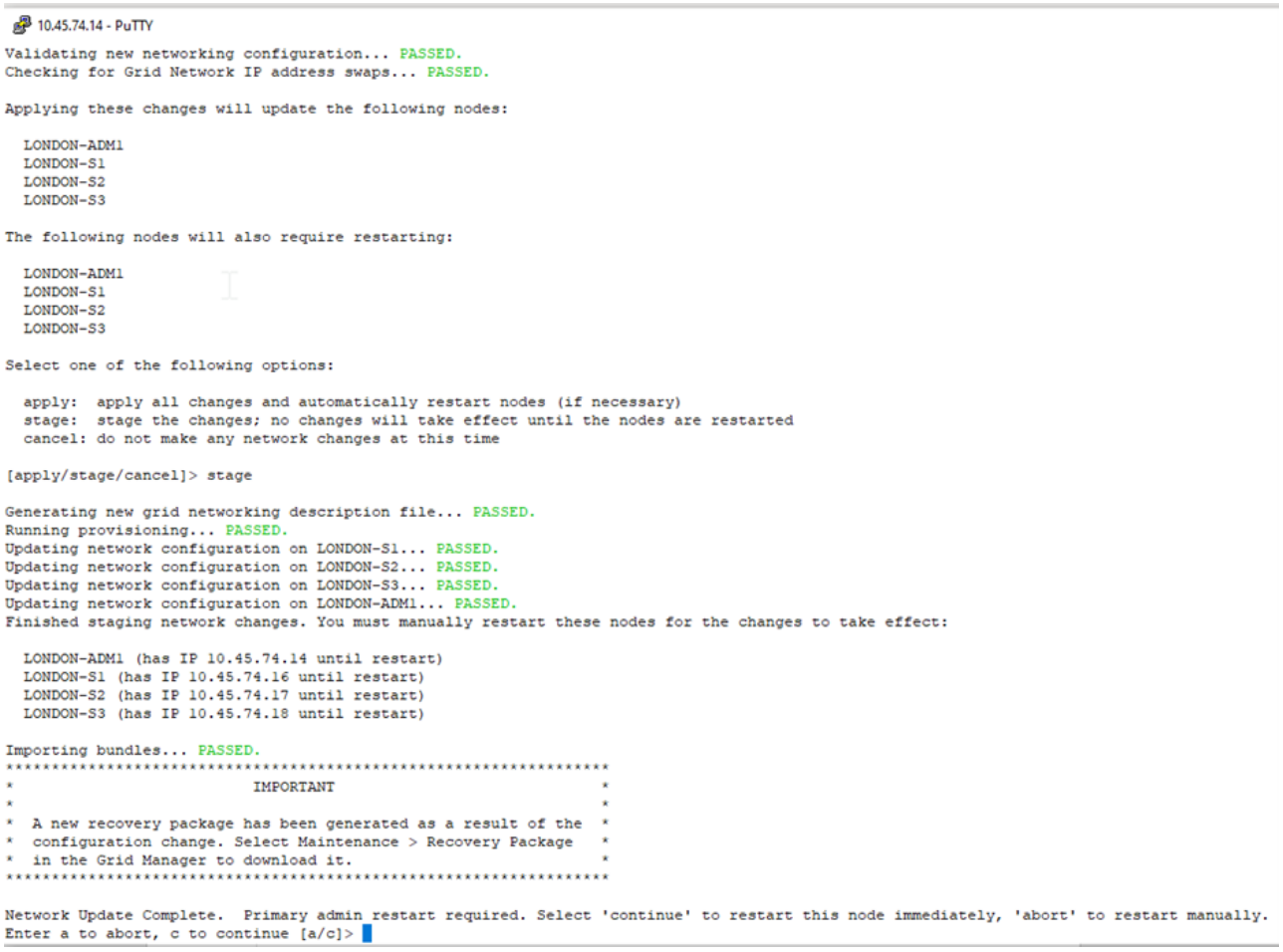
c. sélectionner 10 pour valider et appliquer la modification.

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:   SELECT NODES to edit
2:   EDIT IP/mask and gateway
3:   EDIT admin network subnet lists
4:   EDIT grid network subnet list
5:   SHOW changes
6:   SHOW full configuration, with changes highlighted
7:   VALIDATE changes
8:   SAVE changes, so you can resume later
9:   CLEAR all changes, to start fresh
10:  APPLY changes to the grid
0:   Exit

Selection: 10
```

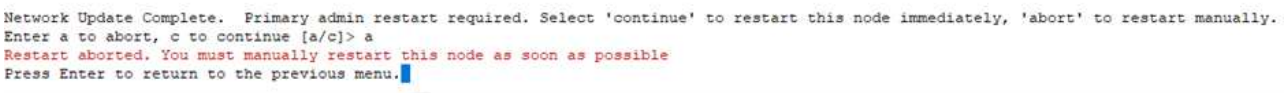
d. Vous devez sélectionner **stage** dans cette étape.

```
Validating new networking configuration... PASSED.
Checking for Grid Network IP address swaps... PASSED.

Applying these changes will update the following nodes:

  LONDON-ADM1
  LONDON-S1
  LONDON-S2
  LONDON-S3

The following nodes will also require restarting:

  LONDON-ADM1
  LONDON-S1
  LONDON-S2
  LONDON-S3

Select one of the following options:

  apply:  apply all changes and automatically restart nodes (if necessary)
  stage:  stage the changes; no changes will take effect until the nodes are restarted
  cancel: do not make any network changes at this time

[apply/stage/cancel]> stage
```

e. Si le nœud d'administration principal est inclus dans la modification ci-dessus, entrez **'a' pour redémarrer manuellement le nœud d'administration principal**



f. Appuyez sur ENTER pour revenir au menu précédent et quitter l'interface change-ip.



3. À partir de Grid Manager, téléchargez le nouveau package de récupération. **Grid Manager** > **Maintenance** > **paquet de récupération**
4. Si une modification VLAN est nécessaire sur l'appliance StorageGRID, reportez-vous à la section Modification du VLAN de l'appliance.
5. Arrêtez tous les nœuds et/ou appliances sur le site, étiquetez/retirez les disques si nécessaire, puis démettez, emballez et déplacez-les.
6. Si vous prévoyez de modifier l'adresse ip du réseau d'administration et/ou le VLAN et l'adresse ip du client, vous pouvez effectuer la modification après le déplacement.

Modification du VLAN de l'appliance

La procédure ci-dessous suppose que vous disposez d'un accès à distance au réseau client ou administrateur de l'appliance StorageGRID pour effectuer la modification à distance.

Étapes

1. Avant d'arrêter l'appareil,
"mettez l'appareil en mode de maintenance".

2. Utilisation d'un navigateur pour accéder à l'interface graphique du programme d'installation de l'appliance StorageGRID à l'aide de https://<admin-or-client-network-ip>:8443. Impossible d'utiliser Grid IP car la nouvelle Grid IP est déjà en place une fois que l'appliance est en mode maintenance.
3. Modifiez le VLAN pour le réseau Grid. Si vous accédez à l'appliance sur le réseau client, vous ne pouvez pas modifier le VLAN client pour le moment, vous pouvez le modifier après le déplacement.
4. connectez l'appliance à l'appliance et arrêtez le nœud en utilisant « shutdoown -h now »
5. Une fois les appliances prêtes sur le nouveau site, accédez à l'interface utilisateur graphique du programme d'installation de l'appliance StorageGRID à l'aide de https://<grid-network-ip>:8443. Vérifiez que l'état du stockage est optimal et que la connectivité réseau est assurée par les autres nœuds Grid à l'aide des outils ping/nmap disponibles dans l'interface graphique.
6. Si vous prévoyez de modifier l'adresse IP du réseau client, vous pouvez modifier le VLAN client à ce stade. Le réseau client n'est pas prêt tant que vous n'avez pas mis à jour l'adresse ip du réseau client à l'aide de l'outil change-ip à l'étape suivante.
7. Quittez le mode maintenance. Dans le programme d'installation de l'appliance StorageGRID, sélectionnez **Avancé** > **redémarrer le contrôleur**, puis sélectionnez **redémarrer dans StorageGRID**.
8. Une fois que tous les nœuds sont actifs et que Grid n'indique aucun problème de connectivité, utilisez change-ip pour mettre à jour le réseau d'administration de l'appliance et le réseau client, si nécessaire.