製品機能ガイド

How to enable StorageGRID in your environment

NetApp
April 26, 2024

目次

製品機能ガイド

AWSまたはGoogle Cloud用のクラウドストレージプールを作成します

StorageGRID オブジェクトを外部のS3バケットに移動する場合は、クラウドストレージプールを使用できます。外部バケットはAmazon S3（AWS）またはGoogle Cloudに属することができます。

必要なもの

- StorageGRID 11.6が設定されました。
- AWSまたはGoogle Cloudで外部のS3バケットをすでにセットアップしておきます。

手順

1. Grid Managerで、* ILM *>*ストレージプール*に移動します。
2. ページのクラウドストレージプールセクションで、 * 作成 * を選択します。

   クラウドストレージプールの作成ポップアップが表示されます。

3. 表示名を入力します。
4. [Provider Type]ドロップダウンリストから[**Amazon S3**]を選択します。

   このプロバイダタイプはAWS S3またはGoogle Cloudに対応しています。

5. クラウドストレージプールに使用するS3バケットのURIを入力します。

   次の2つの形式を使用できます。

   https://host:port`

   http://host:port`

6. S3バケット名を入力します。

   指定する名前はS3バケットの名前と完全に一致する必要があります。一致していないと、クラウドストレージプールの作成が失敗します。クラウドストレージプールの保存後にこの値を変更することはできません。

7. 必要に応じて、アクセスキーIDとシークレットアクセスキーを入力します。
8. ドロップダウンから[* Do not verify Certificate*（証明書を検証しない*）]を選択します。
9. [保存（ Save ）] をクリックします。

想定される結果です

Amazon S3またはGoogle Cloud用のクラウドストレージプールが作成されていることを確認します。

ジョナサン・ウォン著

Azure Blob Storage用のクラウドストレージプールを作成します

StorageGRID オブジェクトを外部のAzureコンテナに移動する場合は、クラウドストレージプールを使用できます。

必要なもの

- StorageGRID 11.6が設定されました。
- 外部のAzureコンテナはすでにセットアップされています。

手順

1. Grid Managerで、* ILM *>*ストレージプール*に移動します。
2. ページのクラウドストレージプールセクションで、 * 作成 * を選択します。

   クラウドストレージプールの作成ポップアップが表示されます。

3. 表示名を入力します。
4. プロバイダタイプドロップダウンリストから「* Azure Blob Storage *」を選択します。
5. クラウドストレージプールに使用するS3バケットのURIを入力します。

   次の2つの形式を使用できます。

   https://host:port`

   http://host:port`

6. Azureコンテナ名を入力します。

   指定する名前はAzureコンテナ名と完全に一致する必要があります。一致していないと、クラウドストレージプールの作成は失敗します。クラウドストレージプールの保存後にこの値を変更することはできません。

7. 必要に応じて、Azureコンテナに関連付けられたアカウント名と認証用のアカウントキーを入力します。
8. ドロップダウンから[* Do not verify Certificate*（証明書を検証しない*）]を選択します。
9. [保存（ Save ）] をクリックします。

想定される結果です

Azure Blob Storage用のクラウドストレージプールが作成されていることを確認します。

ジョナサン・ウォン著

クラウドストレージプールをバックアップに使用する

バックアップ用にクラウドストレージプールにオブジェクトを移動するILMルールを作成できます。

必要なもの

- StorageGRID 11.6が設定されました。
- 外部のAzureコンテナはすでにセットアップされています。

手順

1. Grid Managerで、* ILM > Rules > Create *の順に移動します。
2. 概要 を入力します。
3. ルールをトリガーする基準を入力します。
4. 「 * 次へ * 」をクリックします。
5. オブジェクトをストレージノードにレプリケートします。
6. 配置ルールを追加します。
7. オブジェクトをクラウドストレージプールにレプリケートします
8. 「 * 次へ * 」をクリックします。
9. [保存（ Save ）] をクリックします。

想定される結果です

保持図に、バックアップ用にStorageGRID とクラウドストレージプールにローカルに格納されているオブジェクトが示されていることを確認します。

ILMルールがトリガーされたときにクラウドストレージプールにコピーが存在し、オブジェクトのリストアを実行せずにローカルでオブジェクトを読み出すことができることを確認します。

ジョナサン・ウォン著

StorageGRID 検索統合サービスを設定する

このガイドでは、Amazon StorageGRID 11.6検索統合サービスとオンプレミスのElasticsearchを使用するようにNetAppを設定する手順について詳しく説明します。

はじめに

StorageGRID は、3種類のプラットフォームサービスをサポートしています。

- * StorageGRID CloudMirrorレプリケーション*。StorageGRID バケットから指定された外部のデスティネーションに特定のオブジェクトをミラーリングします。
- 通知。バケット単位のイベント通知：オブジェクトに対して実行された特定の処理に関する通知を、指定された外部のAmazon Simple Notification Service（Amazon SNS）に送信します。
- 検索統合サービス。外部サービスを使用してメタデータを検索または分析できるように、指定されたElasticsearchインデックスにSimple Storage Service（S3）オブジェクトメタデータを送信します。

プラットフォームサービスは、テナントマネージャのUIを使用してS3テナントによって設定されます。詳細については、を参照してください "プラットフォームサービスの使用に関する考慮事項"。

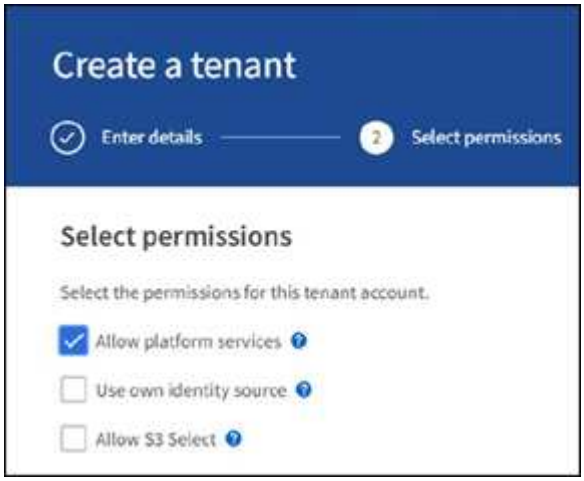
このドキュメントは、の補足資料として機能します "StorageGRID 11.6テナントガイド" およびに、検索統合サービス用のエンドポイントとバケットの設定手順と例を示します。ここで紹介するAmazon Web Services（AWS）またはオンプレミスのElasticsearchセットアップの手順は、基本的なテストやデモ目的にのみ使用

します。

対象読者は、Grid Manager、テナントマネージャに精通している必要があり、S3ブラウザにアクセスして、StorageGRID 検索統合テストの基本的なアップロード（PUT）処理とダウンロード（GET）処理を実行できます。

テナントを作成し、プラットフォームサービスを有効にします

1. Grid Managerを使用してS3テナントを作成し、表示名を入力してS3プロトコルを選択する。
2. [アクセス許可]ページで、[プラットフォームサービスを許可する]オプションを選択します。必要に応じて、他の権限を選択します。



3. テナントのrootユーザの初期パスワードを設定するか、グリッドでフェデレーションが有効になっている場合は、テナントアカウントを設定するためのrootアクセス権限を持つフェデレーテッドグループを選択します。
4. [ルートとしてサインイン]をクリックし、[バケット：バケットの作成と管理]を選択します。

   Tenant Managerのページが表示されます。

5. Tenant Managerで、My Access Keysを選択してS3アクセスキーを作成およびダウンロードし、あとでテストを実施します。

Amazon OpenSearchとの検索統合サービス

Amazon OpenSearch（旧Elasticsearch）サービスのセットアップ

この手順 は、テスト/デモ目的でのみOpenSearchサービスをすばやく簡単にセットアップするために使用します。検索統合サービスにオンプレミスのElasticsearchを使用している場合は、を参照してください 検索統合サービスをオンプレミスのElasticsearchと利用できます。

> OpenSearchサービスに登録するには、有効なAWSコンソールログイン、アクセスキー、シークレットアクセスキー、および権限が必要です。

1. の手順に従って、新しいドメインを作成します "AWS OpenSearchサービス開始前の準備"次の場合を除きます。
   - 手順 4ドメイン名：sgdemo

- 手順10：きめ細かなアクセスコントロール：「きめ細かなアクセスコントロールを有効にする」オプションの選択を解除します。
- 手順12.アクセスポリシー：Configure Level Access Policyを選択し、JSONタブを選択して次の例を使用してアクセスポリシーを変更します。
  - 強調表示されたテキストを、AWS Identity and Access Management（IAM）IDとユーザ名に置き換えます。
  - 強調表示されているテキスト（IPアドレス）を、AWSコンソールへのアクセスに使用したローカルコンピュータのパブリックIPアドレスに置き換えます。
  - ブラウザタブを開き、に移動します "https://checkip.amazonaws.com" をクリックして、パブリックIPを検索してください。

```
{

    "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.

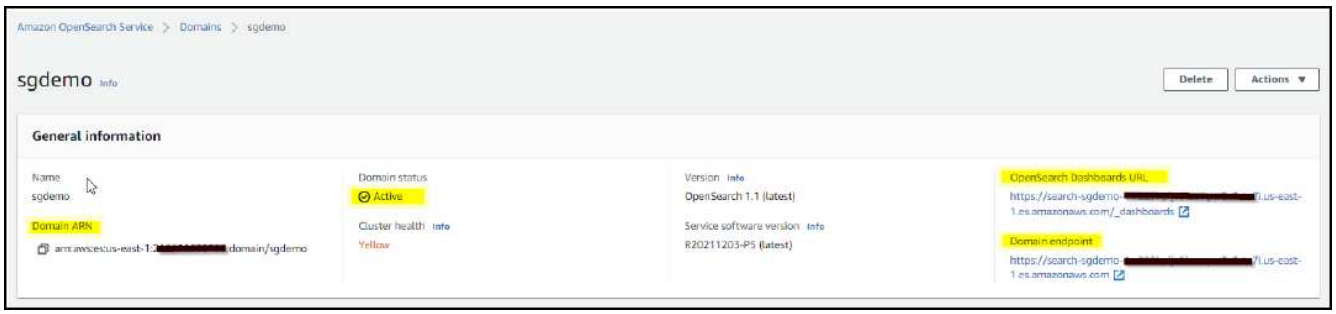
◉ Configure domain level access policy

Visual editor | JSON | Import policy

Access policy

```
3  "Statement": [
4    {
5      "Effect": "Allow",
6      "Principal": {
7        "AWS": "arn:aws:iam::2[redacted]:user/a[redacted]"
8      },
9      "Action": "es:*",
10     "Resource": "arn:aws:es:us-east-1:2[redacted]:domain/sgdemo/*"
11   },
12   {
13     "Effect": "Allow",
14     "Principal": {
15       "AWS": "*"
16     },
17     "Action": [
18       "es:ESHttp*"
19     ],
20     "Condition": {
21       "IpAddress": {
22         "aws:SourceIp": [
23           "216.[redacted]/24"
24         ]
25       }
26     },
27     "Resource": "arn:aws:es:us-east-1:2[redacted]:domain/sgdemo/*"
28   }
```

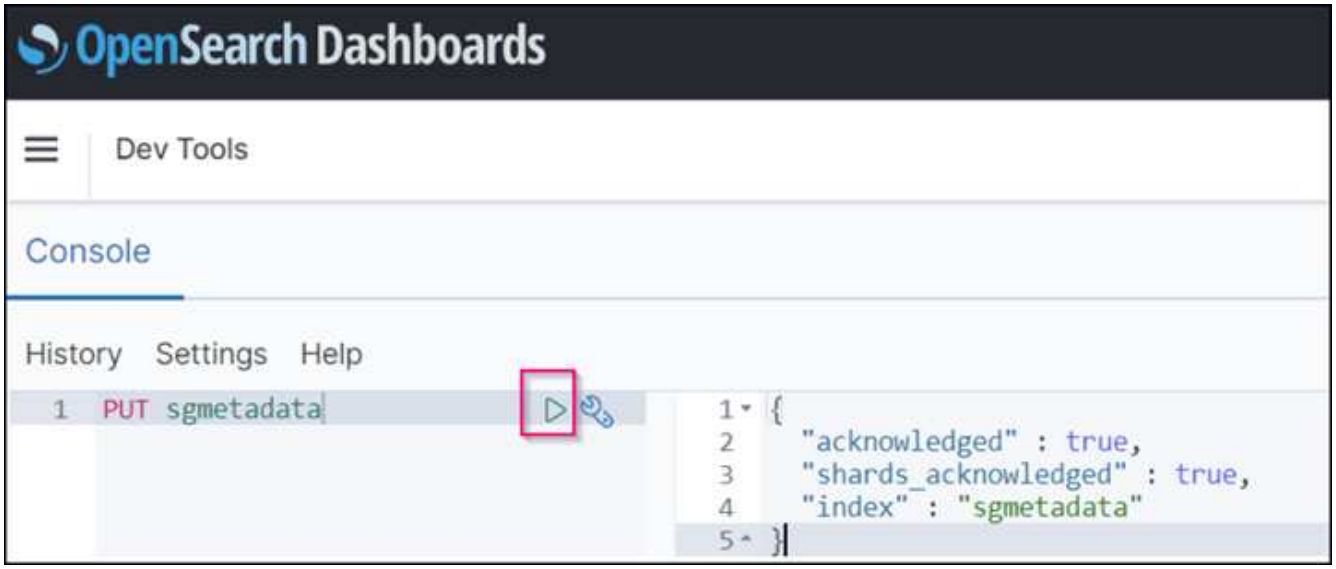
2. ドメインがアクティブになるまで15〜20分待ちます。



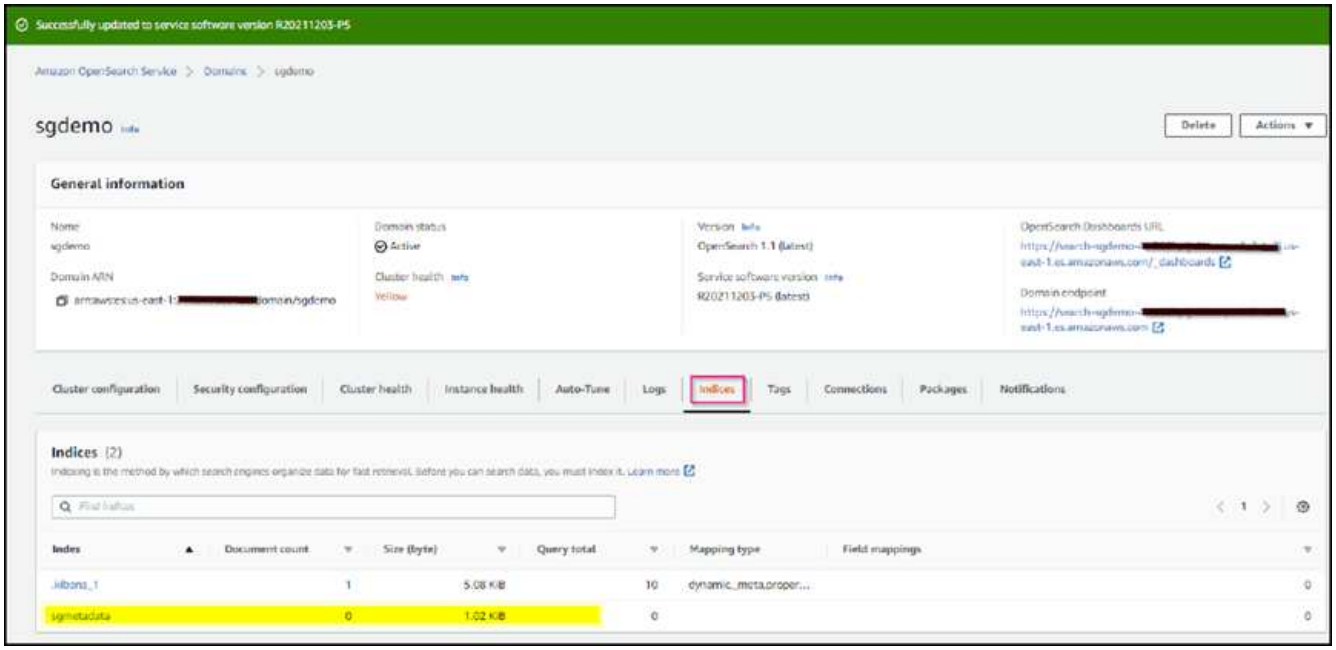
3. OpenSearch Dashboards URLをクリックして、新しいタブでドメインを開き、ダッシュボードにアクセスします。access deniedエラーが表示された場合は、アクセスポリシーのソースIPアドレスがコンピュータのパブリックIPに正しく設定されていて、ドメインダッシュボードへのアクセスが許可されていることを確認します。

4. ダッシュボードの開始ページで、自分で探索（Explore on your own）を選択します。メニューから、[管理]→[開発ツール]を選択します

5. Dev Tools → Consoleで、StorageGRID オブジェクトメタデータの保存にインデックスを使用する「Put <index>」と入力します。次の例では、インデックス名「メタデータ」を使用します。小さい三角形の記号をクリックして、PUTコマンドを実行します。次のスクリーンショットの例に示すように、正しい結果が右側のパネルに表示されます。



6. インデックスがAmazon OpenSearch UIのsgdomain > Indicesの下に表示されていることを確認します。

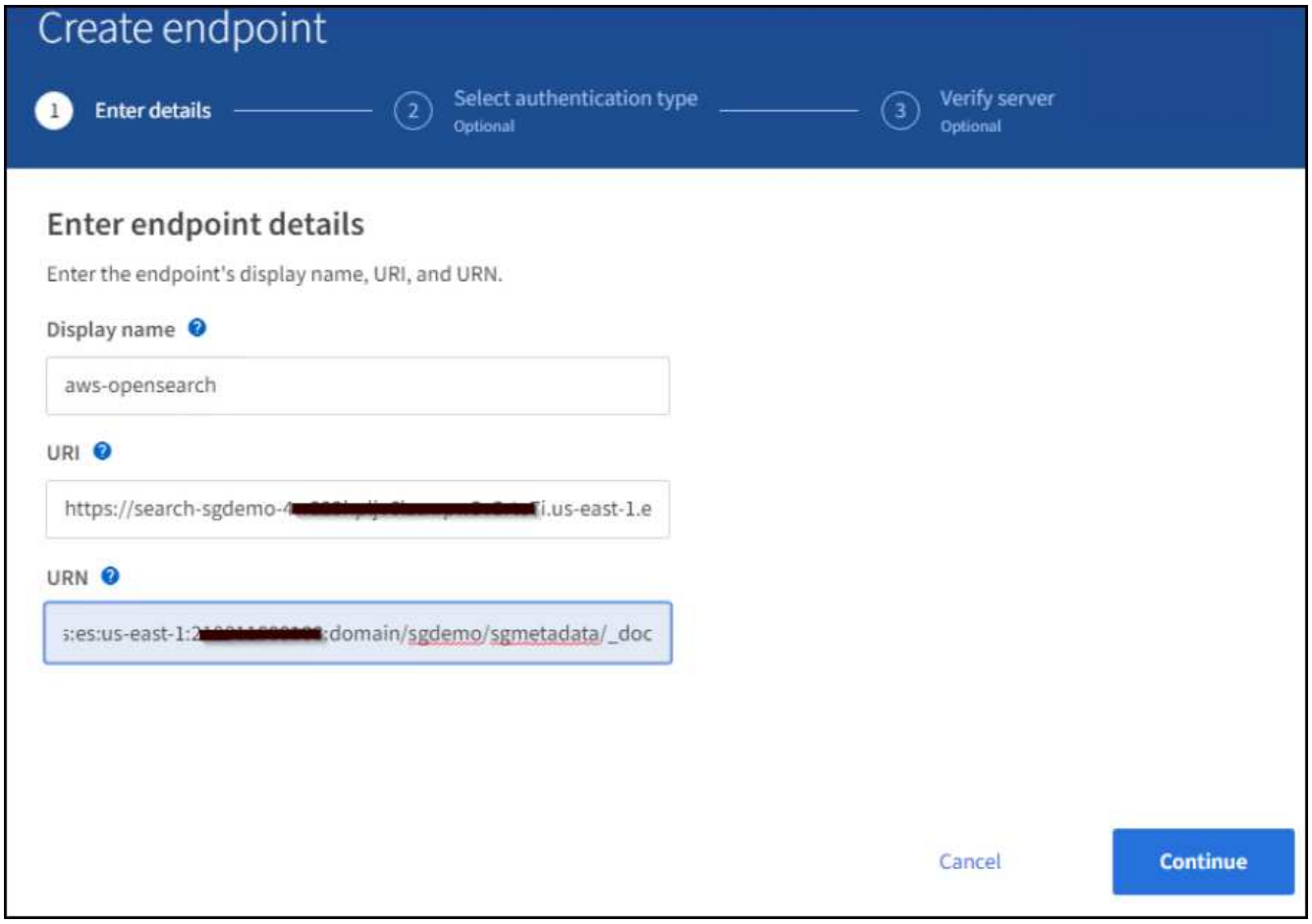


プラットフォームサービスエンドポイントの設定

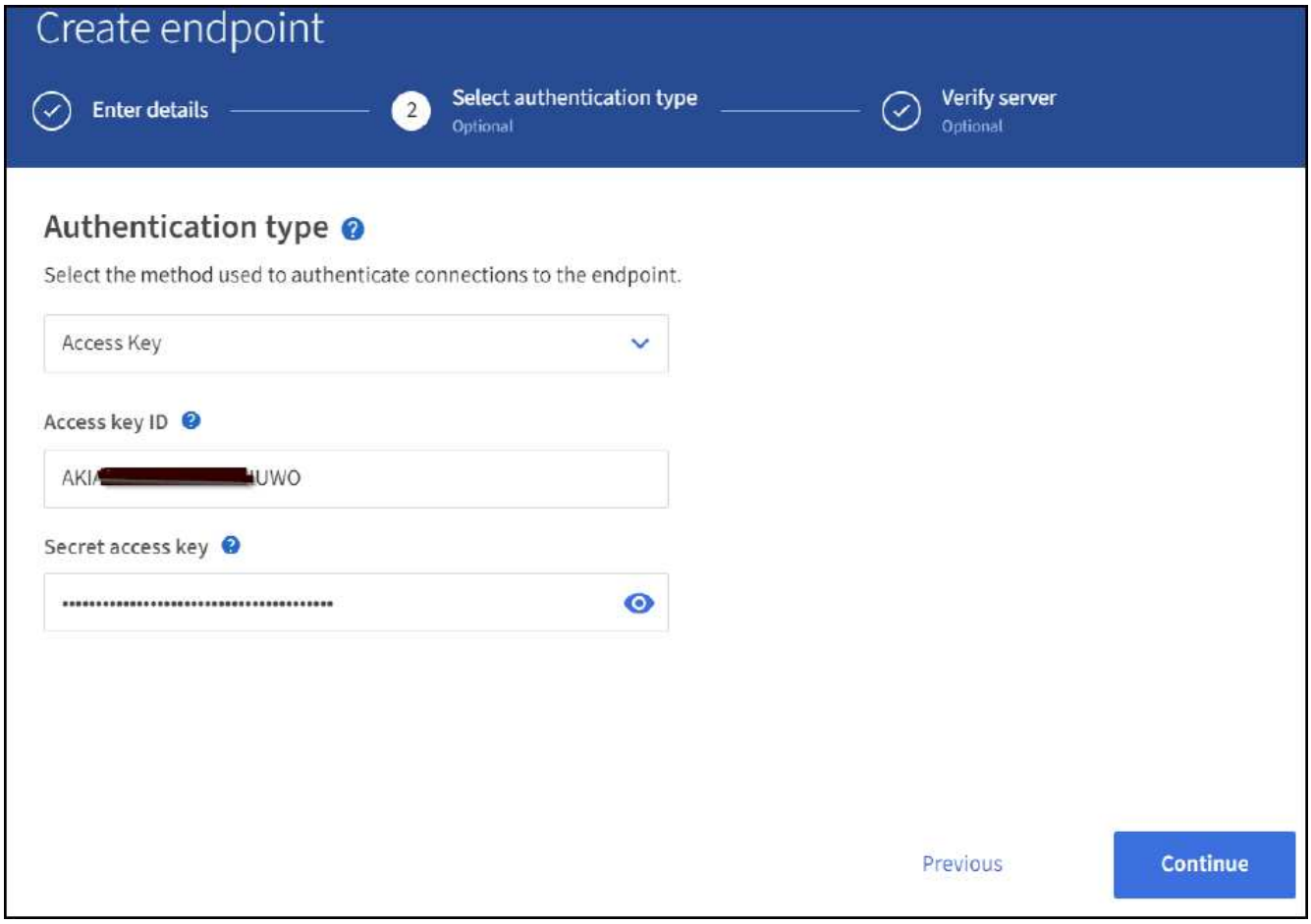
プラットフォームサービスエンドポイントを設定するには、次の手順を実行します。

1. Tenant Managerで、ストレージ（S3）>プラットフォームサービスのエンドポイントに移動します。
2. [エンドポイントの作成]をクリックし、次のように入力して、[続行]をクリックします。
    - 表示名の例は「AWS- OpenSearch」です
    - 手順 フィールドの前の「URI」の手順2の下のスクリーンショットのドメインエンドポイント。
    - URNフィールドで前の手順 の手順2で使用したドメインARNの末尾に'/<index>/_docを追加します

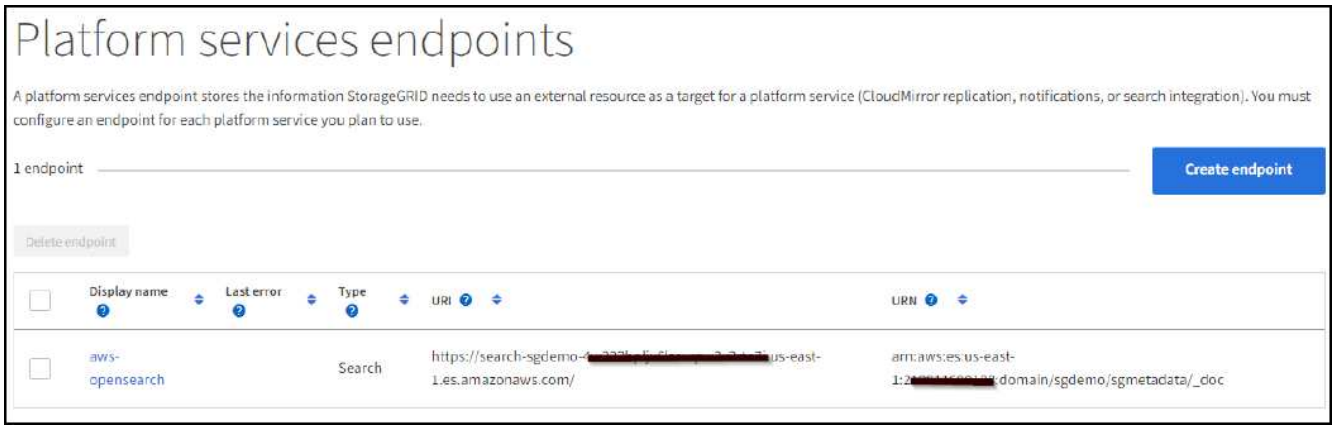
      この例では、URNはarn：aws：es：us-east -1：211234567890：domain/sgdemo/sgmedata/_docになります。



3. Amazon OpenSearchのsgdomainにアクセスするには、認証タイプとしてAccess Keyを選択し、Amazon S3のアクセスキーとシークレットキーを入力します。次のページに移動するには、[続行]をクリックします。



4. エンドポイントを確認するには、Use Operating System CA Certificate and Test and Create Endpointを選択します。検証に成功すると、次の図のようなエンドポイント画面が表示されます。検証に失敗した場合は、URNのパスの末尾に「/<index>/_doc」が含まれていて、AWSアクセスキーとシークレットキーが正しいことを確認してください。



検索統合サービスをオンプレミスの**Elasticsearch**と利用できます

オンプレミスの**Elasticsearch**セットアップ

この手順 は、テスト目的でのみDockerを使用するElasticsearchとKibanaオンプレミスを迅速にセットアップするためのものです。ElasticsearchサーバとKibanaサーバがすでに存在する場合は、ステップ5に進みます。

1. これを実行します "Dockerインストール手順 の略" Dockerをインストールするため。を使用します "CentOS Dockerは手順 をインストールする" このセットアップでは、

```
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
```

   - リブート後にDockerを起動するには、次のように入力します。

```
sudo systemctl enable docker
```

   - 「vm.max_map_count」値を262144に設定します。

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

   - リブート後も設定を維持するには、次のように入力します。

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

2. に従ってください "Elasticsearchクイックスタートガイド" ElasticsearchとKibana Dockerを自己管理のためのセクションでインストールして実行できます。この例では、バージョン8.1をインストールしました。

> Elasticsearchが作成したユーザ名/パスワードとトークンをメモしておきます。これらのトークンは、Kibana UIおよびStorageGRID プラットフォームエンドポイント認証を開始するために必要です。

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.

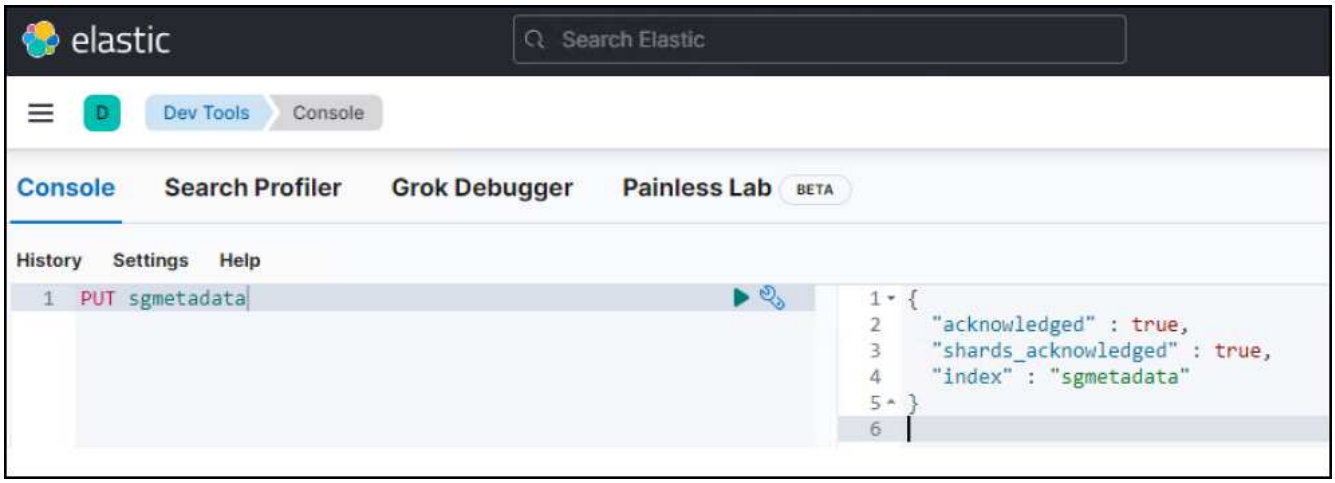
1. In a new terminal session, run:

```
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.

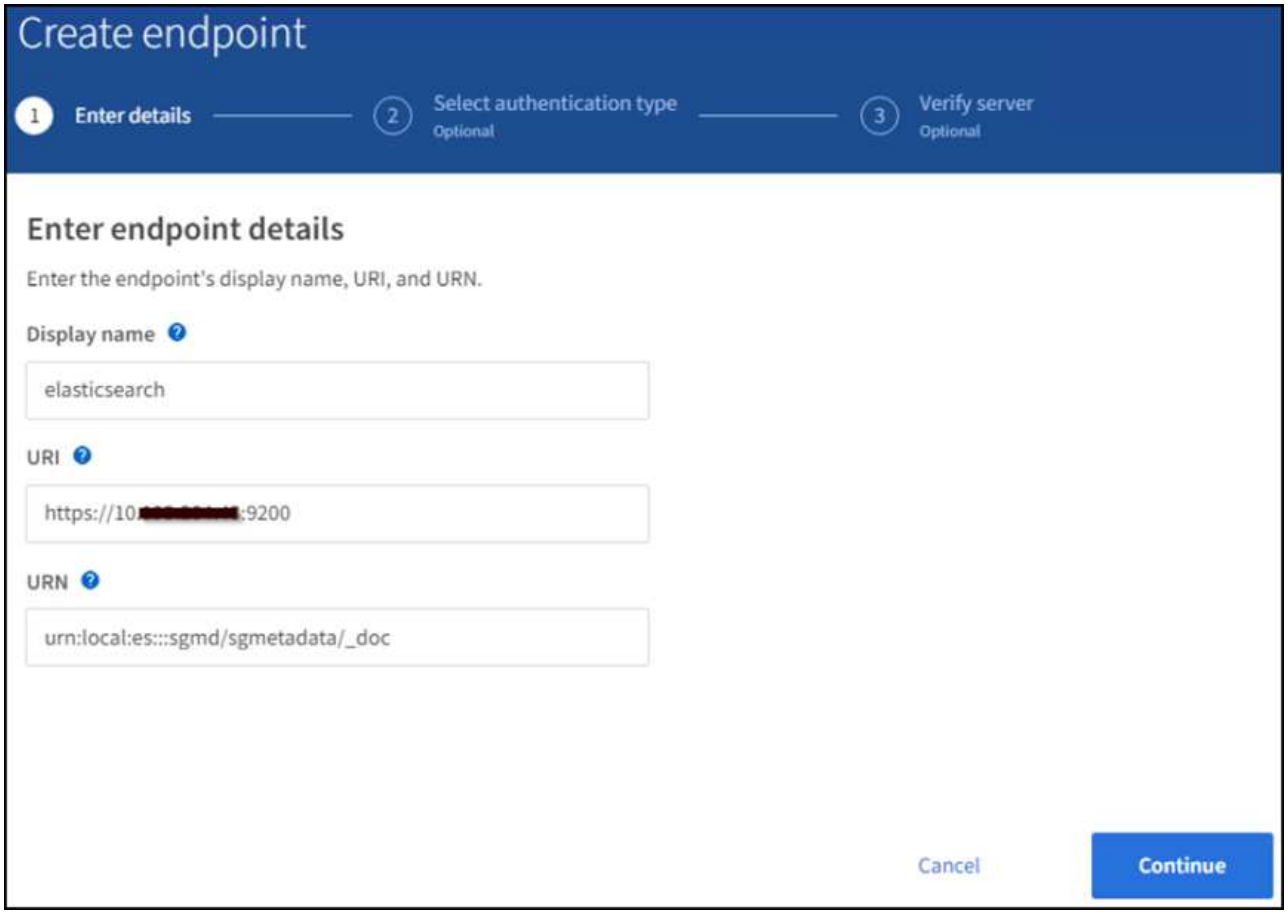
3. Kibana Dockerコンテナが起動すると、コンソールにURLリンク「\ https://0.0.0.0:5601`」が表示されます。0.0.0.0を、URL内のサーバIPアドレスと置き換えます。
4. ユーザ名「elastic」と、前述の手順でElasticによって生成されたパスワードを使用して、Kibana UIにログインします。
5. 初めてログインする場合は、ダッシュボードのようこそページで、自分でエクスプローラ（Explore on your own）を選択します。メニューから、Management > Dev Toolsを選択します。
6. Dev Tools Console画面で、StorageGRID オブジェクトメタデータの保存にこのインデックスを使用する「Put <index>」と入力します。この例では'インデックス名sgmetadataを使用します小さい三角形の記号をクリックして、PUTコマンドを実行します。次のスクリーンショットの例に示すように、正しい結果が右側のパネルに表示されます。



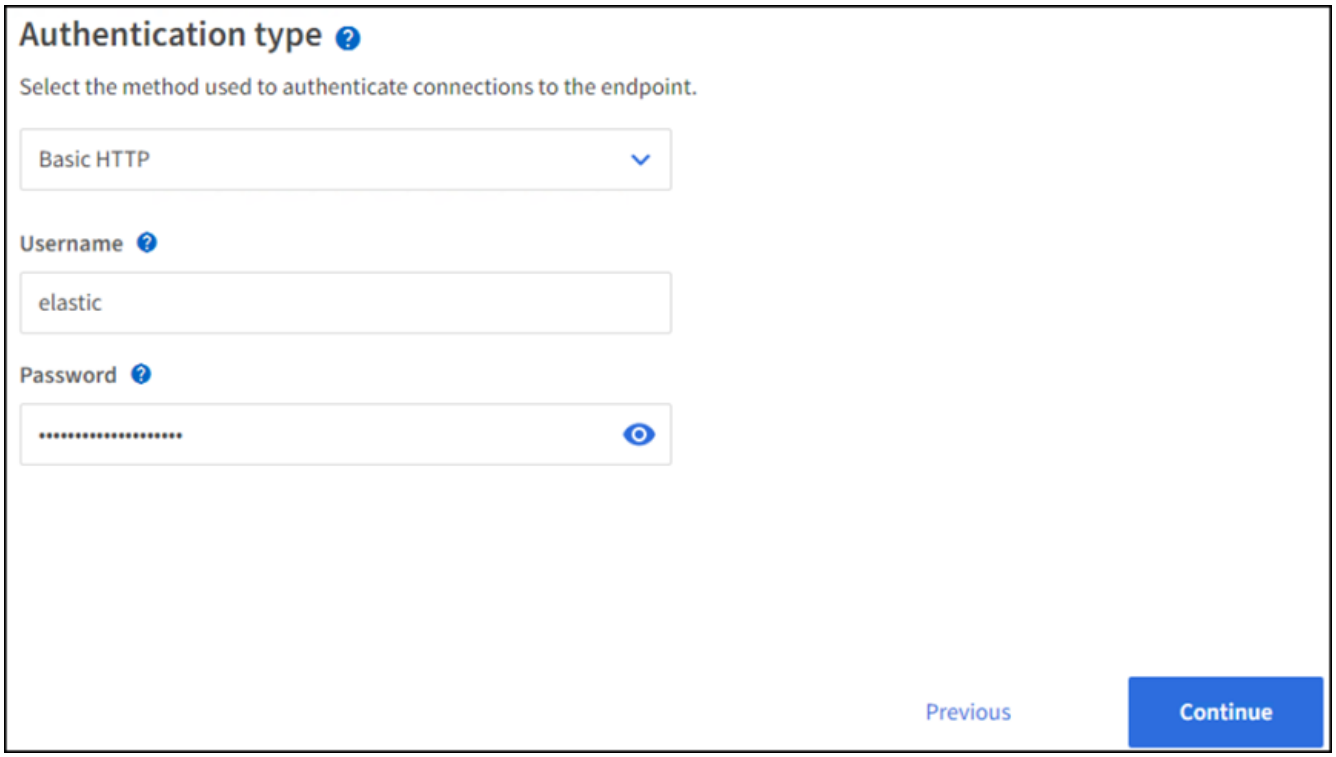
プラットフォームサービスエンドポイントの設定

プラットフォームサービスのエンドポイントを設定するには、次の手順を実行します。

1. Tenant Managerで、ストレージ（S3）>プラットフォームサービスのエンドポイントに移動します
2. [エンドポイントの作成]をクリックし、次のように入力して、[続行]をクリックします。
   - 表示名の例: elastic`
   - URI:`\https://<elasticsearch-server-ipまたはhostname>:9200`
   - urn:`urn:<何か>:es:::<se-unique text>/<index-name>/_doc`ここで、index-nameはKibanaコンソールで使用した名前です。例:`urn:local:es::sgmd/sgmetadata/_doc`

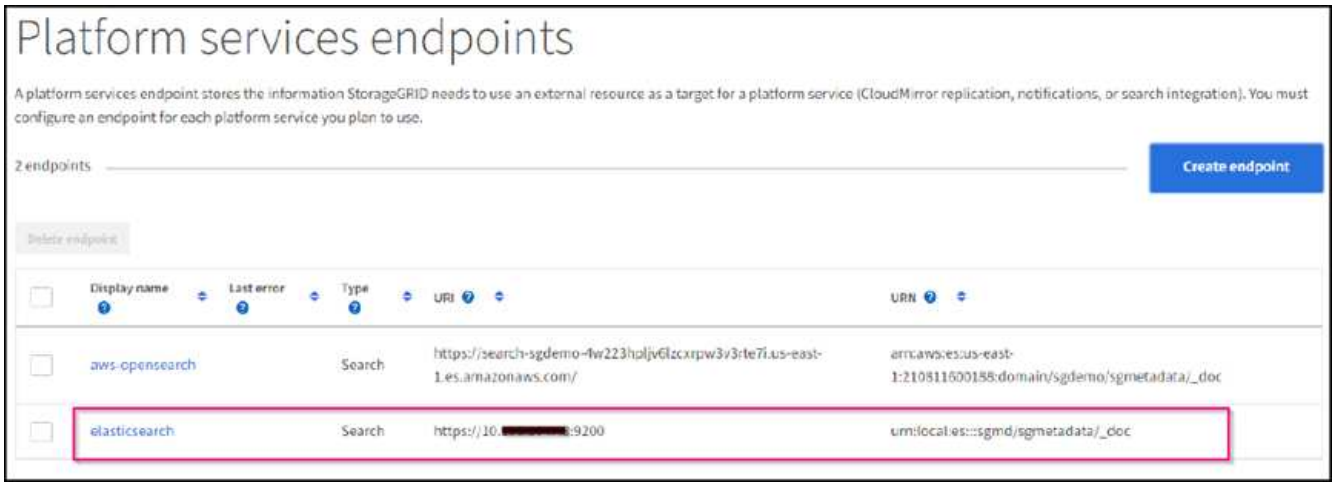


3. 認証タイプとしてBasic HTTPを選択し、Elasticsearchのインストールプロセスによって生成されたユーザ名「elastic」とパスワードを入力します。次のページに移動するには、[続行]をクリックします。



4. エンドポイントを確認するには、Do not verify Certificate and Test and Create Endpointを選択します。検

証に成功すると、次のスクリーンショットと同様のエンドポイント画面が表示されます。検証が失敗した場合は、URN、URI、およびユーザ名とパスワードのエントリが正しいことを確認してください。



バケット検索統合サービスの設定

プラットフォームサービスエンドポイントの作成後、次の手順では、オブジェクトの作成、削除、またはそのメタデータ/タグの更新が行われるたびに定義済みのエンドポイントにオブジェクトメタデータを送信するように、このサービスをバケットレベルで設定します。

Tenant Managerを使用して検索統合を設定し、カスタムのStorageGRID 設定XMLをバケットに次のように適用できます。

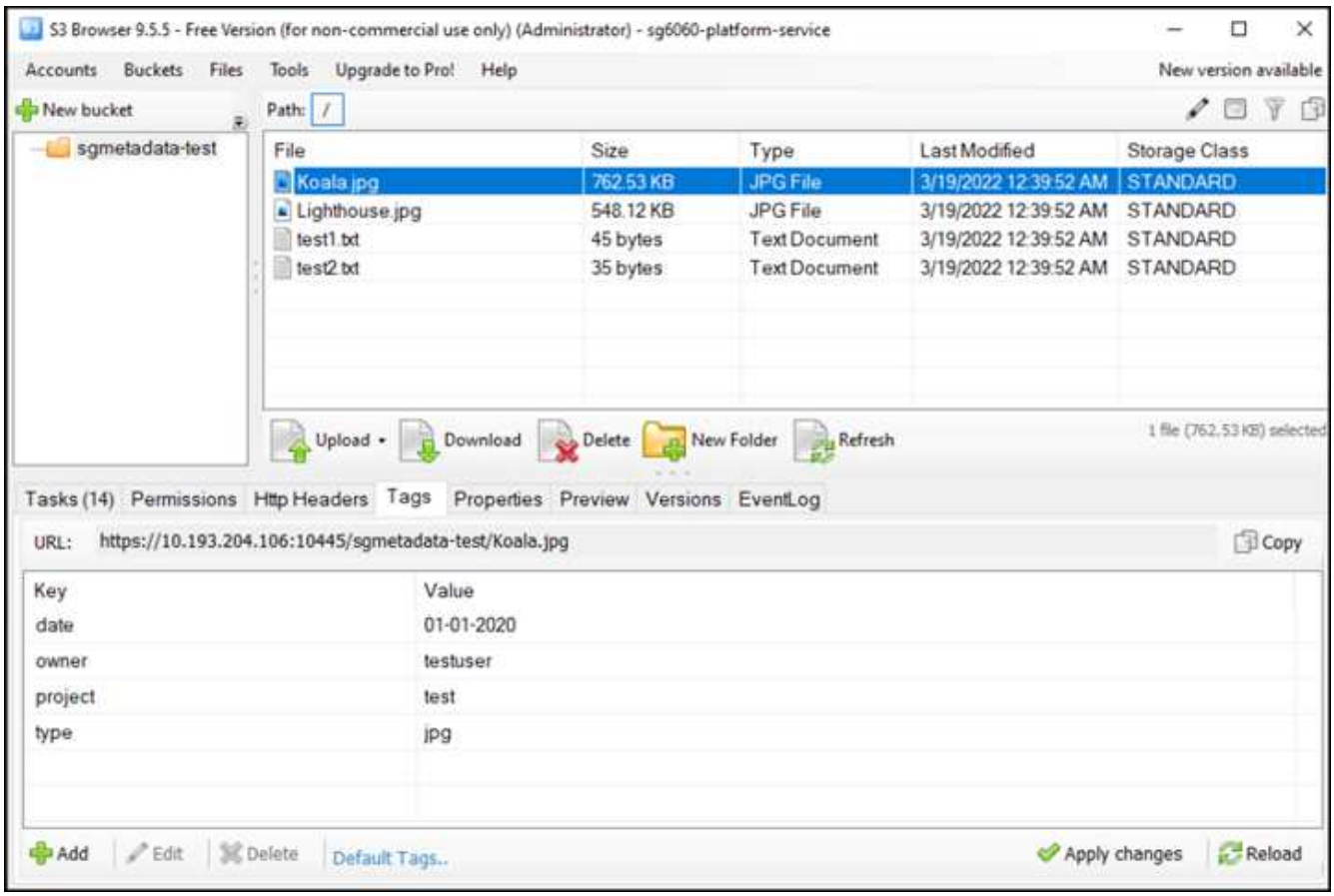
1. Tenant Managerで、Storage（S3）> Bucketsに移動します
2. Create Bucket（バケットの作成）をクリックし、バケット名（例：sgmetadatatest'）を入力して、デフォルトのus-east-1リージョンを受け入れます。
3. [Continue]>[Create Bucket]をクリックします。
4. バケットの概要ページを表示するには、バケット名をクリックし、プラットフォームサービスを選択します。
5. [検索統合を有効にする]ダイアログボックスを選択します。表示されたXMLボックスに、この構文を使用して設定XMLを入力します。

   強調表示されたURNは、定義したプラットフォームサービスエンドポイントと一致する必要があります。別のブラウザタブを開いてTenant Managerにアクセスし、定義済みのプラットフォームサービスエンドポイントからURNをコピーできます。

   この例ではプレフィックスを使用していません。つまり、このバケット内のすべてのオブジェクトのメタデータが、前に定義したElasticsearchエンドポイントに送信されます。

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

6. S3 Browserを使用して、テナントアクセス/シークレットキーを使用してStorageGRID に接続し、テストオブジェクトを「sgmetadata-test」バケットにアップロードし、タグまたはカスタムメタデータをオブジェクトに追加します。



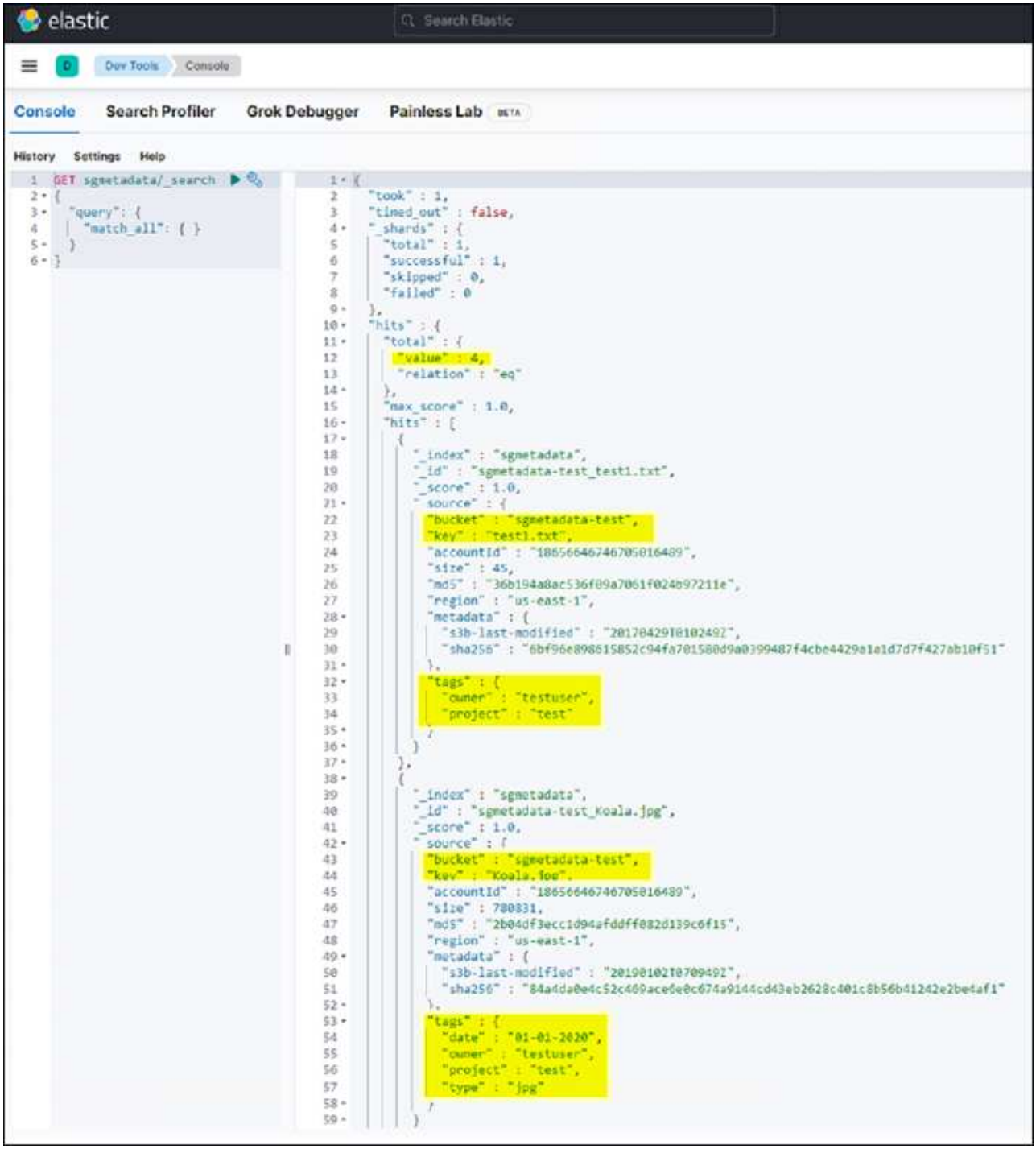
7. Kibana UIを使用して、オブジェクトメタデータがsgmetadataのインデックスにロードされたことを確認します。

   a. メニューから、Management > Dev Toolsを選択します。

   b. 左側のコンソールパネルにサンプルクエリを貼り付け、三角形の記号をクリックして実行します。

      次の例のスクリーンショットでは、クエリ1のサンプル結果に4つのレコードが表示されています。これはバケット内のオブジェクトの数に一致します。

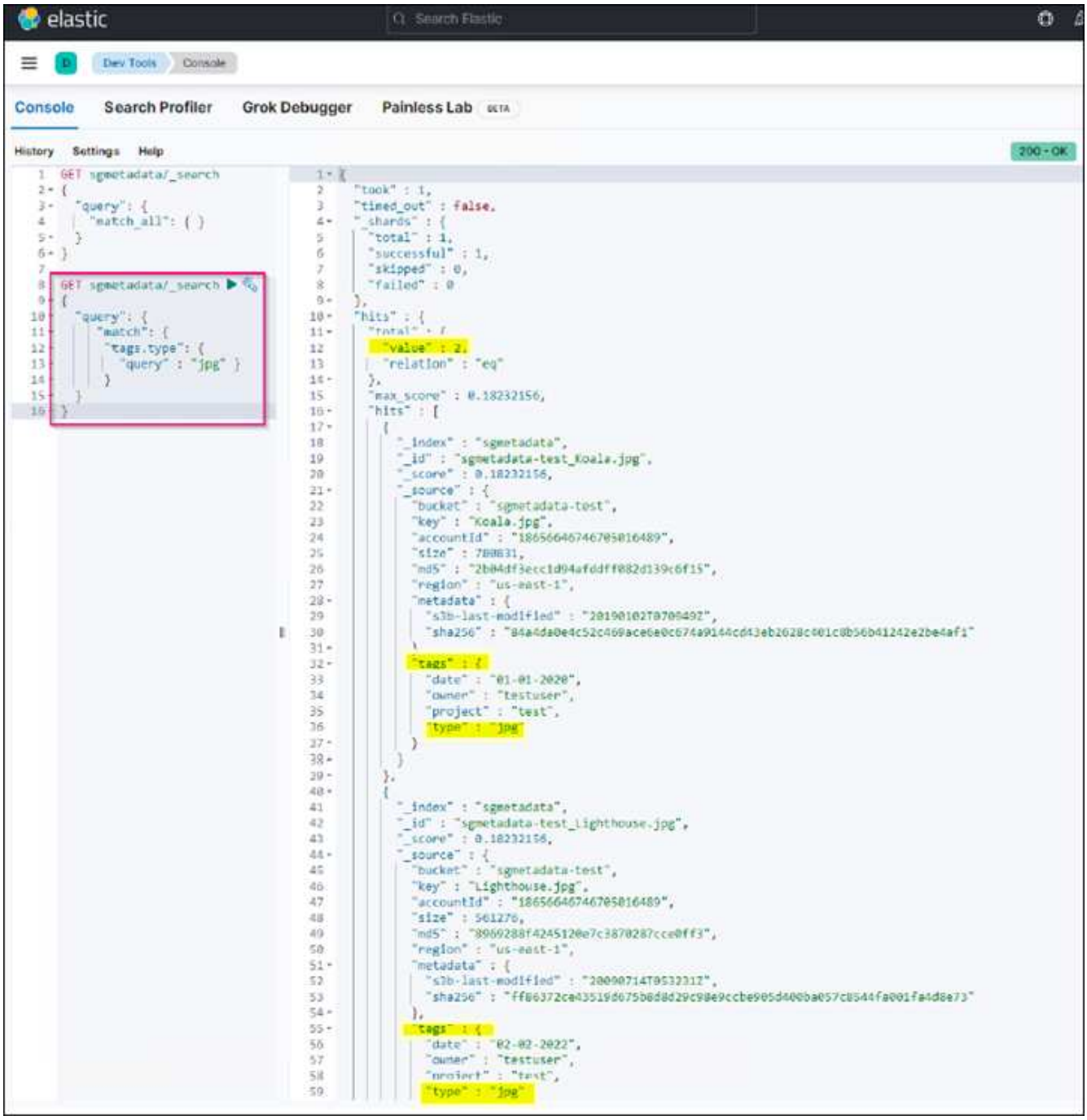
```
GET sgmetadata/_search
{
    "query": {
        "match_all": { }
}
}
```



次のスクリーンショットのクエリ2のサンプル結果は、タグタイプがjpgの2つのレコードを示しています。

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

+



追加情報の参照先

このドキュメントに記載されている情報の詳細については、以下のドキュメントや Web サイトを参照してください。

- "プラットフォームサービスとは"
- "StorageGRID 11.6 ドキュメント"

Angela Cheng著_

ノードクローン

ノードクローンに関する考慮事項とパフォーマンス

ノードクローンに関する考慮事項

ノードクローンを使用すると、機器更改（Tech Refresh）の際に既存のアプライアンスノードをすばやく交換したり、容量を増やしたり、StorageGRID システムのパフォーマンスを向上させたりできます。ノードクローンは、KMSを使用したノード暗号化への変換や、ストレージノードをDDP8からDDP16に変更する場合にも役立ちます。

- ソースノードの使用済み容量は、クローンプロセスの完了に必要な時間とは関係ありません。ノードクローンは、ノードの空きスペースを含むノードのフルコピーです。
- ソースアプライアンスとデスティネーションアプライアンスのPGEバージョンが同じである必要があります
- デスティネーションノードの容量は常にソースノードよりも大きくする必要があります
  - 新しいデスティネーションアプライアンスのドライブサイズがソースよりも大きいことを確認します
  - デスティネーションアプライアンスのドライブサイズが同じで、DDP8用に設定されている場合は、DDP16用にデスティネーションを設定できます。ソースがすでにDDP16用に設定されている場合、ノードのクローニングは実行できません。
  - SG5660またはSG5760アプライアンスからSG6060アプライアンスに移行する場合、SG5x60には容量ドライブが60本搭載されていますが、SG6060には58本しか搭載されていません。
- ノードのクローニングプロセスでは、クローニングプロセスの実行中はソースノードがグリッドに対してオフラインになっている必要があります。この間に追加のノードがオフラインになると、クライアントサービスに影響する可能性があります。
- ストレージノードをオフラインにできるのは15日間だけです。クローニングプロセスの推定日数が15日に近い場合、または15日を超える場合は、拡張と運用停止の手順を使用します。
- 拡張シェルフを搭載したSG6060では、正しいシェルフドライブサイズの時間をベースアプライアンスの時間に追加して、フルクローン期間を取得する必要があります。
- ターゲットストレージアプライアンスのボリューム数は、ソースノードのボリューム数以上である必要があります。16個のオブジェクトストアボリューム（rangedb）を含むソースノードを、12個のオブジェクトストアボリュームを含むターゲットストレージアプライアンスにクローニングすることはできません。これは、ターゲットアプライアンスの容量がソースノードよりも大きい場合でも同様です。ほとんどのストレージアプライアンスにはオブジェクトストアボリュームが16個ありますが、オブジェクトストアボリュームが12個しかないSGF6112ストレージアプライアンスは除きます。たとえば、SG5760からSGF6112にクローニングすることはできません。

ノードクローンのパフォーマンスを見積もります

次の表に、ノードクローンの所要時間の推定値を示します。条件は状況によって異なるため、*太字*で示されたエントリは、ノードが停止した場合に15日を超えるリスクがあります。

DDP8

SG5612 →任意

ネットワークインターフェイスの速度	**4TB**ドライブサイズ	**8TB**ドライブサイズ	**10TB**ドライブサイズ	**12TB**ドライブサイズ	**16TB**ドライブサイズ	**18TB**のドライブサイズ
10Gb	1 日	2日	2.5日	3日	4日	4.5日
25GB	1 日	2日	2.5日	3日	4日	4.5日

SG5712 →任意

ネットワークインターフェイスの速度	**4TB**ドライブサイズ	**8TB**ドライブサイズ	**10TB**ドライブサイズ	**12TB**ドライブサイズ	**16TB**ドライブサイズ	**18TB**のドライブサイズ
10Gb	1 日	2日	2.5日	3日	4日	4.5日
25GB	1 日	2日	2.5日	3日	4日	4.5日

SG5660 → **SG5760**を選択してください

ネットワークインターフェイスの速度	**4TB**ドライブサイズ	**8TB**ドライブサイズ	**10TB**ドライブサイズ	**12TB**ドライブサイズ	**16TB**ドライブサイズ	**18TB**のドライブサイズ
10Gb	3日間	6日	7 日	8.5日	11.5日	• 13日*
25GB	3日間	6日	7 日	8.5日	11.5日	• 13日*

SG5660 → **SG6060**

ネットワークインターフェイスの速度	**4TB**ドライブサイズ	**8TB**ドライブサイズ	**10TB**ドライブサイズ	**12TB**ドライブサイズ	**16TB**ドライブサイズ	**18TB**のドライブサイズ
10Gb	2.5日	4.5日	5.5日	6.5日	9日	10日間
25GB	2日間	4日	5日	6日	8日間	9日

SG5760 → **SG5760**

ネットワークインターフェイスの速度	**4TB**ドライブサイズ	**8TB**ドライブサイズ	**10TB**ドライブサイズ	**12TB**ドライブサイズ	**16TB**ドライブサイズ	**18TB**のドライブサイズ
10Gb	3日間	6日	7 日	8.5日	11.5日	• 13日*
25GB	3日間	6日	7 日	8.5日	11.5日	• 13日*

SG5760 → SG6060

ネットワークインターフェイスの速度	**4TB**ドライブサイズ	**8TB**ドライブサイズ	**10TB**ドライブサイズ	**12TB**ドライブサイズ	**16TB**ドライブサイズ	**18TB**のドライブサイズ
10Gb	2.5日	4.5日	5.5日	6.5日	9日	10日間
25GB	1.5日	3日	3.5日	4.5日	6日	6.5日

SG6060 → SG6060

ネットワークインターフェイスの速度	**4TB**ドライブサイズ	**8TB**ドライブサイズ	**10TB**ドライブサイズ	**12TB**ドライブサイズ	**16TB**ドライブサイズ	**18TB**のドライブサイズ
10Gb	2.5日	4.5日	5.5日	6.5日	8.5日	9.5日
25GB	1.5日	3日	3.5日	4日	5.5日	6日

DDP16

SG5760 → SG5760

ネットワークインターフェイスの速度	**4TB**ドライブサイズ	**8TB**ドライブサイズ	**10TB**ドライブサイズ	**12TB**ドライブサイズ	**16TB**ドライブサイズ	**18TB**のドライブサイズ
10Gb	3.5日	6.5日	8日間	9.5日	12.5日	• 14日*
25GB	3.5日	6.5日	8日間	9.5日	12.5日	• 14日*

SG5760 → SG6060

ネットワークインターフェイスの速度	**4TB**ドライブサイズ	**8TB**ドライブサイズ	**10TB**ドライブサイズ	**12TB**ドライブサイズ	**16TB**ドライブサイズ	**18TB**のドライブサイズ
10Gb	2.5日	5日	6日	7.5日	10日間	11日だ
25GB	2日間	3.5日	4日	5日	6.5日	7 日

SG6060 → SG6060

ネットワークインターフェイスの速度	**4TB**ドライブサイズ	**8TB**ドライブサイズ	**10TB**ドライブサイズ	**12TB**ドライブサイズ	**16TB**ドライブサイズ	**18TB**のドライブサイズ
10Gb	3.5日	5日	6日	7 日	9.5日	10.5日
25GB	2日間	3日	4日	4.5日	6日	7 日

拡張シェルフ（ソースアプライアンスの各シェルフについて、上記の**SG6060**に追加）

ネットワークインターフェイスの速度	**4TB**ドライブサイズ	**8TB**ドライブサイズ	**10TB**ドライブサイズ	**12TB**ドライブサイズ	**16TB**ドライブサイズ	**18TB**のドライブサイズ
10Gb	3.5日	5日	6日	7 日	9.5日	10.5日
25GB	2日間	3日	4日	4.5日	6日	7 日

アロンクライン著

ポート再マッピングの使用方法

さまざまな理由で、着信ポートまたは発信ポートの再マッピングが必要になることがあります。従来のCLBロードバランササービスから現在のnginxサービスロードバランサエンドポイントに移行し、同じポートを維持してクライアントへの影響を軽減する場合、管理ノードクライアントネットワークのクライアントS3にポート443を使用する場合、またはファイアウォールの制限に使用する場合があります。

ポートの再マッピングを使用して、**S3**クライアントを**CLB**から**NGINX**に移行します

StorageGRID 11.3より前のリリースでは、ゲートウェイノードに含まれているロードバランササービスはConnection Load Balancer（CLB）です。StorageGRID 11.3では、HTTPトラフィックのロードバランシングを実現する機能豊富な統合解決策 として、NGINXサービスが導入されました。CLBサービスは現在のリリースのStorageGRID でも引き続き使用できるため、新しいロードバランサエンドポイントの設定でポート8082を再利用することはできません。この問題を回避するために、8082インバウンドポートが10443に再マッピングされます。これにより、ゲートウェイのポート8082に着信するすべてのHTTPS要求は、CLBサービスをバイパスしてNGINXサービスに接続し、ポート10443にリダイレクトされます。以下の手順はVMwareを対象としていますが、PORT_REMAP機能はすべてのインストール方法に適用され、ベアメタル環境とアプライアンスでも同様のプロセスを使用できます。

VMware仮想マシンゲートウェイノードの導入

次の手順は、StorageGRID Open Virtualization Format（OVF）を使用してゲートウェイノードをVMとしてVMware vSphere 7に導入するStorageGRID 環境を対象としています。このプロセスでは、VMを破壊的に削除し、同じ名前と構成でVMを再導入します。VMの電源をオンにする前に、vAppプロパティを変更してポートを再マッピングし、VMの電源をオンにしてノードのリカバリプロセスに従います。

前提条件

- StorageGRID 11.3以降を実行している
- インストールされているStorageGRID バージョンのVMwareインストールファイルをダウンロードし、アクセスできるようにしておきます。
- VMの電源オン/オフ、VMおよびvAppの設定の変更、vCenterからのVMの削除、OVFによるVMの導入を行う権限を持つvCenterアカウントが必要です。
- ロードバランサエンドポイントを作成しておきます
  - ポートが目的のリダイレクトポートに設定されている
  - エンドポイントのSSL証明書がCLBサービス用の[Configuration]/[Server Certificates]/[Object Storage API Service Endpoints Server Certificate]にインストールされているものと同じであるか、クライアントが証明書の変更を承認できる。

```
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.
```

最初のゲートウェイノードを削除します

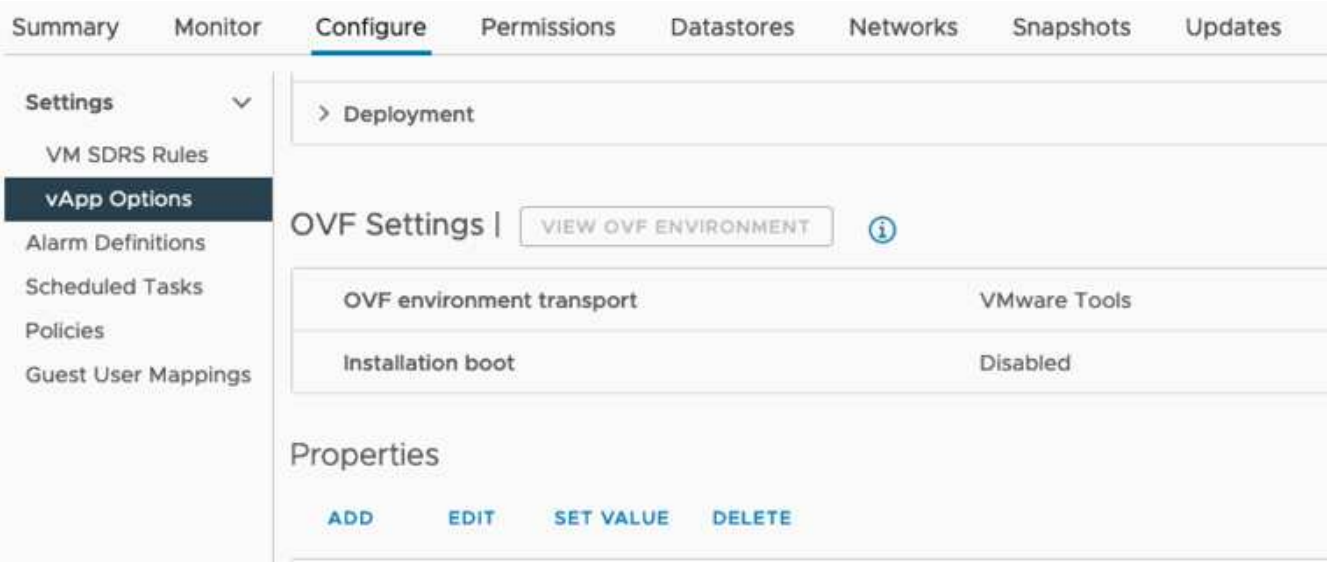
最初のゲートウェイノードを削除するには、次の手順を実行します。

1. グリッドに複数のノードがある場合は、開始するゲートウェイノードを選択します。
2. 必要に応じて、すべてのDNSラウンドロビンエンティティまたはロードバランサプールからノードIPを削除します。
3. Time-To-Live（TTL）と開いているセッションが期限切れになるまで待ちます。
4. VMノードの電源をオフにします。
5. ディスクからVMノードを削除します。

交換用ゲートウェイノードを導入します

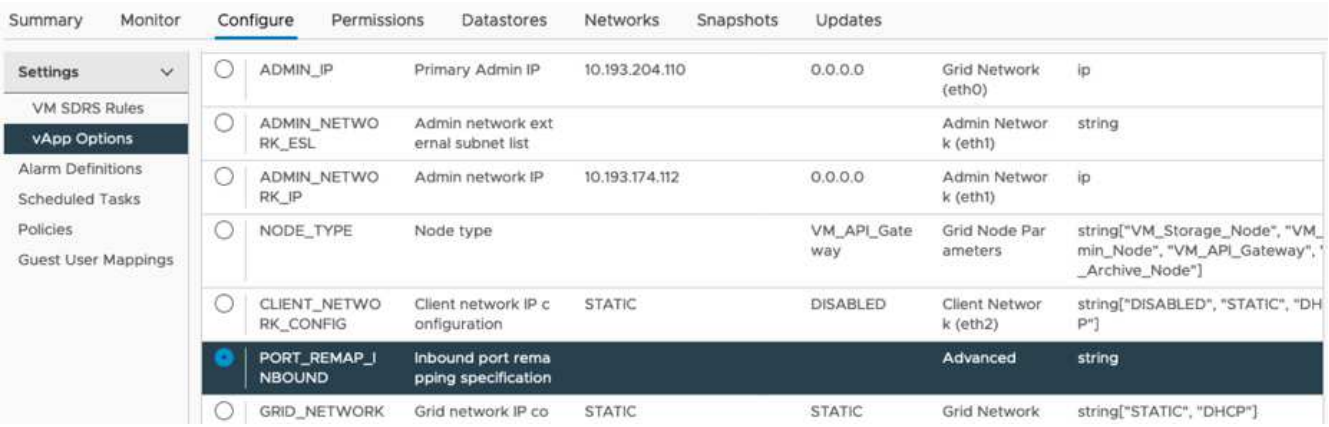
交換用ゲートウェイノードを導入するには、次の手順を実行します。

1. サポートサイトからダウンロードしたインストールパッケージから.ovf、.mf、.vmdkファイルを選択して、OVFから新しいVMを導入します。
   - vsphere-gateway.mf
   - vSphere-gateway.ovf
   - NetApp-sg-11.4.0-20200721.1338.d3969b3.vmdk
2. 導入が完了したら、VMのリストからVMを選択し、[Configure]タブ[vApp Options]を選択します。



タブ"]

3. [Properties]セクションまで下にスクロールし、PORT_REMAP_INBOUNDプロパティを選択します



4. [プロパティ]リストの一番上までスクロールし、[編集]をクリックします

ボタン"]

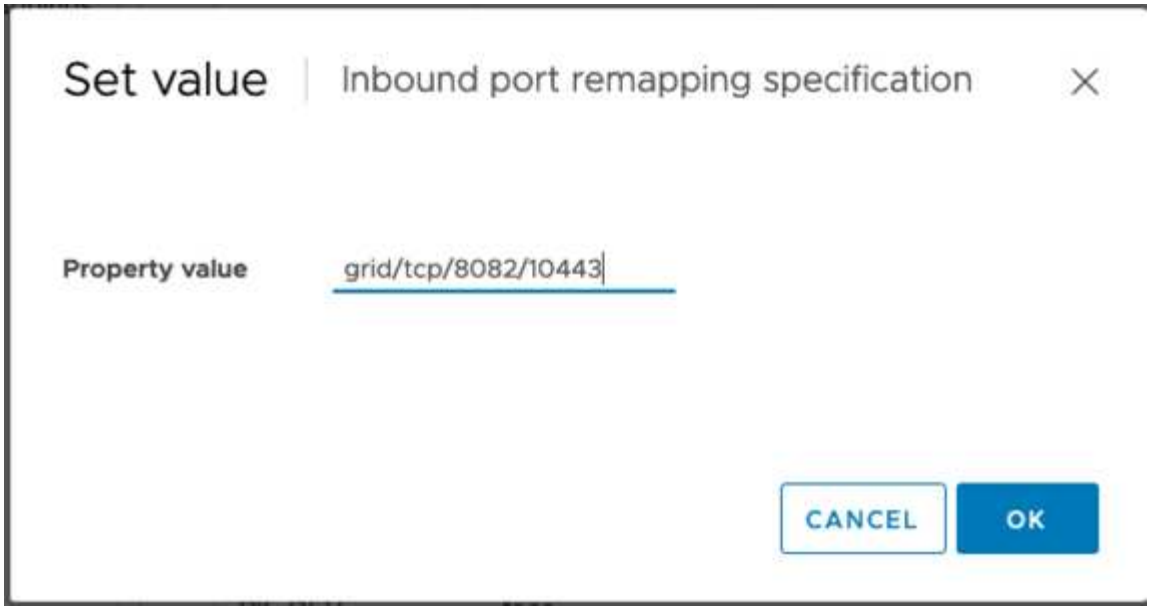
5. [タイプ]タブを選択し、[ユーザー設定可能]チェックボックスがオンになっていることを確認して、[保存]をクリックします。

タブ"]

6. 「PORT_REMAP_INBOUND」プロパティが選択された状態で、[Properties]リストの上部にある[Set Value]をクリックします。

ボタン"]

7. [Property Value]フィールドに、ネットワーク（グリッド、管理者、またはクライアント）、TCP、元のポート（8082）、および新しいポート（10443）をそれぞれの値の間にを含めて入力します（次の図を参照）。

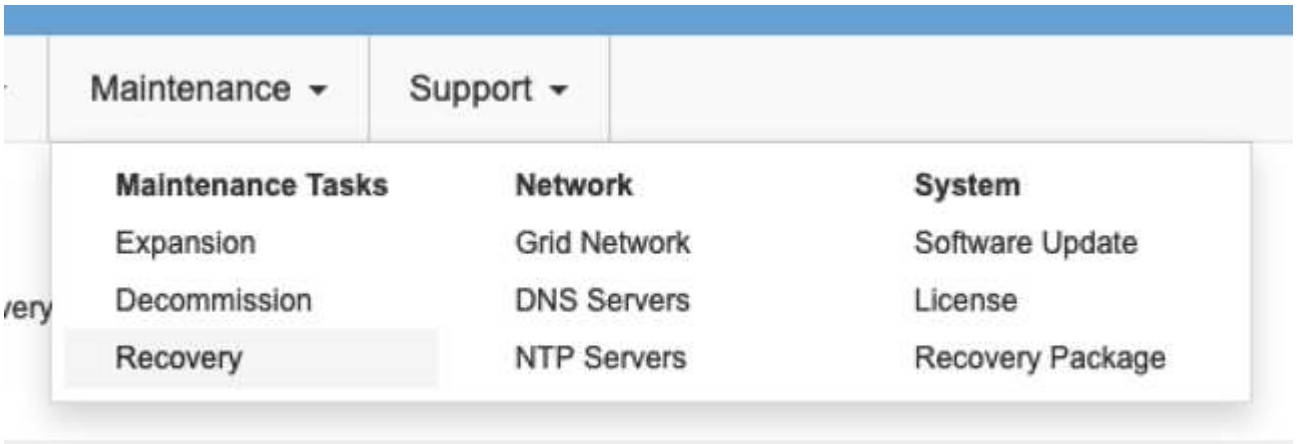


8. 複数のネットワークを使用している場合は、カンマ（,）を使用してネットワークの文字列を区切ります（例：grid/tcp/8082/10443、admin/tcp/8082/10443、client/tcp/8082/10443）

ゲートウェイノードをリカバリ

ゲートウェイノードをリカバリするには、次の手順を実行します。

1. グリッド管理UIの[Maintenance/Recovery]セクションに移動します。



メニュー"]

2. VMノードの電源をオンにし、ノードがグリッド管理UIの[Maintenance/Recovery Pending Nodes]セクションに表示されるまで待ちます。


```
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. ノードのリカバリが完了したら、すべてのDNSラウンドロビンエンティティまたはロードバランサプール（該当する場合）にIPを含めることができます。

   これで、ポート8082のHTTPSセッションはポート10443に接続されます

管理ノードでクライアント**S3**アクセス用のポート**443**を再マッピングします

StorageGRID システムでの管理ノード、または管理ノードを含むHAグループのデフォルトの設定は、ポート443と80が管理およびテナントマネージャUI用に予約されており、ロードバランサエンドポイントには使用できません。これへの解決策 では、ポートの再マッピング機能を使用して、インバウンドポート443をロードバランサエンドポイントとして設定される新しいポートにリダイレクトします。完了したクライアントS3トラフィックでポート443を使用できるようになると、グリッド管理UIにはポート8443経由でのみアクセスでき、テナント管理UIにはポート9443経由でのみアクセスできるようになります。ポートの再マッピング機能は、ノードのインストール時にのみ設定できます。グリッド内のアクティブノードのポートの再マッピングを実装するには、そのノードをインストール前の状態にリセットする必要があります。これは破壊的な手順 であり、設定の変更後にノードをリカバリすることも含まれます。

ログとデータベースをバックアップします

管理ノードには、監査ログ、Prometheus指標のほか、属性、アラーム、アラートに関する履歴情報が格納されます。管理ノードが複数あるということは、このデータのコピーが複数あることを意味します。グリッドに管理ノードが複数ない場合は、このプロセスの最後でノードがリカバリされたあとにリストアできるように、このデータを保持しておく必要があります。グリッドに別の管理ノードがある場合は、リカバリプロセス中にそのノードからデータをコピーできます。グリッド内に別の管理ノードがない場合は、ノードを破棄する前に、次の手順に従ってデータをコピーできます。

監査ログをコピーする

1. 管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`

d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

e. SSH エージェントに SSH 秘密鍵を追加します。入力するコマンド `ssh-add`

f. に記載されているSSHアクセスパスワードを入力します `Passwords.txt` ファイル。

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

2. すべての監査ログファイルを別のグリッドノードの一時的な場所にコピーするディレクトリを作成します。lets use_storage_node_01_：

   a. `ssh admin@storage_node_01_IP`

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

3. 管理ノードに戻り、AMSサービスを停止して新しいログファイルが作成されないようにします。 `service ams stop`

4. audit.log ファイルの名前を変更して、リカバリした管理ノードへのコピー時に既存のファイルが上書きされないようにします。

   a. audit.log の名前を、 yyyy-mm-dd.txt.1 などの一意の番号の付いたファイル名に変更します。たとえば、監査ログファイルの名前を2015-10-25.txt.1に変更できます

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

5. AMSサービスを再起動します。 `service ams start`

6. すべての監査ログファイルをコピーします。 `scp * admin@storage_node_01_IP:/var/local/tmp/saved-audit-logs`

Prometheusデータをコピー

> Prometheus データベースのコピーには 1 時間以上かかる場合があります。管理ノードでサービスが停止している間は、Grid Managerの一部の機能が使用できなくなります。

1. Prometheusデータを別のグリッドノードの一時的な場所にコピーするディレクトリを作成します。この場合もuser_storage_node_01_：

   a. ストレージノードにログインします。

      i. 次のコマンドを入力します。 `ssh admin@storage_node_01_IP`

      ii. に記載されているパスワードを入力します `Passwords.txt` ファイル。

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

2. 管理ノードにログインします。

   a. 次のコマンドを入力します。 `ssh admin@admin_node_IP`

   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。

c. 次のコマンドを入力してrootに切り替えます。 `su -`

d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

e. SSH エージェントに SSH 秘密鍵を追加します。入力するコマンド `ssh-add`

f. に記載されているSSHアクセスパスワードを入力します `Passwords.txt` ファイル。

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

3. 管理ノードから、Prometheusサービスを停止します。 `service prometheus stop`

   a. ソース管理ノードのPrometheusデータベースをストレージノードのバックアップ先ノードにコピーします。 `/rsync -azh --stats "/var/local/mysql_ibdata/prometheus/data" "storage_node_01_IP:/var/local/tmp/prometheus/"`

4. ソース管理ノードでPrometheusサービスを再起動します.`service prometheus start`

履歴情報をバックアップします

履歴情報はMySQLデータベースに保存されます。データベースのコピーをダンプするには、ネットアップのユーザとパスワードが必要です。グリッド内に別の管理ノードがある場合は、この手順は必要なく、リカバリプロセス中に残りの管理ノードからデータベースをクローニングできます。

1. 管理ノードにログインします。

   a. 次のコマンドを入力します。 `ssh admin@admin_node_IP`

   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。

   c. 次のコマンドを入力してrootに切り替えます。 `su -`

   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

   e. SSH エージェントに SSH 秘密鍵を追加します。入力するコマンド `ssh-add`

   f. に記載されているSSHアクセスパスワードを入力します `Passwords.txt` ファイル。

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

2. 管理ノードでStorageGRID サービスを停止し、NTPとMySQLを起動します

   a. すべてのサービスを停止します。 `service servermanager stop`

   b. NTPサービスを再開します。 `service ntp start`.. MySQLサービスを再起動します。 `service mysql start`

3. miデータベースを/var/local/tmpにダンプします

   a. 次のコマンドを入力します。 `mysqldump -u username -p password mi > /var/local/tmp/mysql-mi.sql`

4. MySQLダンプファイルを別のノードにコピーします。ここでは_storage_node_01を使用します。 `scp /var/local/tmp/mysql-mi.sql storage_node_01_IP:/var/local/tmp/mysql-mi.sql`

   a. 他のサーバにパスワードなしでアクセスする必要がなくなった場合は、 SSH エージェントから秘密鍵

を削除します。入力するコマンド `ssh-add -D`

管理ノードをリビルドします

グリッド内の別の管理ノードに必要なすべてのデータとログのバックアップコピーが作成されたか、一時的な場所に格納されたので、次にアプライアンスをリセットしてポートの再マッピングを設定します。

1. アプライアンスをリセットすると、アプライアンスは事前にインストールされた状態に戻り、ホスト名、IP、およびネットワーク設定のみが保持されます。すべてのデータが失われるため、重要な情報のバックアップが確実に作成されます。
   a. 次のコマンドを入力します。 `sgareinstall`

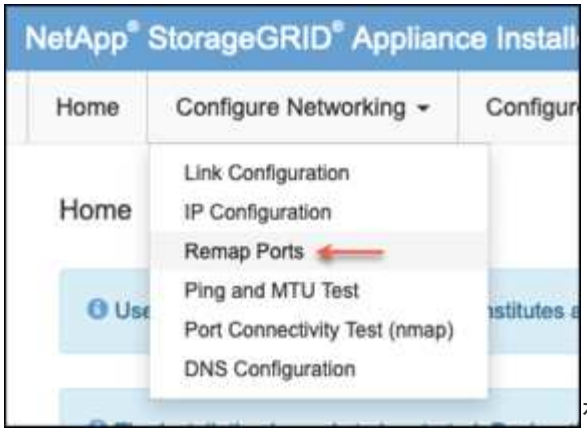
```
root@sg100-01:~ # sgareinstall
WARNING: All StorageGRID Webscale services on this node will be shut
down.
WARNING: Data stored on this node may be lost.
WARNING: You will have to reinstall StorageGRID Webscale to this
node.

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.
```

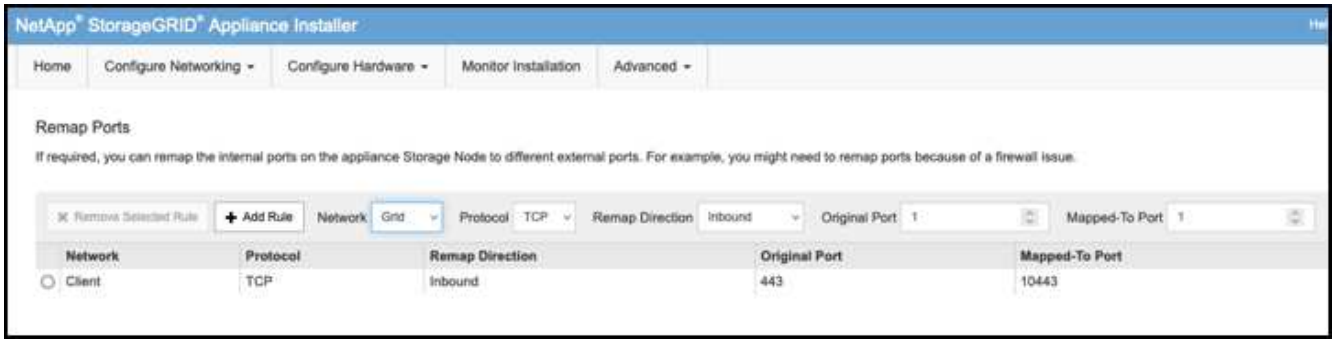
2. しばらくするとアプライアンスがリブートし、ノードのPGE UIにアクセスできるようになります。
3. [Configure Networking]にアクセスします



を選択します"]

4. 目的のネットワーク、プロトコル、方向、およびポートを選択し、[Add Rule]ボタンをクリックします。

> グリッドネットワーク上のインバウンドポート443を再マッピングすると、インストールおよび拡張手順が中断されます。グリッドネットワークのポート443を再マッピングすることは推奨されません。



5. 必要なポートの再マッピングが追加されている場合は、ホームタブに戻り、[Start Installation]ボタンをクリックします。

で管理ノードのリカバリ手順を実行できるようになりました "製品ドキュメント"

データベースとログをリストアします

管理ノードのリカバリが完了したら、指標、ログ、履歴情報をリストアできます。グリッドに別の管理ノードがある場合は、に従ってください "製品ドキュメント" _prometheus-clone-db.sh_and_mi-clone-db.sh_scripts を使用する。これが唯一の管理ノードであり、このデータをバックアップすることを選択した場合は、次の手順に従って情報を復元できます。

監査ログをコピーして元に戻します

1. 管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

e. SSH エージェントに SSH 秘密鍵を追加します。入力するコマンド `ssh-add`

f. に記載されているSSHアクセスパスワードを入力します `Passwords.txt` ファイル。

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

2. 保持されている監査ログファイルをリカバリされた管理ノードにコピーします。 `scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY* .`
3. セキュリティ上の理由により、監査ログがリカバリされた管理ノードにコピーされたことを確認したら、監査ログを障害グリッドノードから削除します。
4. リカバリされた管理ノードで、監査ログファイルのユーザとグループの設定を更新します。 `chown ams-user:bycast *`

監査共有への既存のクライアントアクセスもリストアする必要があります。詳細については、 StorageGRID の管理手順を参照してください。

Prometheus指標をリストア

> Prometheus データベースのコピーには 1 時間以上かかる場合があります。管理ノードでサービスが停止している間は、Grid Managerの一部の機能が使用できなくなります。

1. 管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   e. SSH エージェントに SSH 秘密鍵を追加します。入力するコマンド `ssh-add`
   f. に記載されているSSHアクセスパスワードを入力します `Passwords.txt` ファイル。

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

2. 管理ノードから、Prometheusサービスを停止します。 `service prometheus stop`
   a. 一時的なバックアップ場所から管理ノードにPrometheusデータベースをコピーします。 `/rsync -azh --stats "backup_node:/var/local/tmp/prometheus/" "/var/local/mysql_ibdata/prometheus/"`
   b. データが正しいパスにあり、完全であることを確認します `ls /var/local/mysql_ibdata/prometheus/data/`
3. ソース管理ノードでPrometheusサービスを再起動します.`service prometheus start`

履歴情報をリストアします

1. 管理ノードにログインします。

a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

b. に記載されているパスワードを入力します `Passwords.txt` ファイル。

c. 次のコマンドを入力してrootに切り替えます。 `su -`

d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

e. SSH エージェントに SSH 秘密鍵を追加します。入力するコマンド `ssh-add`

f. に記載されているSSHアクセスパスワードを入力します `Passwords.txt` ファイル。

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

2. 代替ノードからMySQLダンプファイルをコピーします。 `scp grid_node_IP_:/var/local/tmp/mysql-mi.sql /var/local/tmp/mysql-mi.sql`
3. 管理ノードでStorageGRID サービスを停止し、NTPとMySQLを起動します
   a. すべてのサービスを停止します。 `service servermanager stop`
   b. NTPサービスを再開します。 `service ntp start`.. MySQLサービスを再起動します。 `service mysql start`
4. miデータベースを削除し、新しい空のデータベースを作成します。 `mysql -u username -p password -A mi -e "drop database mi; create database mi;"`
5. データベースダンプからMySQLデータベースをリストアします。 `mysql -u username -p password -A mi < /var/local/tmp/mysql-mi.sql`
6. 他のすべてのサービスを再起動します `service servermanager start`

アロンクライン著

グリッドサイトの再配置とサイト全体のネットワーク変更手順

このガイドでは、マルチサイトグリッドでのStorageGRIDサイトの再配置の準備と手順について説明します。この手順を完全に理解し、スムーズなプロセスを実現し、クライアントの中断を最小限に抑えるために事前に計画しておく必要があります。

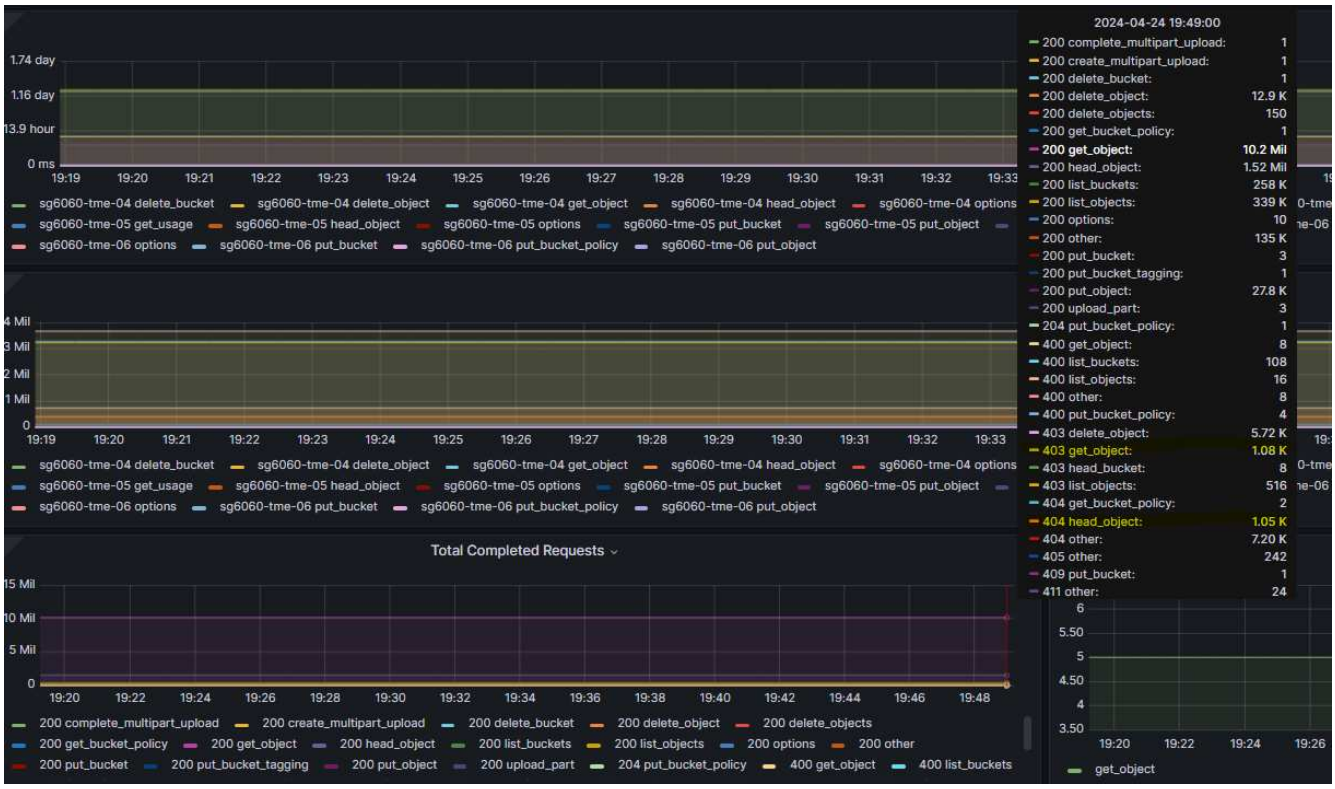
グリッド全体のグリッドネットワークを変更する必要がある場合は、を参照してください。
"グリッド内のすべてのノードの IP アドレスを変更します"。

サイトの再配置前の考慮事項

- Cassandraデータベースの再構築を回避するには、サイトの移動を完了し、すべてのノードを15日以内にオンラインにします。
  "ストレージノードを 15 日以上停止した状態にリカバリします"
- アクティブポリシー内のいずれかのILMルールで厳密な取り込み動作が使用されている場合は、サイトの再配置中にオブジェクトを引き続きグリッドに配置する必要がある場合は、負荷分散またはデュアルコミットに変更することを検討してください。
- ストレージアプライアンスに60本以上のドライブが搭載されている場合は、ディスクドライブが取り付け

られているシェルフを移動しないでください。 パック/移動の前に、各ディスクドライブにラベルを付け、ストレージエンクロージャから取り外します。

- StorageGRIDアプライアンスの変更グリッドネットワークVLANは、管理ネットワークまたはクライアントネットワーク経由でリモートで実行できます。 または、勤務地変更の前後にオンサイトで変更を実施する予定です。
- PUTの前に、お客様のアプリケーションがHEADを使用しているか、存在しないオブジェクトを取得しているかを確認「はい」の場合は、HTTP 500エラーを回避するためにバケットの整合性をstrong-siteに変更します。 不明な場合は、S3の概要Grafanaグラフ*[Grid manager]>[Support]>[Metrics]*を確認し、[Total Completed Request]グラフにカーソルを合わせます。 404 GET Objectまたは404 HEADオブジェクトの数が非常に多い場合は、1つ以上のアプリケーションがHEADまたはGET Non-existenceオブジェクトを使用している可能性があります。カウントは累積値です。異なるタイムライン上にマウスを移動すると、その差が表示されます。



サイトの再配置前に手順で**Grid IP**アドレスを変更

手順

1. 新しいグリッドネットワークサブネットが新しい場所で使用される場合は、"グリッドネットワークサブネットリストにサブネットを追加します。"
2. プライマリ管理ノードにログインし、change-ipを使用してグリッドIPを変更します。再配置用にノードをシャットダウンする前に、変更をステージングする必要があります*。
   a. [Grid IP]で[2]、[1]を選択します。

```
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. 5を選択して変更を表示

```
==============================================================================
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. [10]を選択して確定し、変更を適用します。

```
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. このステップで* stage *を選択する必要があります。

```
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. 上記の変更にプライマリ管理ノードが含まれている場合は、「**a**」と入力して手動でプライマリ管理ノードを再起動します

```
10.45.74.14 - PuTTY
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

Generating new grid networking description file... PASSED.
Running provisioning... PASSED.
Updating network configuration on LONDON-S1... PASSED.
Updating network configuration on LONDON-S2... PASSED.
Updating network configuration on LONDON-S3... PASSED.
Updating network configuration on LONDON-ADM1... PASSED.
Finished staging network changes. You must manually restart these nodes for the changes to take effect:

  LONDON-ADM1 (has IP 10.45.74.14 until restart)
  LONDON-S1 (has IP 10.45.74.16 until restart)
  LONDON-S2 (has IP 10.45.74.17 until restart)
  LONDON-S3 (has IP 10.45.74.18 until restart)

Importing bundles... PASSED.
*****************************************************************
*                          IMPORTANT                            *
*                                                               *
*  A new recovery package has been generated as a result of the *
*  configuration change. Select Maintenance > Recovery Package  *
*  in the Grid Manager to download it.                          *
*****************************************************************

Network Update Complete.  Primary admin restart required. Select 'continue' to restart this node immediately, 'abort' to restart manually.
Enter a to abort, c to continue [a/c]>
```

f. Enterキーを押して前のメニューに戻り、IPインターフェイスの変更を終了します。

```
Network Update Complete.  Primary admin restart required. Select 'continue' to restart this node immediately, 'abort' to restart manually.
Enter a to abort, c to continue [a/c]> a
Restart aborted. You must manually restart this node as soon as possible
Press Enter to return to the previous menu.
```

3. Grid Managerから、新しいリカバリパッケージをダウンロードします。* Grid Manager **>***メンテナンス>* リカバリパッケージ*
4. StorageGRIDアプライアンスでVLANの変更が必要な場合は、を参照してください。 アプライアンスVLANの変更。
5. サイトのすべてのノードおよびアプライアンスをシャットダウンし、必要に応じてディスクドライブにラベルを付けて取り外し、ラックを開梱して梱包して移動します。
6. 管理ネットワークのIP、クライアントのVLAN、IPアドレスを変更する場合は、再配置後に変更を実行できます。

アプライアンス**VLAN**の変更

以下の手順は、リモートから変更を実行するために、StorageGRIDアプライアンスの管理ネットワークまたはクライアントネットワークにリモートアクセスできることを前提としています。

手順

1. アプライアンスをシャットダウンする前に、"アプライアンスをメンテナンスモードにします"。

2. ブラウザを使用したStorageGRIDアプライアンスインストーラGUIへのアクセス https://<admin-or-client-network-ip>:8443。 アプライアンスをメンテナンスモードでブートすると、すでに使用されている新しいグリッドIPとしてグリッドIPを使用することはできません。
3. グリッドネットワークのVLANを変更します。 クライアント・ネットワーク経由でアプライアンスにアクセスする場合、現時点ではクライアントVLANは変更できません。移動後に変更できます。
4. アプライアンスにSSH接続し、「shutdown -h now」を使用してノードをシャットダウン
5. 新しいサイトでアプライアンスの準備が完了したら、を使用してStorageGRIDアプライアンスインストーラのGUIにアクセスします。 https://<grid-network-ip>:8443。 GUIでping / nmapツールを使用して、ストレージが最適な状態であり、他のグリッドノードへのネットワーク接続が確立されていることを確認します。
6. クライアントネットワークIPの変更を計画している場合は、この段階でクライアントVLANを変更できます。 クライアントネットワークは、このあとの手順でIP変更ツールを使用してクライアントネットワークIPを更新するまで準備ができていません。
7. メンテナンスモードを終了します。StorageGRID アプライアンス・インストーラから、 **Advanced**>* Reboot Controller* を選択し、 * Reboot into StorageGRID * を選択します。
8. すべてのノードが稼働し、[Grid]に接続問題が表示されなくなったら、必要に応じてchange-IPを使用してアプライアンスの管理ネットワークとクライアントネットワークを更新します。