제품 기능 가이드

How to enable StorageGRID in your environment

NetApp
March 07, 2024

목차

제품 기능 가이드 . . . 1
AWS 또는 Google Cloud용 클라우드 스토리지 풀을 생성합니다 . . . 1
Azure Blob Storage용 클라우드 스토리지 풀 생성 . . . 2
백업에 클라우드 스토리지 풀 사용 . . . 2
StorageGRID 검색 통합 서비스를 구성합니다 . . . 3
노드 클론 . . . 19
포트 재매핑 사용 방법 . . . 22

제품 기능 가이드

AWS 또는 Google Cloud용 클라우드 스토리지 풀을 생성합니다

StorageGRID 오브젝트를 외부 S3 버킷으로 이동하려는 경우 클라우드 스토리지 풀을 사용할 수 있습니다. 외부 버킷은 Amazon S3(AWS) 또는 Google Cloud에 속할 수 있습니다.

필요한 것

- StorageGRID 11.6이 구성되었습니다.
- AWS 또는 Google Cloud에서 외부 S3 버킷을 이미 설정했습니다.

단계

1. Grid Manager에서 * ILM * > * 스토리지 풀 * 으로 이동합니다.
2. 페이지의 클라우드 스토리지 풀 섹션에서 * 생성 * 을 선택합니다.

   Create Cloud Storage Pool 팝업이 나타납니다.

3. 표시 이름을 입력합니다.
4. 공급자 유형 드롭다운 목록에서 * Amazon S3 * 를 선택합니다.

   이 공급자 유형은 AWS S3 또는 Google Cloud에서 작동합니다.

5. 클라우드 스토리지 풀에 사용할 S3 버킷의 URI를 입력합니다.

   다음 두 가지 형식이 허용됩니다.

   "https://host:port`

   "http://host:port`

6. S3 버킷 이름을 입력합니다.

   지정하는 이름은 S3 버킷의 이름과 정확히 일치해야 합니다. 그렇지 않으면 클라우드 스토리지 풀을 생성하지 못합니다. 클라우드 스토리지 풀을 저장한 후에는 이 값을 변경할 수 없습니다.

7. 선택적으로 액세스 키 ID와 비밀 액세스 키를 입력합니다.
8. 드롭다운에서 * 인증서 확인 안 함 * 을 선택합니다.
9. 저장 * 을 클릭합니다.

예상 결과

Amazon S3 또는 Google Cloud에 대한 클라우드 스토리지 풀이 생성되었는지 확인합니다.

Jonathan Wong이 _

Azure Blob Storage용 클라우드 스토리지 풀 생성

StorageGRID 오브젝트를 외부 Azure 컨테이너로 이동하려는 경우 클라우드 스토리지 풀을 사용할 수 있습니다.

필요한 것

- StorageGRID 11.6이 구성되었습니다.
- 외부 Azure 컨테이너를 이미 설정했습니다.

단계

1. Grid Manager에서 * ILM * > * 스토리지 풀 * 으로 이동합니다.
2. 페이지의 클라우드 스토리지 풀 섹션에서 * 생성 * 을 선택합니다.

   Create Cloud Storage Pool 팝업이 나타납니다.

3. 표시 이름을 입력합니다.
4. 공급자 유형 드롭다운 목록에서 * Azure Blob Storage * 를 선택합니다.
5. 클라우드 스토리지 풀에 사용할 S3 버킷의 URI를 입력합니다.

   다음 두 가지 형식이 허용됩니다.

   "https://host:port`

   "http://host:port`

6. Azure 컨테이너 이름을 입력합니다.

   지정하는 이름은 Azure 컨테이너 이름과 정확히 일치해야 합니다. 그렇지 않으면 클라우드 스토리지 풀을 생성하지 못합니다. 클라우드 스토리지 풀을 저장한 후에는 이 값을 변경할 수 없습니다.

7. 필요한 경우 인증을 위해 Azure 컨테이너의 관련 계정 이름 및 계정 키를 입력합니다.
8. 드롭다운에서 * 인증서 확인 안 함 * 을 선택합니다.
9. 저장 * 을 클릭합니다.

예상 결과

Azure Blob Storage용 Cloud Storage Pool이 생성되었는지 확인합니다.

Jonathan Wong이 _

백업에 클라우드 스토리지 풀 사용

ILM 규칙을 생성하여 백업을 위해 오브젝트를 클라우드 스토리지 풀로 이동할 수 있습니다.

필요한 것

- StorageGRID 11.6이 구성되었습니다.
- 외부 Azure 컨테이너를 이미 설정했습니다.

단계

1. Grid Manager에서 * ILM * > * 규칙 * > * 생성 * 으로 이동합니다.
2. 설명을 입력합니다.
3. 규칙을 트리거할 기준을 입력합니다.
4. 다음 * 을 클릭합니다.
5. 오브젝트를 스토리지 노드로 복제합니다.
6. 배치 규칙을 추가합니다.
7. 객체를 클라우드 스토리지 풀에 복제합니다
8. 다음 * 을 클릭합니다.
9. 저장 * 을 클릭합니다.

예상 결과

보존 다이어그램에 백업용 StorageGRID 및 클라우드 스토리지 풀에 로컬로 저장된 객체가 표시되는지 확인합니다.

ILM 규칙이 트리거되면 클라우드 스토리지 풀에 복사본이 존재하므로 오브젝트 복원을 수행하지 않고 로컬에서 개체를 검색할 수 있는지 확인합니다.

Jonathan Wong이 _

StorageGRID 검색 통합 서비스를 구성합니다

이 가이드는 NetApp StorageGRID 11.6 검색 통합 서비스를 Amazon OpenSearch Service 또는 사내 Elasticsearch와 구성하기 위한 자세한 지침을 제공합니다.

소개

StorageGRID는 세 가지 유형의 플랫폼 서비스를 지원합니다.

- * StorageGRID CloudMirror 복제 *. StorageGRID 버킷에서 지정된 외부 대상으로 특정 객체를 미러링합니다.
- * 알림 *. 객체에서 수행한 특정 작업에 대한 알림을 지정된 외부 Amazon SNS(Amazon Simple Notification Service)로 보내는 버킷당 이벤트 알림입니다.
- * 통합 서비스 검색 *. S3(Simple Storage Service) 개체 메타데이터를 지정된 Elasticsearch 인덱스에 전송하여 외부 서비스를 사용하여 메타데이터를 검색하거나 분석할 수 있습니다.

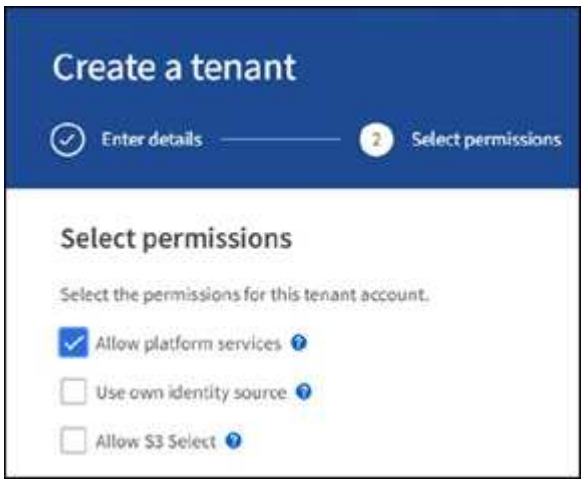
플랫폼 서비스는 테넌트 관리자 UI를 통해 S3 테넌트에서 구성합니다. 자세한 내용은 을 참조하십시오 "플랫폼 서비스 사용에 대한 고려 사항".

이 문서는 에 대한 보충 자료로 사용됩니다 "StorageGRID 11.6 테넌트 가이드" 및 에서는 검색 통합 서비스를 위한 엔드포인트 및 버킷 구성에 대한 단계별 지침과 예제를 제공합니다. 여기에 포함된 AWS(Amazon Web Services) 또는 온프레미스 Elasticsearch 설정 지침은 기본 테스트 또는 데모 전용입니다.

대상 고객은 그리드 관리자, 테넌트 관리자에 익숙해야 하며, StorageGRID 검색 통합 테스트를 위한 기본 업로드(PUT) 및 다운로드(GET) 작업을 수행하기 위해 S3 브라우저에 액세스할 수 있어야 합니다.

테넌트 생성 및 플랫폼 서비스 활성화

1. Grid Manager를 사용하여 S3 테넌트를 생성하고 표시 이름을 입력한 다음 S3 프로토콜을 선택합니다.
2. 사용 권한 페이지에서 플랫폼 서비스 허용 옵션을 선택합니다. 필요한 경우 다른 사용 권한을 선택합니다.



3. 테넌트 루트 사용자 초기 암호를 설정하거나, 격자에서 페더레이션 식별 이 설정된 경우 테넌트 계정을 구성할 루트 액세스 권한이 있는 통합 그룹을 선택합니다.
4. 루트로 로그인 을 클릭하고 버킷:버킷 생성 및 관리 를 선택합니다.

   그러면 Tenant Manager 페이지로 이동합니다.

5. Tenant Manager에서 내 액세스 키를 선택하여 나중에 테스트할 S3 액세스 키를 생성하고 다운로드합니다.

Amazon OpenSearch로 통합 서비스를 검색합니다

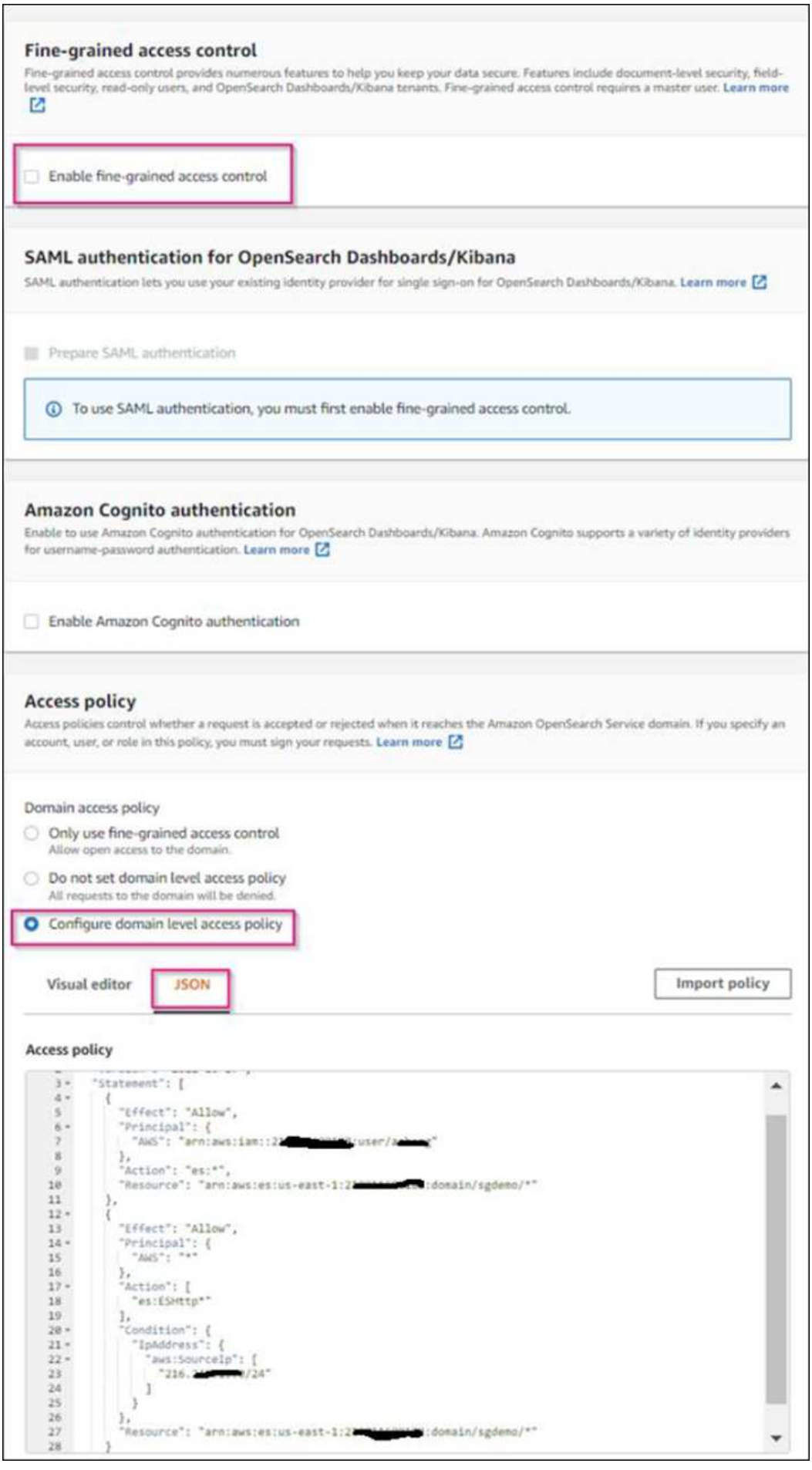
Amazon OpenSearch(이전의 **Elasticsearch)** 서비스 설정

테스트/데모용으로만 OpenSearch 서비스를 빠르고 간편하게 설정하려면 이 절차를 사용하십시오. 온-프레미스 Elasticsearch를 사용하여 검색 통합 서비스를 사용하는 경우 섹션을 참조하십시오 온-프레미스 Elasticsearch와 통합 서비스를 검색합니다.

> OpenSearch 서비스에 가입하려면 유효한 AWS 콘솔 로그인, 액세스 키, 비밀 액세스 키 및 권한이 있어야 합니다.

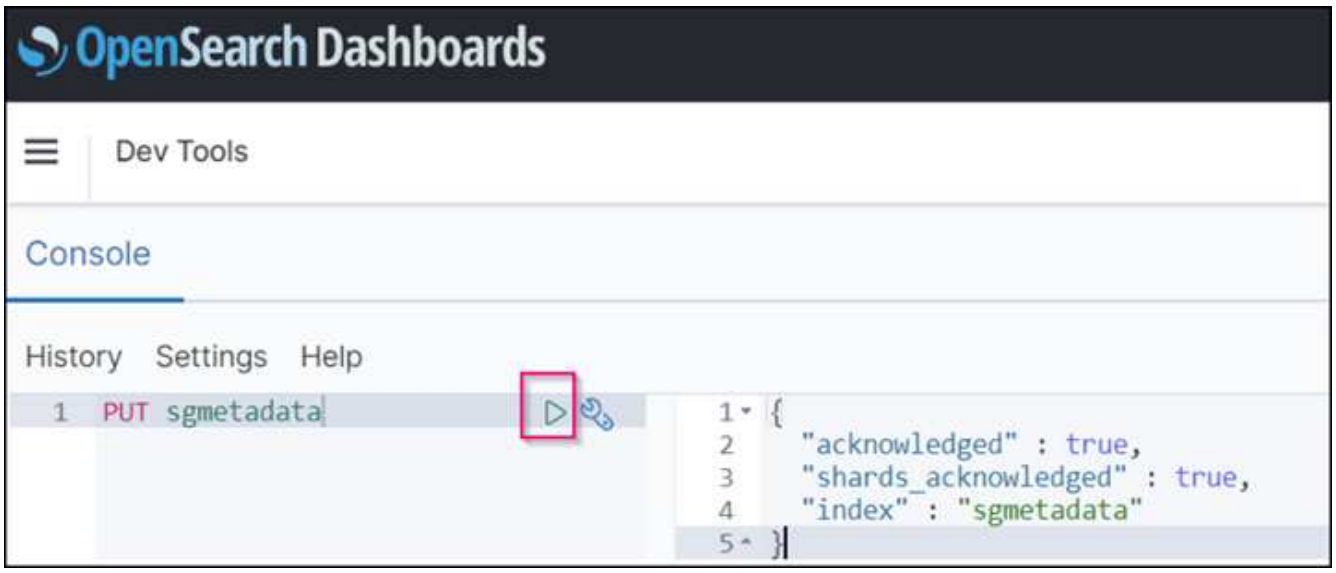
1. 의 지침에 따라 새 도메인을 만듭니다 "AWS OpenSearch 서비스 시작"다음 사항을 제외한 경우:
   - 4단계. 도메인 이름: sgdemo
   - 10단계. 세분화된 액세스 제어: 세분화된 액세스 제어 사용 옵션을 선택 취소합니다.
   - 12단계. 액세스 정책: 레벨 액세스 정책 구성을 선택하고 JSON 탭을 선택하여 다음 예를 사용하여 액세스 정책을 수정합니다.
     - 강조 표시된 텍스트를 사용자 고유의 AWS ID 및 액세스 관리(IAM) ID 및 사용자 이름으로 바꿉니다.
     - 강조 표시된 텍스트(IP 주소)를 AWS 콘솔에 액세스하는 데 사용한 로컬 컴퓨터의 공용 IP 주소로 바꿉니다.
     - 브라우저 탭을 에 엽니다 "https://checkip.amazonaws.com" 공용 IP를 찾습니다.

```
{

    "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/*"
        }
    ]
}
```

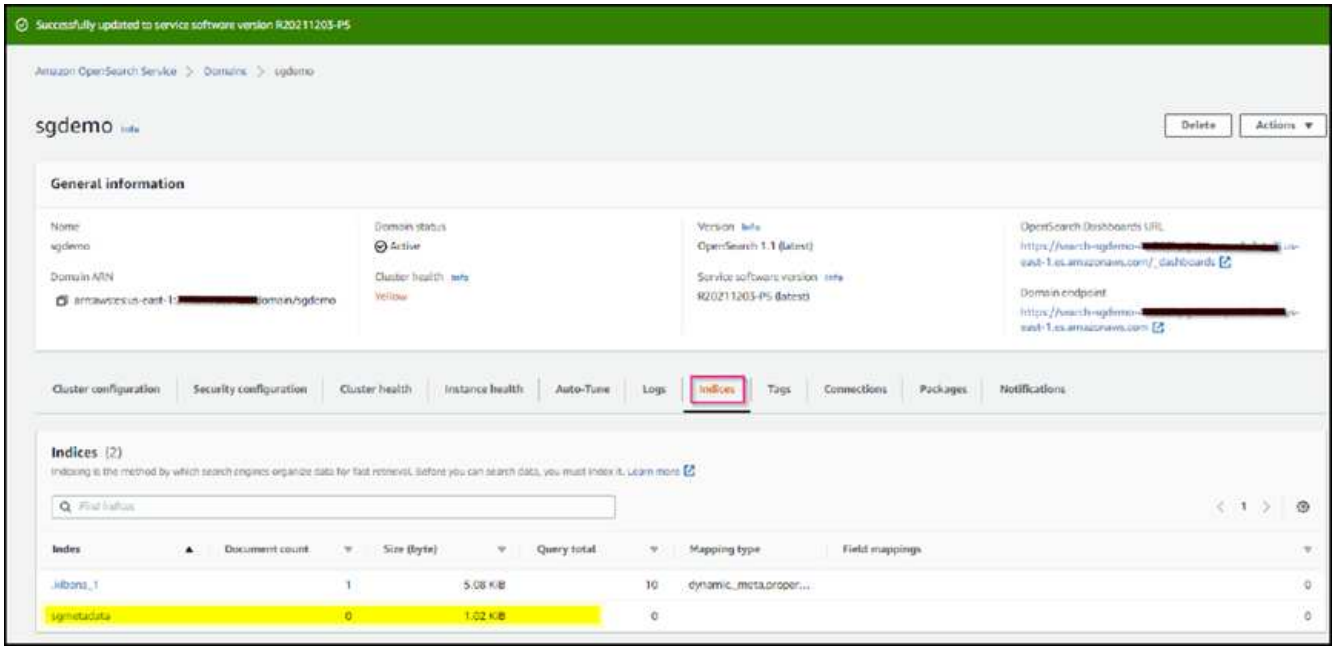

Fine-grained access control
Fine-grained access control provides numerous features to help you keep your data secure. Features include document-level security, field-level security, read-only users, and OpenSearch Dashboards/Kibana tenants. Fine-grained access control requires a master user. Learn more
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. 도메인이 활성화될 때까지 15-20분 정도 기다립니다.

3. OpenSearch Dashboards URL 을 클릭하여 새 탭에서 도메인을 열고 대시보드에 액세스합니다. 액세스 거부 오류가 발생하면 도메인 대시보드에 액세스할 수 있도록 액세스 정책 원본 IP 주소가 컴퓨터 공용 IP로 올바르게 설정되어 있는지 확인합니다.
4. 대시보드 시작 페이지에서 직접 탐색 을 선택합니다. 메뉴에서 관리 → 개발 도구 로 이동합니다
5. 개발 도구 → 콘솔에서 StorageGRID 개체 메타데이터를 저장하기 위해 인덱스를 사용하는 'Put <index>'를 입력합니다. 다음 예에서는 인덱스 이름 'gmetadata'를 사용합니다. 작은 삼각형 기호를 클릭하여 PUT 명령을 실행합니다. 다음 예제 스크린샷과 같이 오른쪽 패널에 예상 결과가 표시됩니다.



6. 색인이 sgdomain > Indices 아래의 Amazon OpenSearch UI에서 표시되는지 확인합니다.

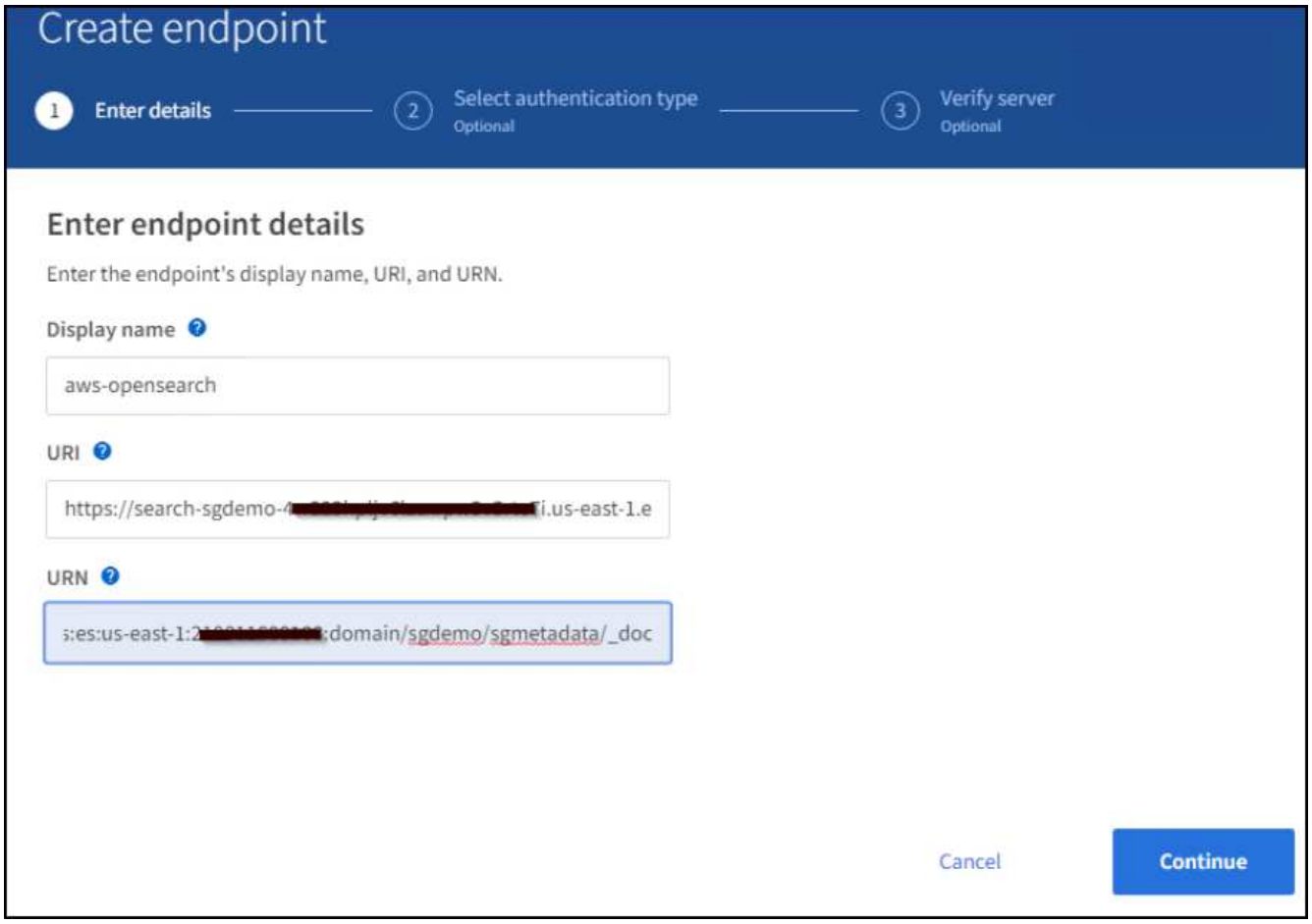


플랫폼 서비스 엔드포인트 구성

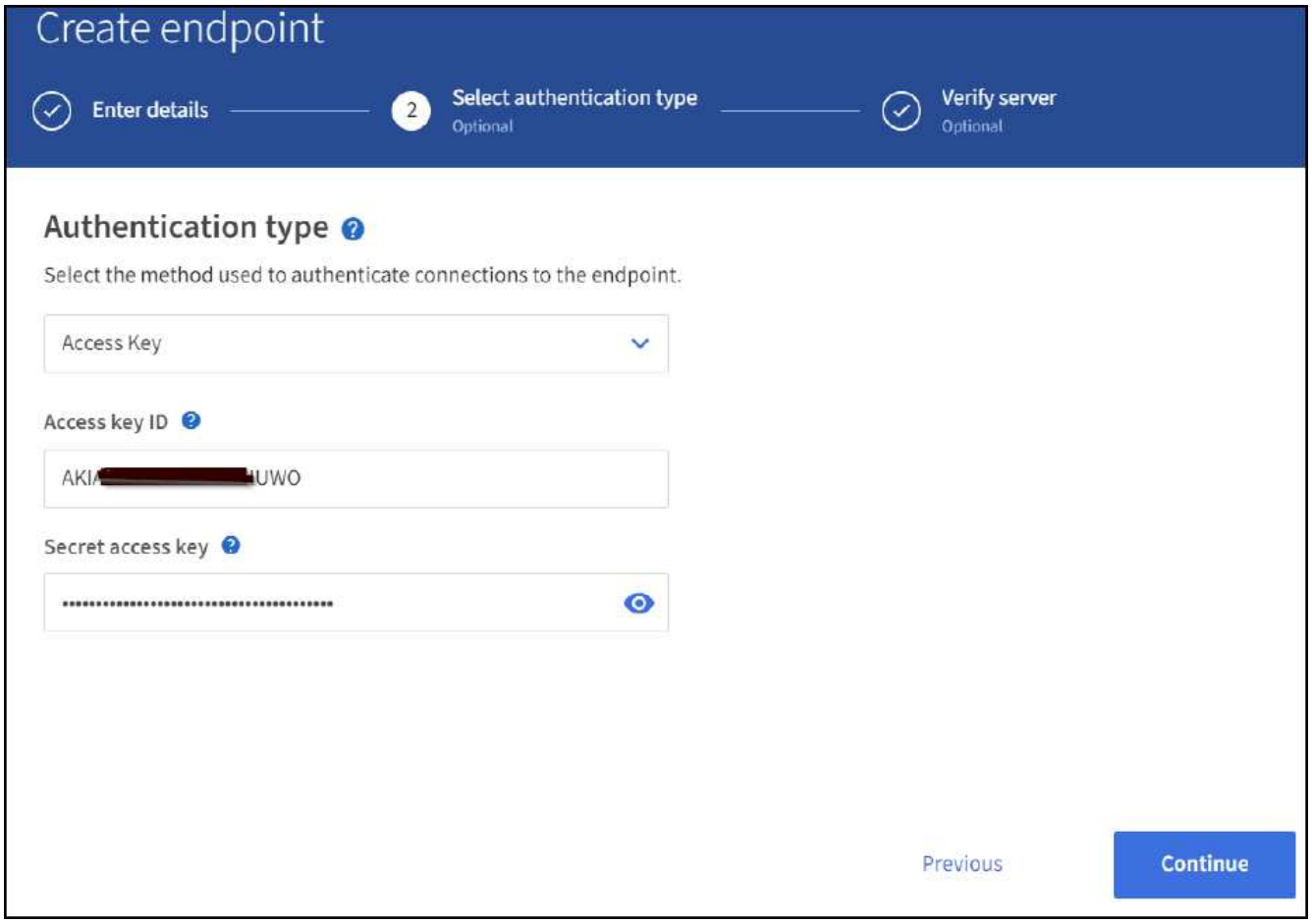
플랫폼 서비스 끝점을 구성하려면 다음 단계를 수행하십시오.

1. 테넌트 관리자 에서 스토리지(S3) > 플랫폼 서비스 엔드포인트 로 이동합니다.
2. 끝점 만들기 를 클릭하고 다음을 입력한 다음 계속 을 클릭합니다.
   - 표시 이름 예 AWS-OpenSearch
   - 예제 스크린샷의 도메인 끝점은 URI 필드의 이전 절차의 2단계 아래에 있습니다.
   - URN 필드의 이전 절차 2단계에서 사용한 ARN 도메인을 ARN의 끝에 추가하는 /<index>/_doc'를 추가한다.

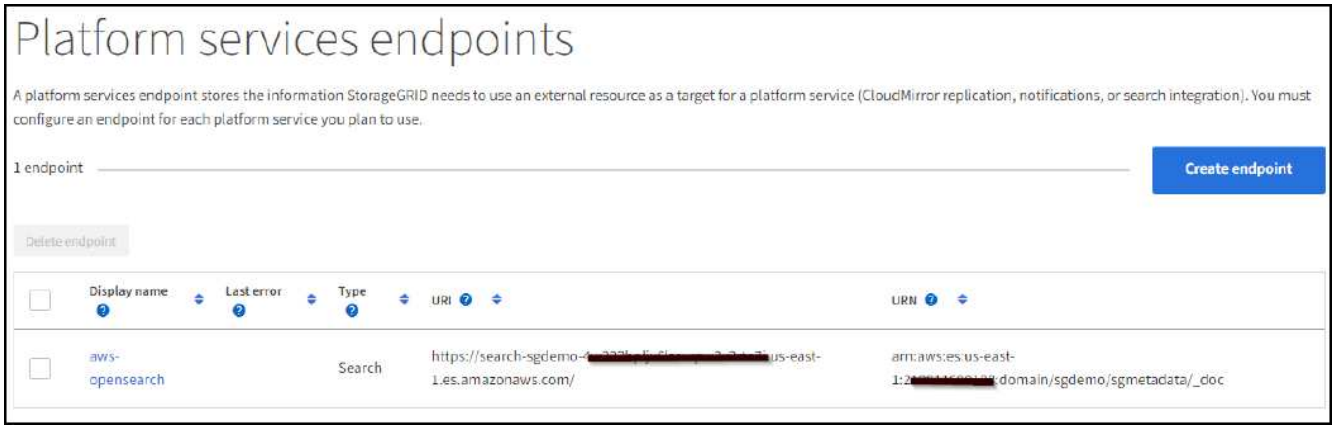
     이 예에서 URN은 'arn:aws:es:us-east-1:211234567890:domain/sgdemo/sgmedata/_doc'가 됩니다.



3. Amazon OpenSearch sgdomain에 액세스하려면 인증 유형으로 Access Key를 선택한 다음 Amazon S3 액세스 키와 암호 키를 입력합니다. 다음 페이지로 이동하려면 계속 을 클릭합니다.



4. 끝점을 확인하려면 운영 체제 CA 인증서 사용 및 끝점 테스트 및 만들기 를 선택합니다. 확인이 성공하면 다음 그림과 유사한 엔드포인트 화면이 표시됩니다. 확인이 실패하면 경로 끝에 URN에 "/<index>/_doc"가 포함되어 있고 AWS 액세스 키와 비밀 키가 올바른지 확인합니다.



온-프레미스 **Elasticsearch**와 통합 서비스를 검색합니다

온-프레미스 **Elasticsearch** 설정

이 절차는 테스트 목적으로만 Docker를 사용하여 사내 Elasticsearch 및 Kibana를 빠르게 설정하기 위한 것입니다. Elasticsearch 및 Kibana 서버가 이미 있는 경우 5단계로 이동합니다.

1. 다음 단계를 따르십시오 "Docker 설치 절차" Docker를 설치합니다. 을 사용합니다 "CentOS Docker 설치 절차" 를

클릭합니다.

```
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
```

- 재부팅 후 Docker를 시작하려면 다음을 입력합니다.

```
sudo systemctl enable docker
```

- VM.max_map_count 값을 262144로 설정한다.

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

- 재부팅 후 설정을 유지하려면 다음을 입력합니다.

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

2. 를 따릅니다 "Elasticsearch 빠른 시작 가이드" Elasticsearch 및 Kibana Docker를 설치하고 실행하기 위한 자가 관리 섹션입니다. 이 예에서는 버전 8.1을 설치했습니다.

참고 Elasticsearch에서 만든 사용자 이름/암호 및 토큰을 아래로 하여 Kibana UI 및 StorageGRID 플랫폼 엔드포인트 인증을 시작해야 합니다.

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.

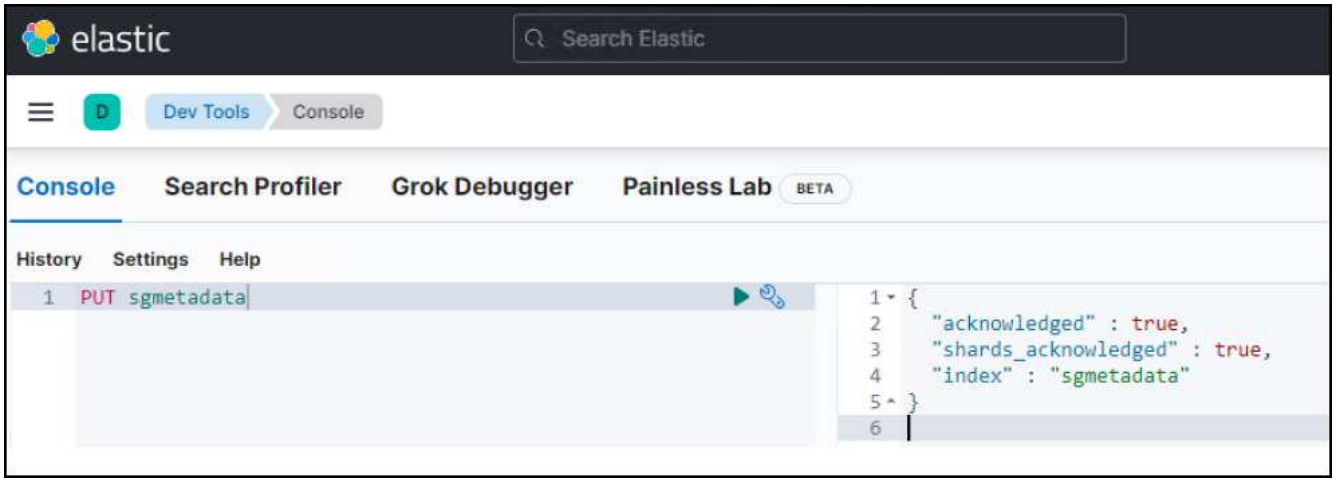
1. In a new terminal session, run:

```
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.

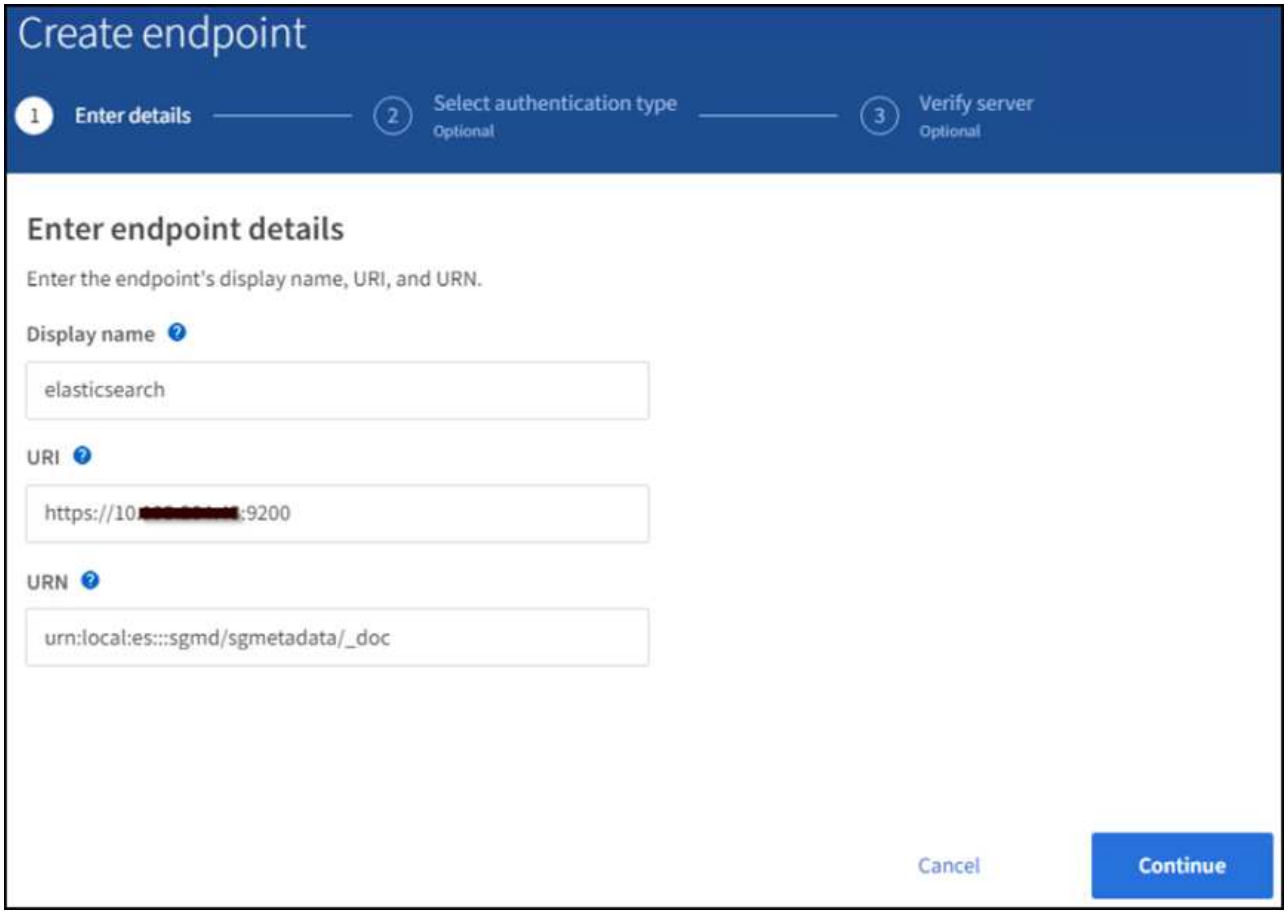
3. Kibana Docker 컨테이너가 시작되면 URL 링크 'https://0.0.0.0:5601` 가 콘솔에 표시됩니다. 0.0.0.0을 URL의 서버 IP 주소로 바꿉니다.
4. 사용자 이름 탄력성과 이전 단계에서 Elastic에 의해 생성된 암호를 사용하여 Kibana UI에 로그인합니다.
5. 처음 로그인하는 경우 대시보드 시작 페이지에서 직접 탐색 을 선택합니다. 메뉴에서 관리 > 개발 도구 를 선택합니다.
6. 개발 도구 콘솔 화면에서 StorageGRID 개체 메타데이터를 저장하기 위해 이 인덱스를 사용하는 "Put <index>"를 입력합니다. 이 예에서는 인덱스 이름 'gmetadata'를 사용합니다. 작은 삼각형 기호를 클릭하여 PUT 명령을 실행합니다. 다음 예제 스크린샷과 같이 오른쪽 패널에 예상 결과가 표시됩니다.



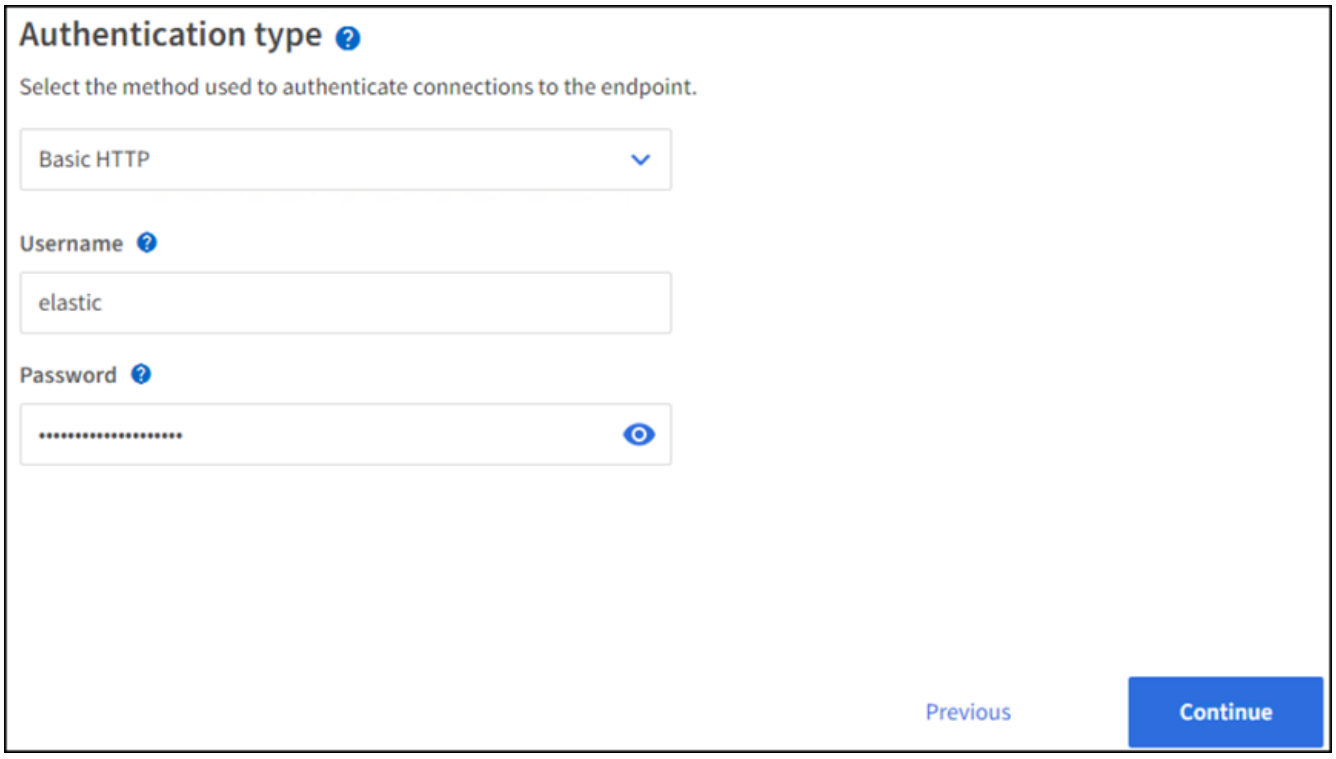
플랫폼 서비스 엔드포인트 구성

플랫폼 서비스에 대한 끝점을 구성하려면 다음 단계를 수행하십시오.

1. 테넌트 관리자에서 스토리지(S3) > 플랫폼 서비스 엔드포인트로 이동합니다
2. 끝점 만들기 를 클릭하고 다음을 입력한 다음 계속 을 클릭합니다.
   - 이름 표시 예: 탄력적인 검색
   - Uri:'https://<elasticsearch-server-ip or hostname>:9200'입니다
   - urn:'urn:<something>:es:::<some-unique-text>/<index-name>/_doc' 여기서 index-name은 Kibana 콘솔에서 사용한 이름입니다. 예: 'urn:local:es::::sgmd/sgmetadata/_doc'

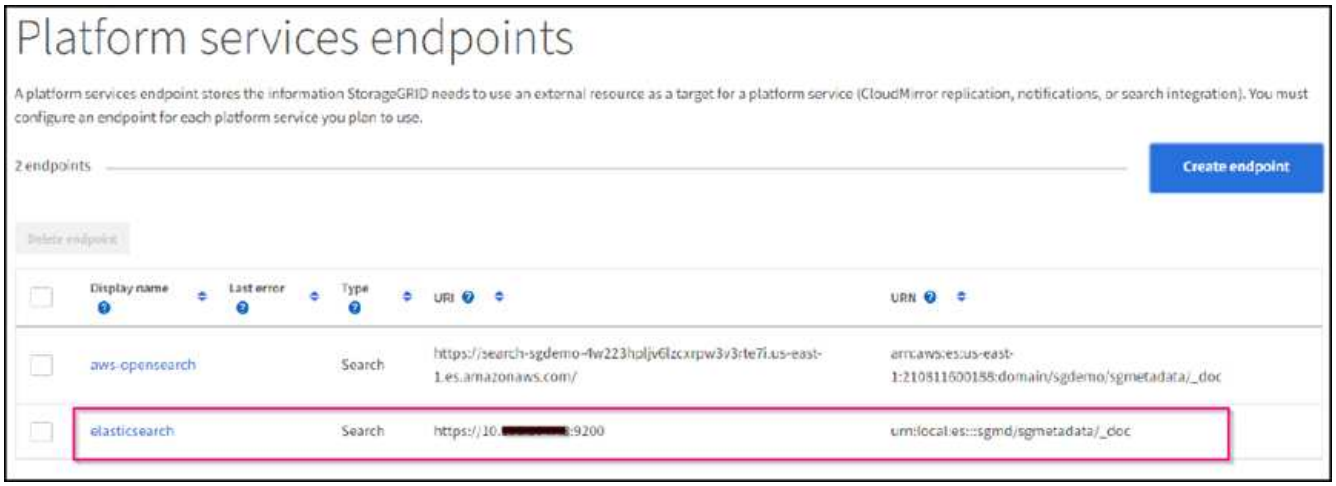


3. 인증 유형으로 기본 HTTP 를 선택하고 Elasticsearch 설치 프로세스에서 생성된 사용자 이름 'elastic'과 암호를 입력합니다. 다음 페이지로 이동하려면 계속 을 클릭합니다.



4. 인증서 확인 안 함 및 테스트 및 끝점 만들기 를 선택하여 끝점을 확인합니다. 확인이 성공하면 다음 스크린샷과

유사한 엔드포인트 화면이 표시됩니다. 확인에 실패하면 URN, URI 및 사용자 이름/암호 항목이 올바른지 확인합니다.



버킷 검색 통합 서비스 구성

플랫폼 서비스 끝점을 만든 후 다음 단계는 개체가 생성, 삭제 또는 해당 메타데이터 또는 태그가 업데이트될 때마다 개체 메타데이터를 정의된 끝점으로 보내도록 버킷 수준에서 이 서비스를 구성하는 것입니다.

다음과 같이 테넌트 관리자를 사용하여 사용자 지정 StorageGRID 구성 XML을 버킷에 적용하여 검색 통합을 구성할 수 있습니다.

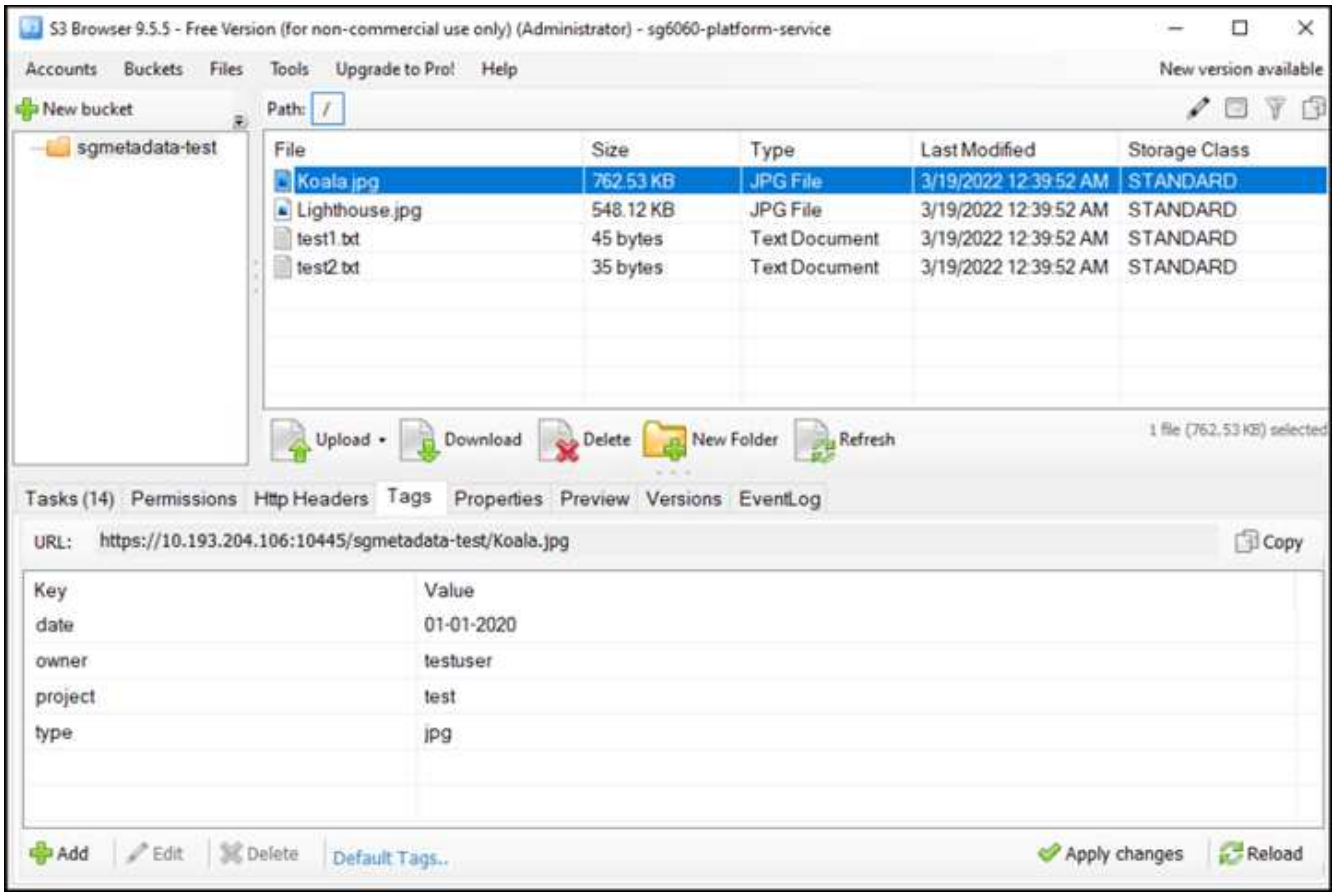
1. 테넌트 관리자 에서 스토리지(S3) > 버킷 으로 이동합니다
2. Create Bucket을 클릭하고 bucket 이름(예: 'gmetadata-test')을 입력한 후 기본 us-east-1 영역을 그대로 사용합니다.
3. 계속 > 버킷 생성 을 클릭합니다.
4. 버킷 개요 페이지를 표시하려면 버킷 이름을 클릭한 다음 플랫폼 서비스를 선택합니다.
5. 검색 통합 활성화 대화 상자를 선택합니다. 제공된 XML 상자에 이 구문을 사용하여 구성 XML을 입력합니다.

   강조 표시된 URN은 사용자가 정의한 플랫폼 서비스 끝점과 일치해야 합니다. 다른 브라우저 탭을 열어 테넌트 관리자에 액세스하고 정의된 플랫폼 서비스 끝점에서 URN을 복사할 수 있습니다.

   이 예에서는 접두어를 사용하지 않았습니다. 즉, 이 버킷의 모든 객체에 대한 메타데이터가 이전에 정의된 Elasticsearch 끝점으로 전송됩니다.

```
<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 브라우저를 사용하여 테넌트 액세스/암호 키를 사용하여 StorageGRID에 연결하고, 테스트 객체를 '메타데이터 테스트' 버킷에 업로드하고, 태그나 사용자 지정 메타데이터를 객체에 추가합니다.



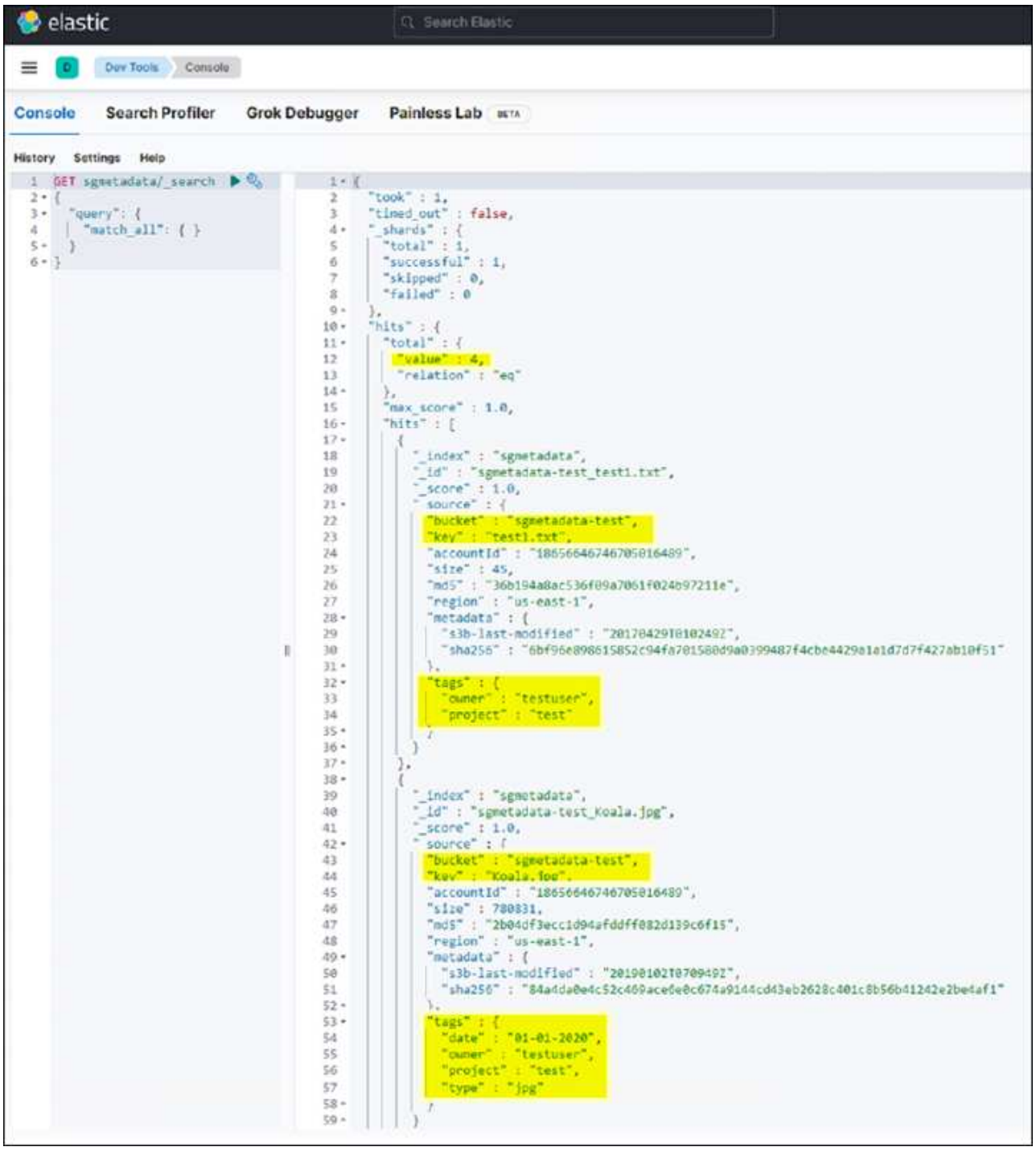
7. Kibana UI를 사용하여 오브젝트 메타데이터가 sgmetadata의 인덱스에 로드되었는지 확인합니다.

   a. 메뉴에서 관리 > 개발 도구 를 선택합니다.

   b. 왼쪽의 콘솔 패널에 샘플 쿼리를 붙여넣고 삼각형 기호를 클릭하여 실행합니다.

      다음 예제 스크린샷의 쿼리 1 예제 결과는 네 개의 레코드를 보여 줍니다. 이는 버킷의 오브젝트 수와 일치합니다.

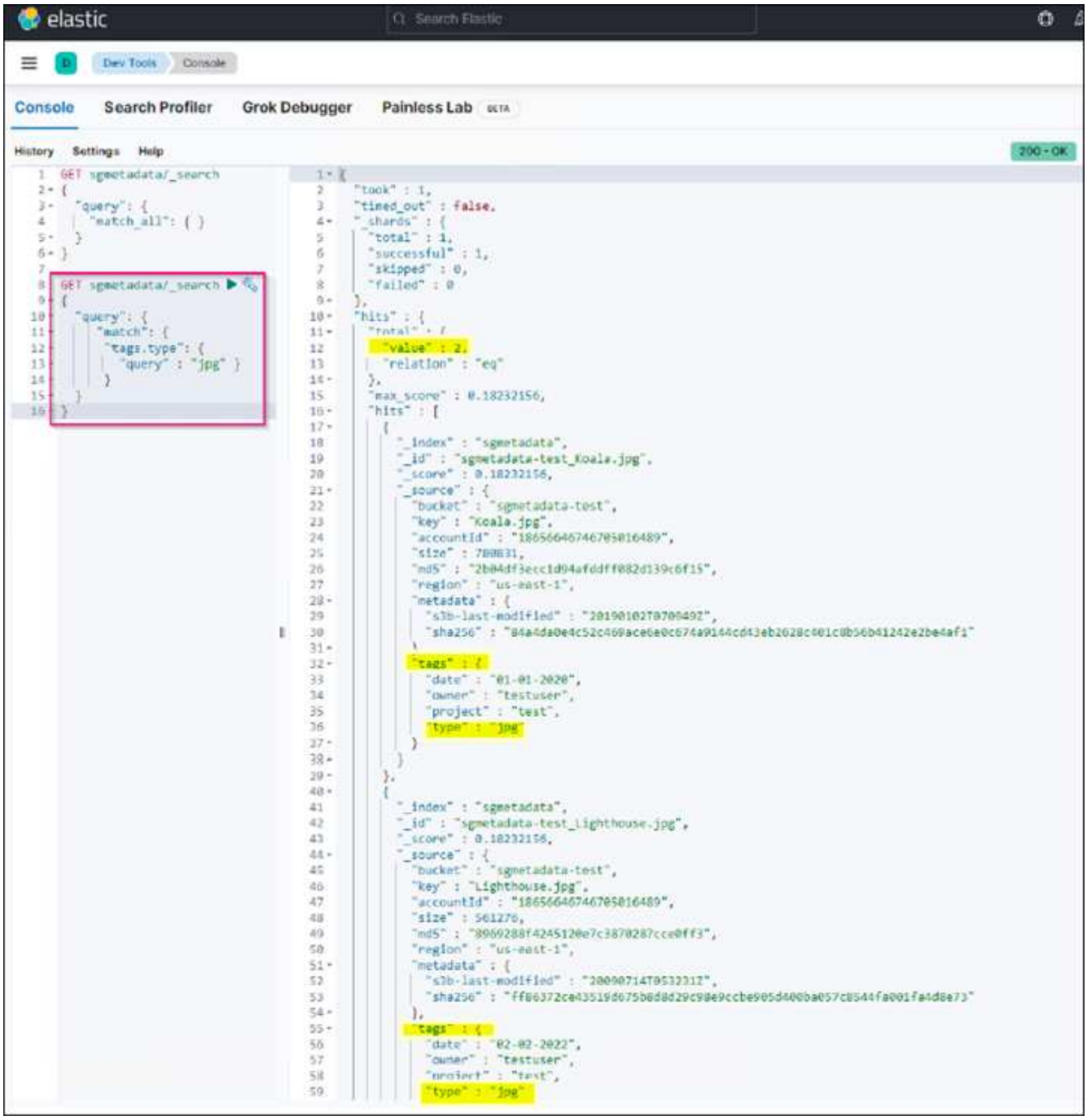
```
GET sgmetadata/_search
{
    "query": {
        "match_all": { }
}
}
```



다음 스크린샷의 쿼리 2 샘플 결과는 태그 유형 jpg의 두 레코드를 보여 줍니다.

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

+



추가 정보를 찾을 수 있는 위치

이 문서에 설명된 정보에 대해 자세히 알아보려면 다음 문서 및/또는 웹 사이트를 검토하십시오.

- "플랫폼 서비스란 무엇입니까"
- "StorageGRID 11.6 문서"

안젤라 청 _ 에 의해

노드 클론

노드 클론 고려 사항 및 성능

노드 클론 고려 사항

노드 클론은 기술 업데이트, 용량 증가 또는 StorageGRID 시스템 성능 향상을 위해 기존 어플라이언스 노드를 빠르게 교체할 수 있는 방법이 될 수 있습니다. 노드 클론은 KMS를 사용하여 노드 암호화로 변환하거나 스토리지 노드를 DDP8에서 DDP16으로 변경하는 경우에도 유용합니다.

- 소스 노드의 사용된 용량은 클론 프로세스를 완료하는 데 필요한 시간과 관련이 없습니다. 노드 클론은 노드의 여유 공간을 포함하는 노드의 전체 복사본입니다.
- 소스 및 대상 장비는 동일한 PGE 버전이어야 합니다
- 대상 노드의 용량은 항상 소스보다 커야 합니다
  - 새 대상 어플라이언스의 드라이브 크기가 소스보다 큰지 확인하십시오
  - 대상 어플라이언스의 크기가 동일한 드라이브가 DDP8에 대해 구성된 경우 DDP16의 대상을 구성할 수 있습니다. 소스가 DDP16에 대해 이미 구성되어 있으면 노드 클론을 사용할 수 없습니다.
  - SG5660 또는 SG5760 어플라이언스에서 SG6060 어플라이언스로 이동하는 경우 SG5x60은 60개의 대용량 드라이브를 지원하며 SG6060은 58만 지원합니다.
- 노드 클론 프로세스를 수행하려면 클론 생성 프로세스 동안 소스 노드가 그리드에 대해 오프라인 상태여야 합니다. 이 시간 동안 추가 노드가 오프라인이 되면 클라이언트 서비스에 영향을 줄 수 있습니다.
- 스토리지 노드는 15일 동안만 오프라인 상태가 될 수 있습니다. 복제 프로세스 추정치가 15일에 가깝거나 15일을 초과할 경우 확장 및 서비스 해제 절차를 사용하십시오.
- 확장 쉘프가 있는 SG6060의 경우, 전체 클론 기간을 가져오려면 기본 어플라이언스 시간의 시간에 올바른 쉘프 드라이브 크기에 대한 시간을 추가해야 합니다.

노드 클론 성능 추정치

다음 표에는 노드 클론 기간에 대해 계산된 추정치가 나와 있습니다. 조건이 다양하므로 * BOLD * 의 항목은 노드 다운에 대해 15일 제한을 초과할 위험이 있습니다.

DDP8

SG5612 → 임의

네트워크 인터페이스 속도	**4TB** 드라이브 크기	**8TB** 드라이브 크기	**10TB** 드라이브 크기	**12TB** 드라이브 크기	**16TB** 드라이브 크기	**18TB** 드라이브 크기
10GB	1일	2일	2.5일	3일	4일	4.5일
25GB	1일	2일	2.5일	3일	4일	4.5일

SG5712 → 임의

네트워크 인터페이스 속도	**4TB** 드라이브 크기	**8TB** 드라이브 크기	**10TB** 드라이브 크기	**12TB** 드라이브 크기	**16TB** 드라이브 크기	**18TB** 드라이브 크기
10GB	1일	2일	2.5일	3일	4일	4.5일
25GB	1일	2일	2.5일	3일	4일	4.5일

SG5660 → **SG5760**

네트워크 인터페이스 속도	**4TB** 드라이브 크기	**8TB** 드라이브 크기	**10TB** 드라이브 크기	**12TB** 드라이브 크기	**16TB** 드라이브 크기	**18TB** 드라이브 크기
10GB	3일	6일	7일	8.5일	11.5일	• 13일 *
25GB	3일	6일	7일	8.5일	11.5일	• 13일 *

SG5660 → **SG6060**

네트워크 인터페이스 속도	**4TB** 드라이브 크기	**8TB** 드라이브 크기	**10TB** 드라이브 크기	**12TB** 드라이브 크기	**16TB** 드라이브 크기	**18TB** 드라이브 크기
10GB	2.5일	4.5일	5.5일	6.5일	9일	10일
25GB	2일	4일	5일	6일	8일	9일

SG5760 → **SG5760**

네트워크 인터페이스 속도	**4TB** 드라이브 크기	**8TB** 드라이브 크기	**10TB** 드라이브 크기	**12TB** 드라이브 크기	**16TB** 드라이브 크기	**18TB** 드라이브 크기
10GB	3일	6일	7일	8.5일	11.5일	• 13일 *
25GB	3일	6일	7일	8.5일	11.5일	• 13일 *

SG5760 → SG6060

네트워크 인터페이스 속도	**4TB** 드라이브 크기	**8TB** 드라이브 크기	**10TB** 드라이브 크기	**12TB** 드라이브 크기	**16TB** 드라이브 크기	**18TB** 드라이브 크기
10GB	2.5일	4.5일	5.5일	6.5일	9일	10일
25GB	1.5일	3일	3.5일	4.5일	6일	6.5일

SG6060 → SG6060

네트워크 인터페이스 속도	**4TB** 드라이브 크기	**8TB** 드라이브 크기	**10TB** 드라이브 크기	**12TB** 드라이브 크기	**16TB** 드라이브 크기	**18TB** 드라이브 크기
10GB	2.5일	4.5일	5.5일	6.5일	8.5일	9.5일
25GB	1.5일	3일	3.5일	4일	5.5일	6일

DDP16을 참조하십시오

SG5760 → SG5760

네트워크 인터페이스 속도	**4TB** 드라이브 크기	**8TB** 드라이브 크기	**10TB** 드라이브 크기	**12TB** 드라이브 크기	**16TB** 드라이브 크기	**18TB** 드라이브 크기
10GB	3.5일	6.5일	8일	9.5일	12.5일	• 14일 *
25GB	3.5일	6.5일	8일	9.5일	12.5일	• 14일 *

SG5760 → SG6060

네트워크 인터페이스 속도	**4TB** 드라이브 크기	**8TB** 드라이브 크기	**10TB** 드라이브 크기	**12TB** 드라이브 크기	**16TB** 드라이브 크기	**18TB** 드라이브 크기
10GB	2.5일	5일	6일	7.5일	10일	11일
25GB	2일	3.5일	4일	5일	6.5일	7일

SG6060 → SG6060

네트워크 인터페이스 속도	**4TB** 드라이브 크기	**8TB** 드라이브 크기	**10TB** 드라이브 크기	**12TB** 드라이브 크기	**16TB** 드라이브 크기	**18TB** 드라이브 크기
10GB	3.5일	5일	6일	7일	9.5일	10.5일

네트워크 인터페이스 속도	**4TB** 드라이브 크기	**8TB** 드라이브 크기	**10TB** 드라이브 크기	**12TB** 드라이브 크기	**16TB** 드라이브 크기	**18TB** 드라이브 크기
25GB	2일	3일	4일	4.5일	6일	7일

확장 쉘프(소스 어플라이언스의 각 쉘프에 대해 **SG6060** 위에 추가)

네트워크 인터페이스 속도	**4TB** 드라이브 크기	**8TB** 드라이브 크기	**10TB** 드라이브 크기	**12TB** 드라이브 크기	**16TB** 드라이브 크기	**18TB** 드라이브 크기
10GB	3.5일	5일	6일	7일	9.5일	10.5일
25GB	2일	3일	4일	4.5일	6일	7일

_ 아론 클라인 _

포트 재매핑 사용 방법

여러 가지 이유로 인해 수신 포트 또는 아웃바운드 포트를 다시 매핑해야 할 수 있습니다. 레거시 CLB 로드 밸런서 서비스에서 현재 nginx 서비스 로드 밸런서 끝점으로 이동하고 동일한 포트를 유지하여 클라이언트에 대한 영향을 줄이거나, 관리 노드 클라이언트 네트워크에서 클라이언트 S3에 포트 443을 사용하거나, 방화벽 제한 사항에 대해 사용할 수 있습니다.

포트 재맵을 사용하여 **CLB**에서 **NGINX**로 **S3** 클라이언트를 마이그레이션합니다

StorageGRID 11.3 이전의 릴리스에서는 게이트웨이 노드에 포함된 로드 밸런서 서비스가 CLB(연결 로드 밸런서)입니다. StorageGRID 11.3에서 NetApp은 HTTP(s) 트래픽 로드 밸런싱을 위한 기능이 풍부한 통합 솔루션으로 NGINX 서비스를 도입했습니다. CLB 서비스는 StorageGRID의 현재 릴리스에서 계속 사용할 수 있으므로 새 로드 밸런서 엔드포인트 구성에서 포트 8082를 다시 사용할 수 없습니다. 이 문제를 해결하려면 8082 인바운드 포트를 10443으로 다시 매핑합니다. 이렇게 하면 게이트웨이 리디렉션의 포트 8082에 들어오는 모든 HTTPS 요청이 포트 10443으로 리디렉션되고 CLB 서비스를 우회하여 NGINX 서비스에 연결됩니다. 다음 지침은 VMware에 대한 지침이지만 port_remap 기능은 모든 설치 방법을 사용하며 베어 메탈 배포 및 어플라이언스에 유사한 프로세스를 사용할 수 있습니다.

VMware 가상 머신 게이트웨이 노드 구축

다음 단계는 StorageGRID OVF(Open Virtualization Format)를 사용하여 VMware vSphere 7에서 VM으로 게이트웨이 노드를 구축하는 StorageGRID 구축 단계입니다. 이 프로세스에서는 VM을 소멸적으로 제거하고 동일한 이름 및 구성으로 VM을 다시 배포해야 합니다. VM의 전원을 켜기 전에 vApp 속성을 변경하여 포트를 다시 매핑한 다음 VM의 전원을 켜고 노드 복구 프로세스를 따르십시오.

필수 구성 요소

- StorageGRID 11.3 이상을 실행하고 있습니다
- 설치된 StorageGRID 버전 VMware 설치 파일을 다운로드하여 액세스할 수 있습니다.
- VM의 전원을 켜거나 끄고, VM 및 vApp의 설정을 변경하고, vCenter에서 VM을 제거하고, OVF로 VM을 구축할 수

있는 권한이 있는 vCenter 계정이 있습니다.

- 로드 밸런서 끝점을 만들었습니다
  - 포트가 원하는 리디렉션 포트로 구성되어 있습니다
  - 엔드포인트 SSL 인증서는 Configuration/Server Certificates/Object Storage API Service Endpoints Server Certificate의 CLB 서비스에 설치된 것과 동일하며, 그렇지 않은 경우 클라이언트는 인증서 변경을 수락할 수 있습니다.

> 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.

첫 번째 게이트웨이 노드를 제거합니다

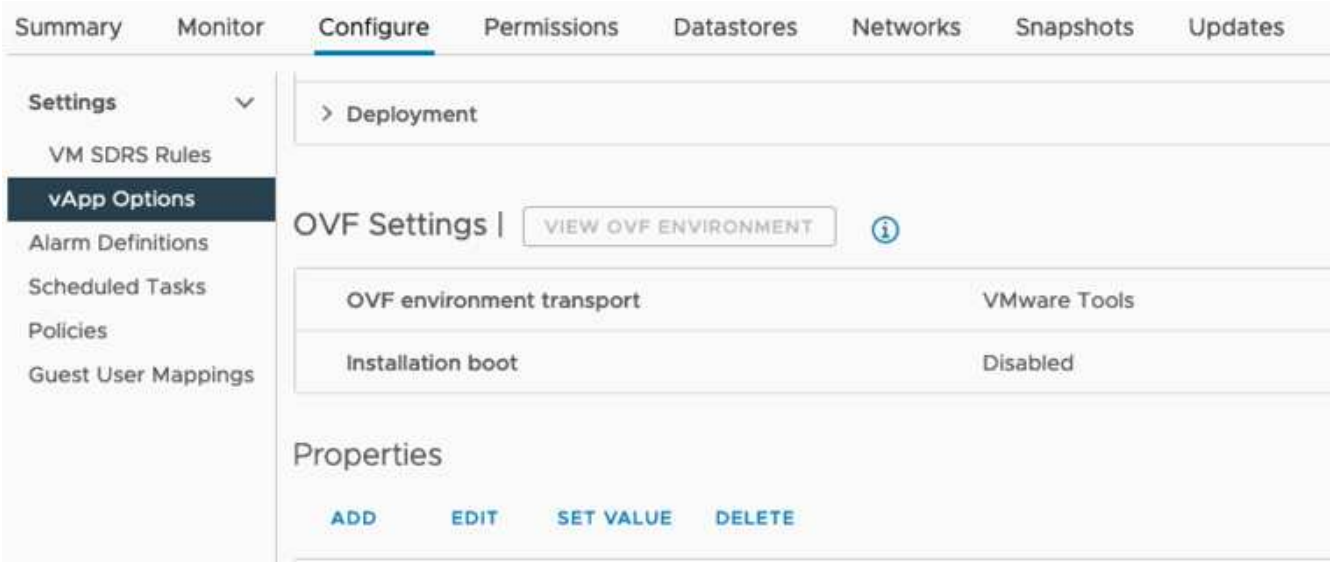
첫 번째 게이트웨이 노드를 제거하려면 다음 단계를 수행하십시오.

1. 그리드에 둘 이상의 노드가 있는 경우 시작할 게이트웨이 노드를 선택합니다.
2. 해당되는 경우 모든 DNS 라운드 로빈 엔터티 또는 로드 밸런서 풀에서 노드 IP를 제거합니다.
3. TTL(Time-to-Live)과 열려 있는 세션이 만료될 때까지 기다립니다.
4. VM 노드의 전원을 끕니다.
5. 디스크에서 VM 노드를 제거합니다.

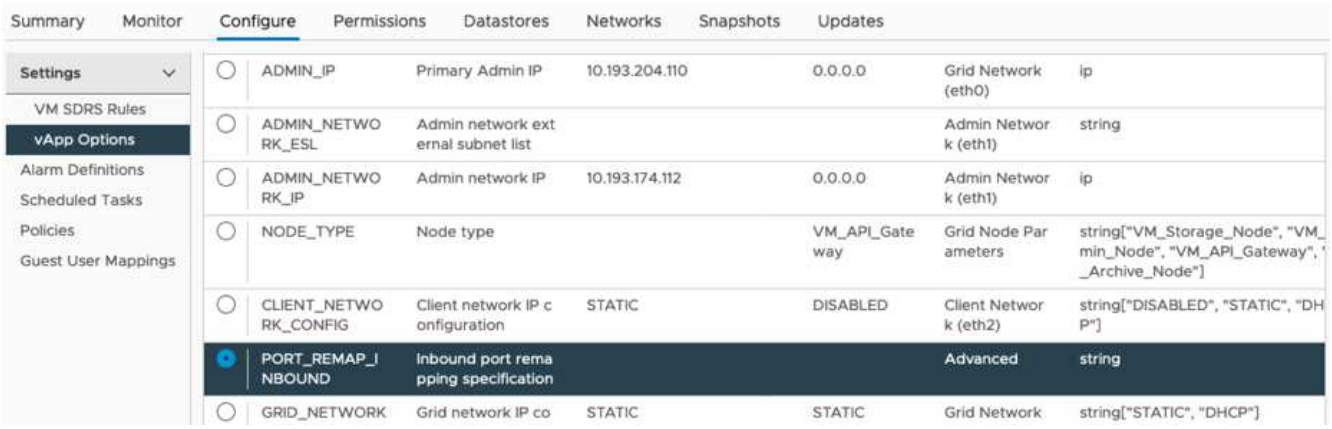
교체용 게이트웨이 노드를 배포합니다

교체 게이트웨이 노드를 배포하려면 다음 단계를 수행하십시오.

1. OVF에서 새 VM을 구축하고 지원 사이트에서 다운로드한 설치 패키지에서 .ovf, .mf 및 .vmdk 파일을 선택합니다.
   - vsphere - gateway.mf
   - vsphere - gateway.ovf
   - NetApp-SG-11.4.0-20200721.1338.d3969b3.vmdk
2. VM이 구축된 후 VM 목록에서 해당 VM을 선택하고 Configure 탭 vApp Options를 선택합니다.



3. 속성 섹션으로 스크롤하고 port_remap_inbound 속성을 선택합니다

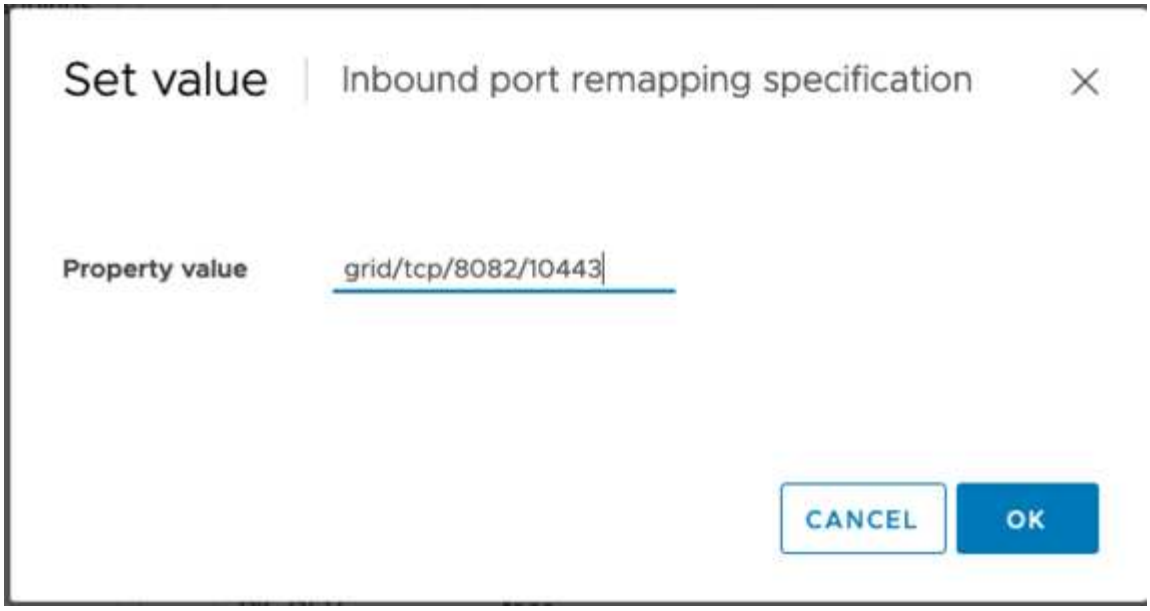


4. 속성 목록 맨 위로 스크롤하여 편집 을 클릭합니다

5. 유형 탭을 선택하고 사용자 구성 가능 확인란이 선택되어 있는지 확인한 다음 저장을 클릭합니다.

6. 속성 목록 상단에서 "port_remap_inbound" 속성을 선택한 상태에서 값 설정 을 클릭합니다.

7. 속성 값 필드에 네트워크(그리드, 관리자 또는 클라이언트), TCP, 원래 포트(8082) 및 새 포트(10443)를 입력합니다(아래 그림에 표시된 대로 각 값 사이에 “/”가 있음).

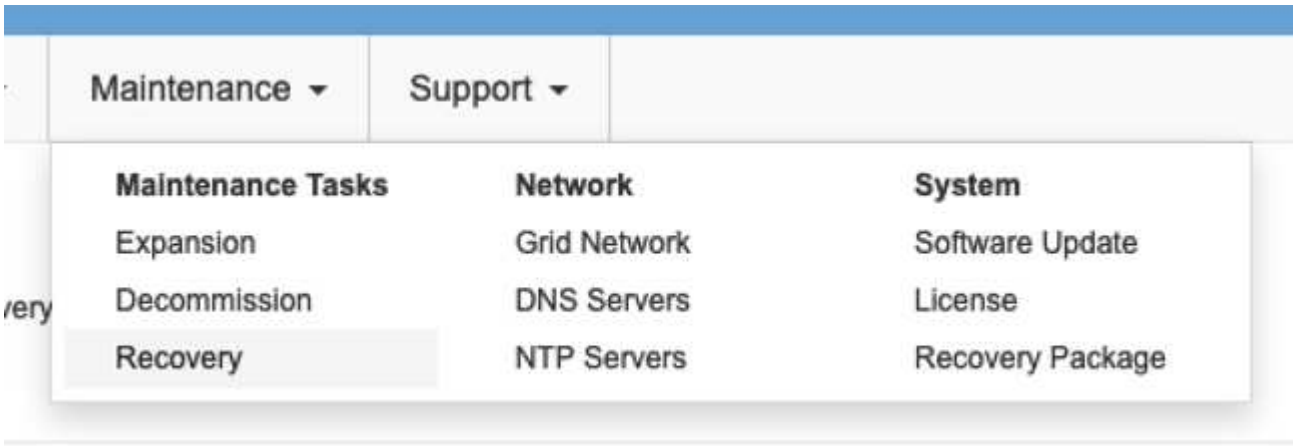


8. 여러 네트워크를 사용하는 경우 네트워크 문자열을 구분하려면 쉼표(,)를 사용합니다(예: GRID/TCP/8082/10443, admin/TCP/8082/10443, client/TCP/8082/10443)

게이트웨이 노드를 복구합니다

게이트웨이 노드를 복구하려면 다음 단계를 수행하십시오.

1. Grid Management UI의 Maintenance/Recovery 섹션으로 이동합니다.



2. VM 노드의 전원을 켜고 Grid Management UI의 Maintenance/Recovery Pending Nodes 섹션에 노드가 나타날 때까지 기다립니다.

> 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. 노드가 복구된 후에는 해당하는 경우 모든 DNS 라운드 로빈 엔터티 또는 로드 밸런서 풀에 IP를 포함할 수 있습니다.

   이제 포트 8082의 모든 HTTPS 세션이 포트 10443으로 이동합니다

관리 노드에서 클라이언트 **S3** 액세스를 위한 포트 **443**을 다시 매핑합니다

관리 노드 또는 관리 노드가 포함된 HA 그룹에 대한 StorageGRID 시스템의 기본 구성은 포트 443 및 80을 관리 및 테넌트 관리자 UI용으로 예약하기 위한 것이며 로드 밸런서 끝점에 사용할 수 없습니다. 이에 대한 해결 방법은 포트 재매핑 기능을 사용하고 인바운드 포트 443을 로드 밸런서 끝점으로 구성할 새 포트로 리디렉션하는 것입니다. 이 작업이 완료되면 클라이언트 S3 트래픽에서 포트 443을 사용할 수 있고, 그리드 관리 UI는 포트 8443을 통해서만 액세스할 수 있으며, 테넌트 관리 UI는 포트 9443에서만 액세스할 수 있습니다. 재매핑 포트 기능은 노드 설치 시에만 구성할 수 있습니다. 활성 노드의 포트 재맵을 그리드에서 구현하려면 미리 설치된 상태로 재설정해야 합니다. 이 작업은 구성을 변경한 후 노드 복구를 포함하는 제거 절차입니다.

백업 로그 및 데이터베이스

관리 노드에는 속성, 경보 및 경고에 대한 내역 정보뿐만 아니라 감사 로그, Prometheus 메트릭이 포함됩니다. admin 노드가 여러 개인 경우 이 데이터의 복사본이 여러 개 있습니다. 그리드에 admin 노드가 여러 개 없는 경우, 이 프로세스가 끝날 때 노드를 복구한 후에 이 데이터를 보존하여 복원해야 합니다. 그리드에 다른 관리 노드가 있는 경우 복구 프로세스 중에 해당 노드의 데이터를 복사할 수 있습니다. 그리드에 다른 관리 노드가 없는 경우 노드를 삭제하기 전에 다음 지침에 따라 데이터를 복사할 수 있습니다.

감사 로그를 복사합니다

1. 관리자 노드에 로그인합니다.
   a. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`
   b. 에 나열된 암호를 입력합니다 `Passwords.txt` 파일.
   c. 루트로 전환하려면 다음 명령을 입력합니다. `su -`
   d. 에 나열된 암호를 입력합니다 `Passwords.txt` 파일.
   e. SSH 에이전트에 SSH 개인 키를 추가합니다. 입력: `ssh-add`

f. 에 나열된 SSH 액세스 암호를 입력합니다 `Passwords.txt` 파일.

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

2. 디렉토리를 생성하여 모든 감사 로그 파일을 별도의 그리드 노드의 임시 위치에 복사합니다. use_storage_node_01_:
   a. `ssh admin@storage_node_01_IP`
   b. `mkdir -p /var/local/tmp/saved-audit-logs`
3. 관리 노드로 돌아가서 AMS 서비스를 중지하여 새 로그 파일을 생성하지 않도록 합니다. `service ams stop`
4. audit.log 파일을 복구된 관리 노드에 복사할 때 기존 파일을 덮어쓰지 않도록 파일 이름을 바꿉니다.
   a. audit.log 이름을 yyyy-mm-dd.txt.1과 같이 번호가 지정된 고유한 파일 이름으로 바꿉니다. 예를 들어 감사 로그 파일의 이름을 2015-10-25.txt.1로 바꿀 수 있습니다

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

5. AMS 서비스를 다시 시작합니다. `service ams start`
6. 모든 감사 로그 파일 복사: `scp * admin@storage_node_01_IP:/var/local/tmp/saved-audit-logs`

Prometheus 데이터를 복사합니다

Prometheus 데이터베이스를 복사하는 데 1시간 이상이 걸릴 수 있습니다. 일부 그리드 관리자 기능은 관리 노드에서 서비스가 중지되는 동안 사용할 수 없습니다.

1. 디렉토리를 생성하여 Prometheus 데이터를 별도의 그리드 노드의 임시 위치에 복사합니다. 다시 한 번 사용자_storage_node_01_입니다.
   a. 스토리지 노드에 로그인합니다.
      i. 다음 명령을 입력합니다. `ssh admin@storage_node_01_IP`
      ii. 에 나열된 암호를 입력합니다 `Passwords.txt` 파일.
      iii. mkdir -p /var/local/tmp/Prometheus'입니다
2. 관리자 노드에 로그인합니다.
   a. 다음 명령을 입력합니다. `ssh admin@admin_node_IP`
   b. 에 나열된 암호를 입력합니다 `Passwords.txt` 파일.
   c. 루트로 전환하려면 다음 명령을 입력합니다. `su -`
   d. 에 나열된 암호를 입력합니다 `Passwords.txt` 파일.
   e. SSH 에이전트에 SSH 개인 키를 추가합니다. 입력: `ssh-add`

f. 에 나열된 SSH 액세스 암호를 입력합니다 `Passwords.txt` 파일.

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

3. 관리 노드에서 Prometheus 서비스를 중지합니다. `service prometheus stop`
   a. 소스 관리 노드에서 스토리지 노드 백업 위치로 Prometheus 데이터베이스를 복사합니다. 노드: `/rsync -azh --stats "/var/local/mysql_ibdata/prometheus/data" " storage_node_01_IP:/var/local/tmp/prometheus/"`
4. 소스 관리 노드에서 Prometheus 서비스를 다시 시작합니다.`service prometheus start`

내역 정보 백업

내역 정보는 MySQL 데이터베이스에 저장됩니다. 데이터베이스 복사본을 덤프하려면 NetApp의 사용자 및 암호가 필요합니다. 그리드에 다른 관리 노드가 있는 경우 이 단계는 필요하지 않으며 복구 프로세스 중에 나머지 관리 노드에서 데이터베이스를 복제할 수 있습니다.

1. 관리자 노드에 로그인합니다.
   a. 다음 명령을 입력합니다. `ssh admin@admin_node_IP`
   b. 에 나열된 암호를 입력합니다 `Passwords.txt` 파일.
   c. 루트로 전환하려면 다음 명령을 입력합니다. `su -`
   d. 에 나열된 암호를 입력합니다 `Passwords.txt` 파일.
   e. SSH 에이전트에 SSH 개인 키를 추가합니다. 입력: `ssh-add`
   f. 에 나열된 SSH 액세스 암호를 입력합니다 `Passwords.txt` 파일.

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

2. 관리자 노드에서 StorageGRID 서비스를 중지하고 NTP 및 MySQL을 시작합니다
   a. 모든 서비스 중지: `service servermanager stop`
   b. NTP 서비스 다시 시작: `service ntp start`.. MySQL 서비스를 다시 시작합니다. `service mysql start`
3. mi 데이터베이스를 /var/local/tmp에 덤프합니다
   a. 다음 명령을 입력합니다. `mysqldump -u username -p password mi > /var/local/tmp/mysql-mi.sql`
4. MySQL dump 파일을 대체 노드에 복사합니다. *storage_node_01*을 사용합니다. *`scp /var/local/tmp/mysql-mi.sql _storage_node_01_IP:/var/local/tmp/mysql-mi.sql`*
   a. 다른 서버에 대한 암호 없는 액세스가 더 이상 필요하지 않으면 SSH 에이전트에서 개인 키를 제거합니다. 입력: `ssh-add -D`

관리 노드를 재구축합니다

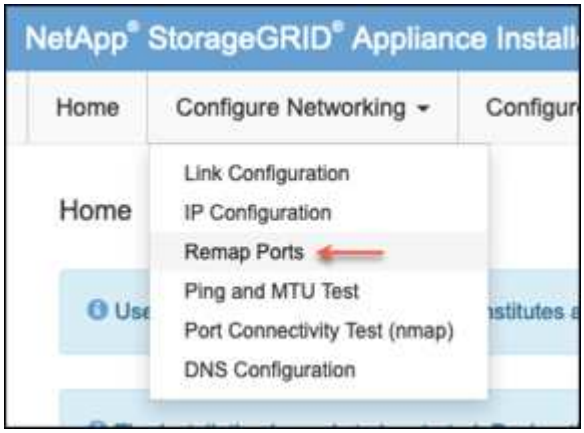
이제 원하는 모든 데이터의 백업 복사본이 있으며 그리드의 다른 관리 노드에 기록하거나 임시 위치에 저장되었으므로 어플라이언스를 재설정하여 포트 재맵을 구성할 수 있습니다.

1. 어플라이언스를 재설정하면 사전 설치된 상태로 돌아가고 호스트 이름, IP 및 네트워크 구성만 유지됩니다. 모든 데이터가 손실되므로 중요한 정보를 백업하도록 했습니다.

   a. 다음 명령을 입력합니다. `sgareinstall`

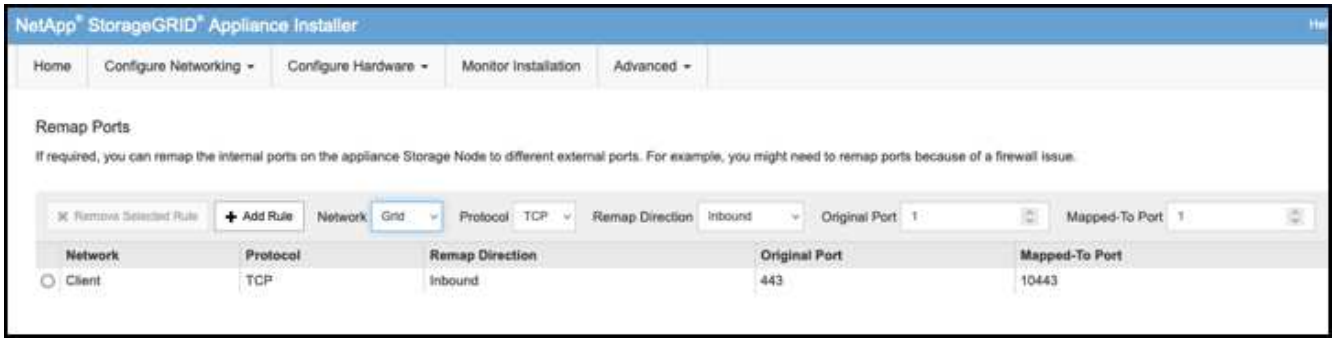
```
root@sg100-01:~ # sgareinstall
WARNING: All StorageGRID Webscale services on this node will be shut
down.
WARNING: Data stored on this node may be lost.
WARNING: You will have to reinstall StorageGRID Webscale to this
node.

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. 잠시 후 어플라이언스가 재부팅되고 노드 PGE UI에 액세스할 수 있습니다.
3. Configure Networking으로 이동합니다



4. 원하는 네트워크, 프로토콜, 방향 및 포트를 선택한 다음 규칙 추가 버튼을 클릭합니다.

> 그리드 네트워크에서 인바운드 포트 443을 다시 매핑하면 설치와 확장 절차가 중단됩니다. 그리드 네트워크에서 포트 443을 다시 매핑하지 않는 것이 좋습니다.



5. 원하는 포트 재맵이 추가되었습니다. 홈 탭으로 돌아가 설치 시작 버튼을 클릭합니다.

이제 의 관리 노드 복구 절차를 수행할 수 있습니다 "제품 설명서"

데이터베이스 및 로그 복원

이제 관리 노드가 복구되었으므로 메트릭, 로그 및 기간별 정보를 복구할 수 있습니다. 그리드에 다른 관리 노드가 있는 경우, 에 따르십시오 "제품 설명서" Prometheus-clone-db.sh_and_mi-clone-db.sh_scripts를 사용합니다. 이 노드가 유일한 관리 노드이고 이 데이터를 백업하도록 선택한 경우 다음 단계에 따라 정보를 복원할 수 있습니다.

감사 로그를 다시 복사합니다

1. 관리자 노드에 로그인합니다.
   a. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`
   b. 에 나열된 암호를 입력합니다 `Passwords.txt` 파일.
   c. 루트로 전환하려면 다음 명령을 입력합니다. `su -`
   d. 에 나열된 암호를 입력합니다 `Passwords.txt` 파일.
   e. SSH 에이전트에 SSH 개인 키를 추가합니다. 입력: `ssh-add`
   f. 에 나열된 SSH 액세스 암호를 입력합니다 `Passwords.txt` 파일.

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

2. 보존된 감사 로그 파일을 복구된 관리 노드에 복사합니다. `scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY* .`
3. 보안을 위해 장애가 발생한 그리드 노드에서 복구된 관리 노드에 성공적으로 복사되었는지 확인한 후 감사 로그를 삭제합니다.
4. 복구된 관리 노드에서 감사 로그 파일의 사용자 및 그룹 설정을 업데이트합니다. `chown ams-user:bycast *`

또한 감사 공유에 대한 기존 클라이언트 액세스도 복원해야 합니다. 자세한 내용은 StorageGRID 관리 지침을 참조하십시오.

Prometheus 메트릭을 복원합니다

Prometheus 데이터베이스를 복사하는 데 1시간 이상이 걸릴 수 있습니다. 일부 그리드 관리자 기능은 관리 노드에서 서비스가 중지되는 동안 사용할 수 없습니다.

1. 관리자 노드에 로그인합니다.
   a. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`
   b. 에 나열된 암호를 입력합니다 `Passwords.txt` 파일.
   c. 루트로 전환하려면 다음 명령을 입력합니다. `su -`
   d. 에 나열된 암호를 입력합니다 `Passwords.txt` 파일.
   e. SSH 에이전트에 SSH 개인 키를 추가합니다. 입력: `ssh-add`
   f. 에 나열된 SSH 액세스 암호를 입력합니다 `Passwords.txt` 파일.

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

2. 관리 노드에서 Prometheus 서비스를 중지합니다. `service prometheus stop`
   a. 임시 백업 위치에서 관리자 노드로 Prometheus 데이터베이스를 복사합니다. `/rsync -azh --stats "backup_node:/var/local/tmp/prometheus/" "/var/local/mysql_ibdata/prometheus/"`
   b. 데이터가 올바른 경로에 있고 완전한지 확인합니다 `ls /var/local/mysql_ibdata/prometheus/data/`
3. 소스 관리 노드에서 Prometheus 서비스를 다시 시작합니다.`service prometheus start`

내역 정보를 복원합니다

1. 관리자 노드에 로그인합니다.
   a. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`
   b. 에 나열된 암호를 입력합니다 `Passwords.txt` 파일.
   c. 루트로 전환하려면 다음 명령을 입력합니다. `su -`
   d. 에 나열된 암호를 입력합니다 `Passwords.txt` 파일.
   e. SSH 에이전트에 SSH 개인 키를 추가합니다. 입력: `ssh-add`
   f. 에 나열된 SSH 액세스 암호를 입력합니다 `Passwords.txt` 파일.

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

2. 대체 노드에서 MySQL 덤프 파일을 복사합니다. `scp grid_node_IP_:/var/local/tmp/mysql-mi.sql /var/local/tmp/mysql-mi.sql`
3. 관리자 노드에서 StorageGRID 서비스를 중지하고 NTP 및 MySQL을 시작합니다

a. 모든 서비스 중지: `service servermanager stop`

b. NTP 서비스 다시 시작: `service ntp start`.. MySQL 서비스를 다시 시작합니다. `service mysql start`

4. mi 데이터베이스를 드롭하고 비어 있는 새 데이터베이스를 생성합니다. `mysql -u username -p password -A mi -e "drop database mi; create database mi;"`
5. 데이터베이스 덤프에서 MySQL 데이터베이스 복원: `mysql -u username -p password -A mi < /var/local/tmp/mysql-mi.sql`
6. 다른 서비스를 모두 다시 시작합니다 `service servermanager start`

_ 아론 클라인 _

저작권 정보

상표 정보