Produktfunktionshandbücher

How to enable StorageGRID in your environment

NetApp
April 26, 2024

Inhalt

Produktfunktionshandbücher

Cloud Storage Pool für AWS oder Google Cloud erstellen

Sie können einen Cloud Storage Pool verwenden, wenn Sie StorageGRID-Objekte in einen externen S3-Bucket verschieben möchten. Der externe Bucket kann zu Amazon S3 (AWS) oder Google Cloud gehören.

Was Sie benötigen

- StorageGRID 11.6 wurde konfiguriert.
- Sie haben bereits einen externen S3-Bucket auf AWS oder Google Cloud eingerichtet.

Schritte

1. Navigieren Sie im Grid Manager zu **ILM** > **Storage Pools**.
2. Wählen Sie im Abschnitt Cloud-Speicherpools der Seite **Erstellen** aus.

   Das Popup-Fenster „Cloud-Speicherpool erstellen“ wird angezeigt.

3. Geben Sie einen Anzeigenamen ein.
4. Wählen Sie in der Dropdown-Liste Provider Type * Amazon S3* aus.

   Dieser Provider-Typ funktioniert für AWS S3 oder Google Cloud.

5. Geben Sie den URI für den S3-Bucket ein, der für den Cloud-Storage-Pool verwendet werden soll.

   Es sind zwei Formate zulässig:

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

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

6. Geben Sie den S3-Bucket-Namen ein.

   Der angegebene Name muss exakt mit dem Namen des S3-Buckets übereinstimmen. Andernfalls schlägt die Erstellung von Cloud-Storage-Pool fehl. Sie können diesen Wert nicht ändern, nachdem der Cloud-Speicherpool gespeichert wurde.

7. Geben Sie optional die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel ein.
8. Wählen Sie in der Dropdown-Liste * Zertifikat nicht überprüfen* aus.
9. Klicken Sie Auf **Speichern**.

Erwartetes Ergebnis

Es muss sichergestellt werden, dass ein Cloud-Storage-Pool für Amazon S3 oder Google Cloud erstellt wurde.

Von Jonathan Wong

Cloud Storage Pool für Azure Blob Storage erstellen

Sie können einen Cloud Storage Pool verwenden, wenn Sie StorageGRID-Objekte in

einen externen Azure Container verschieben möchten.

Was Sie benötigen

- StorageGRID 11.6 wurde konfiguriert.
- Sie haben bereits einen externen Azure-Container eingerichtet.

Schritte

1. Navigieren Sie im Grid Manager zu **ILM** > **Storage Pools**.
2. Wählen Sie im Abschnitt Cloud-Speicherpools der Seite **Erstellen** aus.

   Das Popup-Fenster „Cloud-Speicherpool erstellen“ wird angezeigt.

3. Geben Sie einen Anzeigenamen ein.
4. Wählen Sie in der Dropdown-Liste Provider Type * Azure Blob Storage* aus.
5. Geben Sie den URI für den S3-Bucket ein, der für den Cloud-Storage-Pool verwendet werden soll.

   Es sind zwei Formate zulässig:

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

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

6. Geben Sie den Azure-Containernamen ein.

   Der angegebene Name muss exakt mit dem Azure-Containernamen übereinstimmen. Andernfalls schlägt die Erstellung des Cloud-Storage-Pools fehl. Sie können diesen Wert nicht ändern, nachdem der Cloud-Speicherpool gespeichert wurde.

7. Geben Sie optional den zugeordneten Kontonamen und den Kontokschlüssel des Azure-Containers für die Authentifizierung ein.
8. Wählen Sie in der Dropdown-Liste * Zertifikat nicht überprüfen* aus.
9. Klicken Sie Auf **Speichern**.

Erwartetes Ergebnis

Erstellen eines Cloud-Storage-Pools für Azure Blob Storage bestätigen

Von Jonathan Wong

Verwenden Sie einen Cloud Storage Pool für Backups

Sie können eine ILM-Regel erstellen, um Objekte für Backups in einen Cloud Storage-Pool zu verschieben.

Was Sie benötigen

- StorageGRID 11.6 wurde konfiguriert.
- Sie haben bereits einen externen Azure-Container eingerichtet.

Schritte

1. Navigieren Sie im Grid Manager zu **ILM** > **Regeln** > **Erstellen**.

2. Geben Sie eine Beschreibung ein.
3. Geben Sie ein Kriterium ein, um die Regel auszulösen.
4. Klicken Sie Auf **Weiter**.
5. Replizieren Sie das Objekt auf Storage Nodes.
6. Fügen Sie eine Platzierungsregel hinzu.
7. Replizieren des Objekts in den Cloud Storage Pool
8. Klicken Sie Auf **Weiter**.
9. Klicken Sie Auf **Speichern**.

Erwartetes Ergebnis

Vergewissern Sie sich, dass im Aufbewahrungsdiagramm die lokal in StorageGRID gespeicherten Objekte und in einem Cloud-Speicherpool für Backups angezeigt werden.

Vergewissern Sie sich, dass bei Auslösung der ILM-Regel im Cloud Storage Pool eine Kopie vorhanden ist und Sie das Objekt lokal abrufen können, ohne ein Objekt wiederherstellen zu müssen.

Von Jonathan Wong

Konfigurieren Sie den Integrationsservice für die StorageGRID Suche

Dieses Handbuch enthält detaillierte Anweisungen zur Konfiguration des NetApp StorageGRID 11.6 Suchintegrationsservice mit Amazon OpenSearch Service oder On-Premises-Elasticsearch.

Einführung

StorageGRID unterstützt drei Arten von Plattform-Services.

- **StorageGRID CloudMirror Replikation**. Spiegeln bestimmter Objekte aus einem StorageGRID-Bucket auf ein angegebenes externes Ziel
- **Benachrichtigungen**. Bucket-spezifische Ereignisbenachrichtigungen senden Benachrichtigungen über bestimmte Aktionen, die an Objekten durchgeführt werden, an einen bestimmten externen Amazon Simple Notification Service (Amazon SNS).
- **Integrationsservice suchen**. Senden von einfachen Storage Service (S3) Objektmetadaten in einen angegebenen Elasticsearch-Index, wo Sie die Metadaten mithilfe des externen Service durchsuchen oder analysieren können.

Plattform-Services werden vom S3-Mandanten über die Mandanten-Manager-UI konfiguriert. Weitere Informationen finden Sie unter "Überlegungen bei der Verwendung von Plattform-Services".

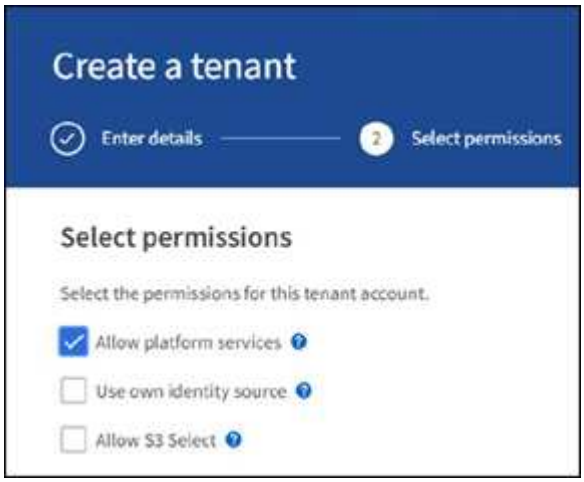
Dieses Dokument dient als Ergänzung zum "StorageGRID 11.6 Mandantenleitfaden" Und enthält Schritt-für-Schritt-Anleitungen und Beispiele für die Endpunkt- und Bucket-Konfiguration für Suchintegrations-Services. Die hier enthaltene Anleitung zur Einrichtung von Amazon Web Services (AWS) oder lokalen Elasticsearch-Services dienen nur zu Test- oder Demonstrationszwecken.

Zielgruppen sollten mit Grid Manager, Mandanten-Manager vertraut sein und über den S3-Browser Zugang verfügen, um grundlegende Vorgänge zum Hochladen (PUT) und Herunterladen (GET) für StorageGRID-

Suchintegrationstests durchzuführen.

Erstellung von Mandanten und Aktivierung von Plattform-Services

1. Erstellen Sie einen S3-Mandanten mithilfe von Grid Manager, geben Sie einen Anzeigenamen ein und wählen Sie das S3-Protokoll aus.
2. Wählen Sie auf der Berechtigungsseite die Option Plattformdienste zulassen. Wählen Sie ggf. andere Berechtigungen aus.



3. Richten Sie das ursprüngliche Kennwort des Mandanten-Root-Benutzers ein, oder wählen Sie, falls im Raster der Identifikationsverbund aktiviert ist, welche föderierte Gruppe Root-Zugriffsberechtigungen hat, um das Mandantenkonto zu konfigurieren.
4. Klicken Sie auf als Stamm anmelden und wählen Sie Bucket: Erstellen und verwalten.

   Dies führt Sie zur Seite Tenant Manager.

5. Wählen Sie im Tenant Manager My Access Keys aus, um den S3-Zugriffsschlüssel für spätere Tests zu erstellen und herunterzuladen.

Integrationsservices mit Amazon OpenSearch suchen

Einrichtung des Amazon OpenSearch Service (ehemals Elasticsearch)

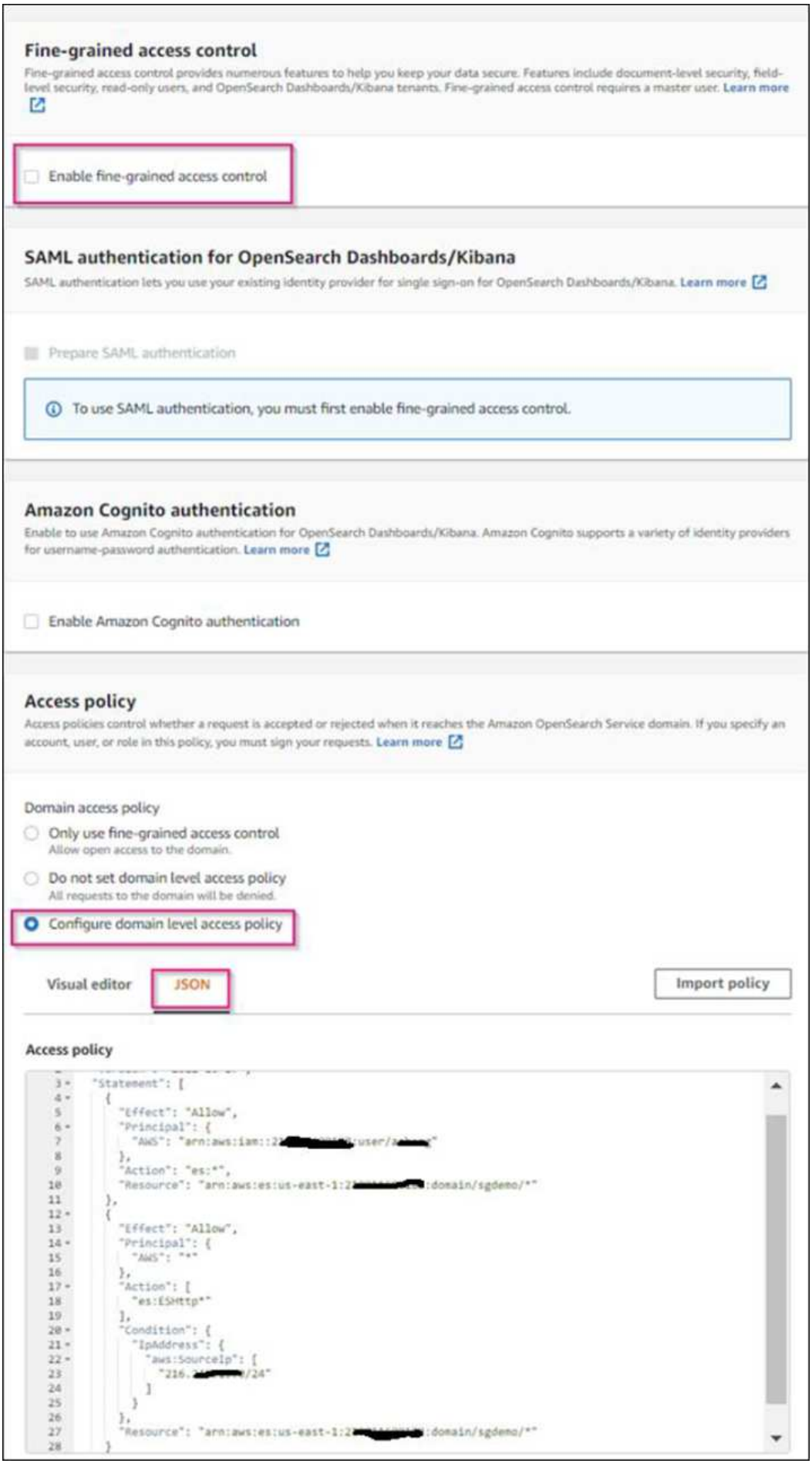
Verwenden Sie dieses Verfahren für eine schnelle und einfache Einrichtung des OpenSearch-Dienstes nur zu Test-/Demo-Zwecken. Wenn Sie On-Premises-Elasticsearch für Suchintegrationsservices verwenden, lesen Sie den Abschnitt Suchintegrations-Services für On-Premises-Elasticsearch.

> Sie müssen über eine gültige Anmeldung für die AWS-Konsole, einen Zugriffsschlüssel, einen geheimen Zugriffsschlüssel und die Berechtigung zum Abonnieren des OpenSearch-Dienstes verfügen.

1. Erstellen Sie mithilfe der Anweisungen von eine neue Domäne "AWS OpenSearch Service – erste Schritte", Mit Ausnahme der folgenden:
   - Schritt 4: Domain-Name: Sgdemo
   - Schritt 10: Feinkörnige Zugriffssteuerung: Deaktivieren Sie die Option Enable Fine-genarainable Access Control.

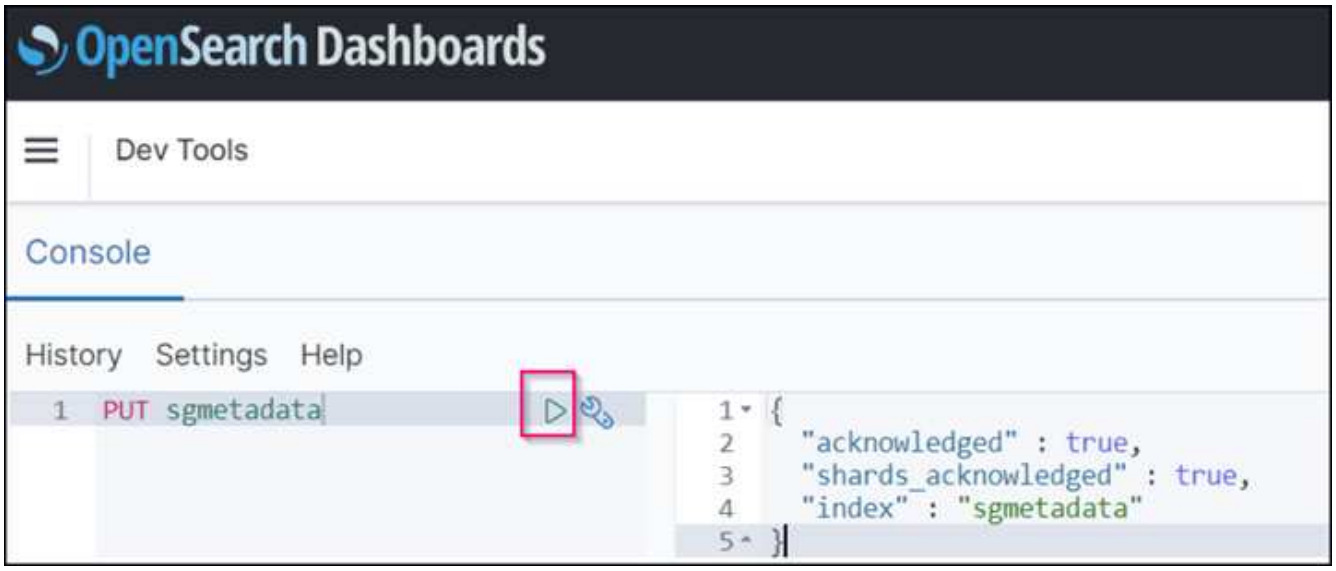
- Schritt 12: Zugriffsrichtlinie: Wählen Sie Zugriffsrichtlinie auf Zugriffsebene konfigurieren, wählen Sie die Registerkarte JSON aus, um die Zugriffsrichtlinie anhand des folgenden Beispiels zu ändern:
  - Ersetzen Sie den hervorgehobenen Text durch Ihre eigene AWS IAM-ID (Identity and Access Management) und Ihren Benutzernamen.
  - Ersetzen Sie den markierten Text (die IP-Adresse) durch die öffentliche IP-Adresse Ihres lokalen Computers, über den Sie auf die AWS-Konsole zugreifen.
  - Öffnen Sie eine Browserregisterkarte für "https://checkip.amazonaws.com" Um Ihre öffentliche IP zu finden.

```
{

    "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/*"
        }
    ]
}
```

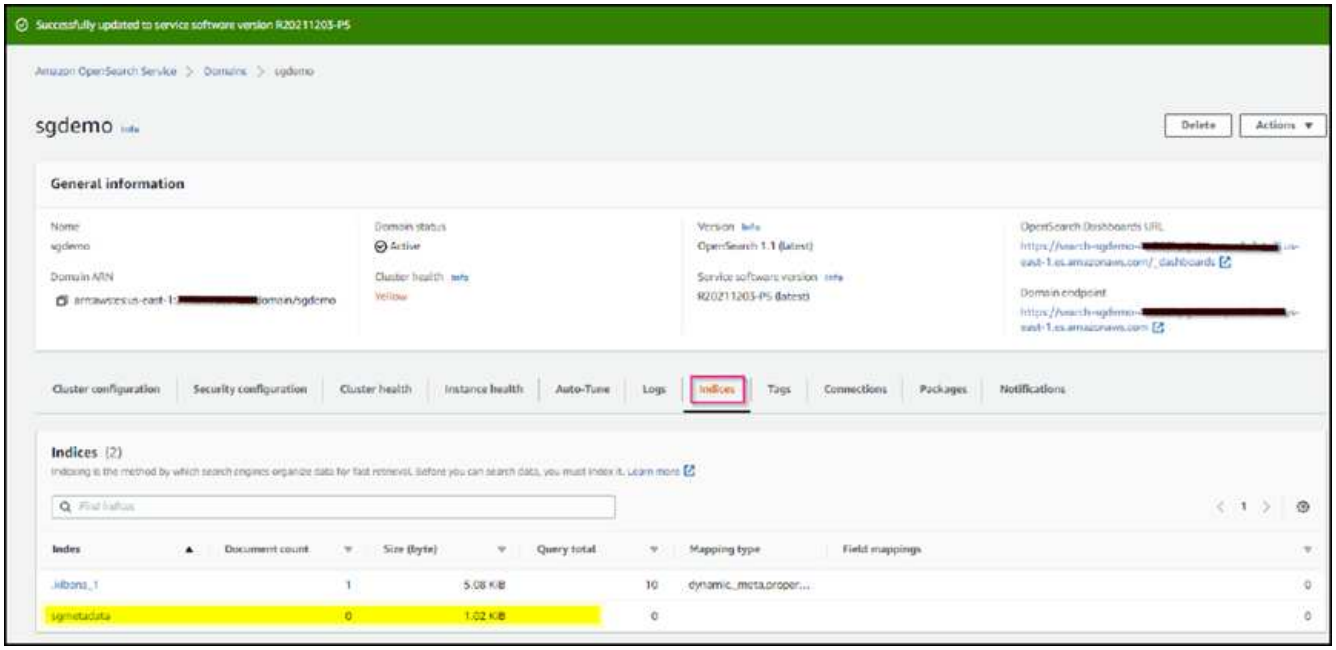

Fine-grained access control
Fine-grained access control provides numerous features to help you keep your data secure. Features include document-level security, field-level security, read-only users, and OpenSearch Dashboards/Kibana tenants. Fine-grained access control requires a master user. Learn more
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. Warten Sie 15 bis 20 Minuten, bis die Domain aktiv ist.

3. Klicken Sie auf OpenSearch Dashboards URL, um die Domäne in einer neuen Registerkarte zu öffnen, um auf das Dashboard zuzugreifen. Wenn ein Fehler beim Zugriff verweigert wird, überprüfen Sie, ob die Quell-IP-Adresse der Zugriffsrichtlinie korrekt auf Ihre öffentliche IP-Adresse des Computers eingestellt ist, um den Zugriff auf das Domain-Dashboard zu ermöglichen.
4. Wählen Sie auf der Willkommensseite des Dashboards „Explore“ auf eigene Faust aus. Wählen Sie im Menü „Management → Entwicklungstools“
5. Geben Sie unter Dev Tools → Console ein `PUT <index>` Wo Sie den Index zum Speichern von StorageGRID-Objektmetadaten verwenden. Im folgenden Beispiel verwenden wir den Indexnamen 'sgmetadaten'. Klicken Sie auf das kleine Dreieck-Symbol, um den PUT-Befehl auszuführen. Das erwartete Ergebnis wird im rechten Bereich angezeigt, wie im folgenden Beispiel Screenshot dargestellt.



6. Überprüfen Sie, ob der Index über die Benutzeroberfläche von Amazon OpenSearch unter sgdomain > Indizes sichtbar ist.

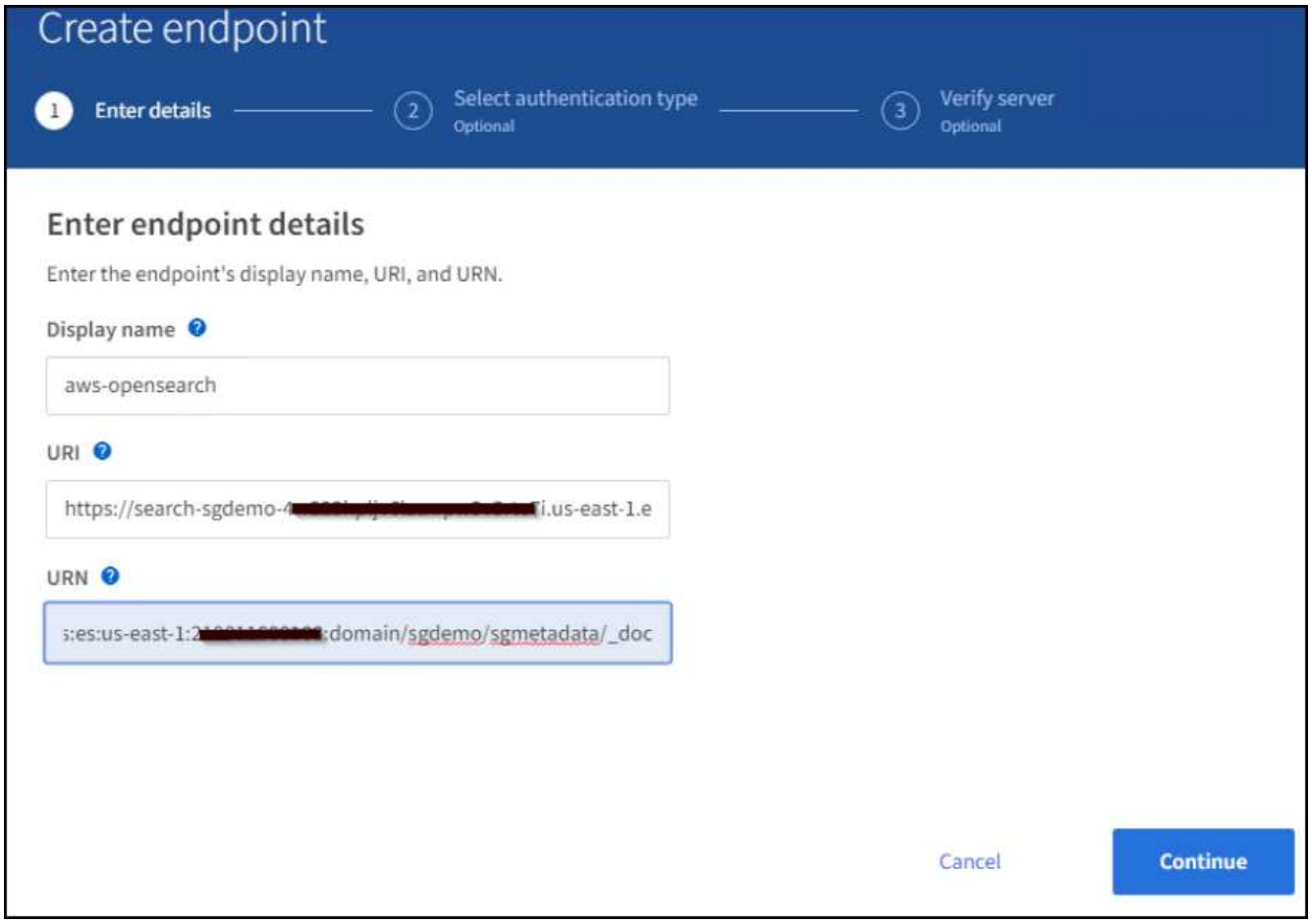


Endpoint-Konfiguration für Plattform-Services

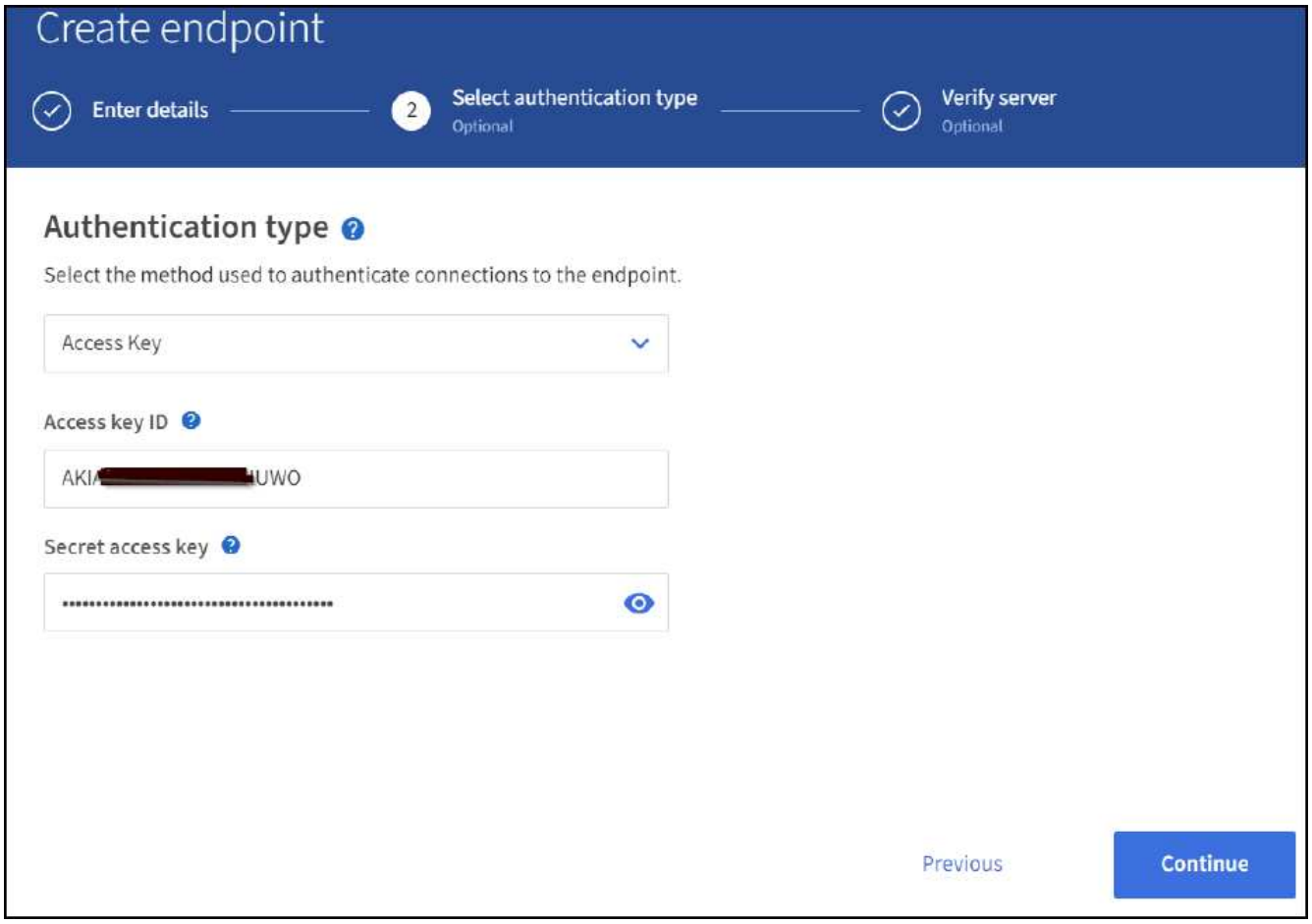
Gehen Sie wie folgt vor, um die Endpunkte der Plattformservices zu konfigurieren:

1. In Tenant Manager wechseln Sie zu STORAGE(S3) > Plattform-Services-Endpunkten.
2. Klicken Sie auf Endpunkt erstellen, geben Sie Folgendes ein und klicken Sie dann auf Weiter:
   - Beispiel für einen Anzeigenamen `aws-opensearch`
   - Der Domänenendpunkt im Beispiel-Screenshot unter Schritt 2 des vorhergehenden Verfahrens im URI-Feld.
   - Die Domäne ARN, die in Schritt 2 des vorhergehenden Verfahrens im Feld URN verwendet wurde und addieren `/<index>/_doc` Bis zum Ende von ARN.

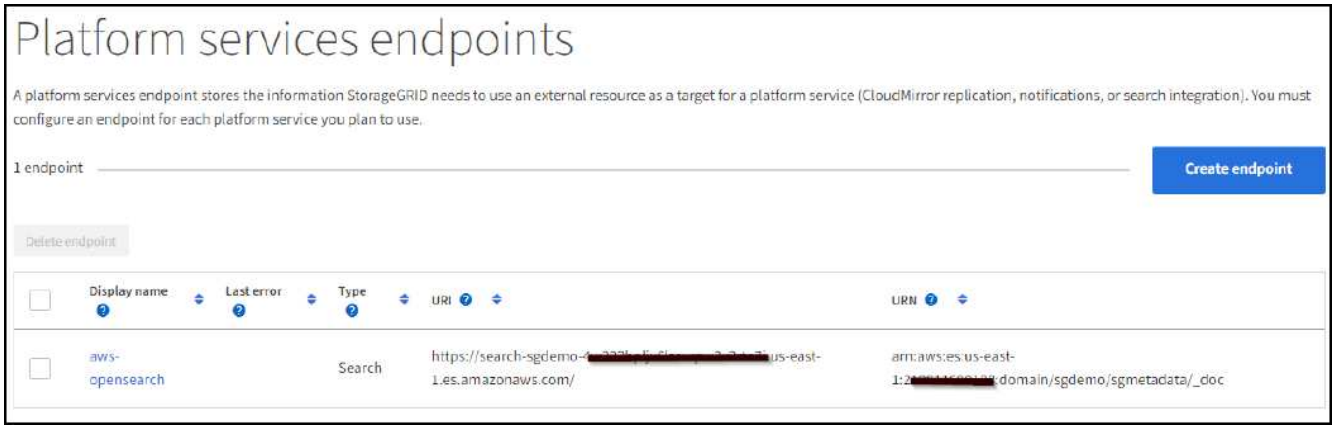
     In diesem Beispiel wird URN `arn:aws:es:us-east-1:211234567890:domain/sgdemo /sgmedata/_doc`.



3. Um auf die Amazon OpenSearch sgdomain zuzugreifen, wählen Sie als Authentifizierungstyp den Zugriffsschlüssel aus, und geben Sie dann den Amazon S3-Zugriffsschlüssel und den geheimen Schlüssel ein. Um zur nächsten Seite zu gelangen, klicken Sie auf Weiter.



4. Um den Endpunkt zu überprüfen, wählen Sie Operating System CA Certificate und Test and Create Endpoint aus. Wenn die Überprüfung erfolgreich ist, wird ein Endpunkt-Bildschirm angezeigt, der der folgenden Abbildung entspricht. Wenn die Überprüfung fehlschlägt, überprüfen Sie, ob der URN umfasst `/<index>/_doc` Am Ende des Pfads und der AWS Zugriffsschlüssel und der Geheimschlüssel sind korrekt.



Suchintegrations-Services für On-Premises-Elasticsearch

Elasticsearch-Einrichtung vor Ort

Dieses Verfahren dient der schnellen Einrichtung von vor-Ort-Elasticsearch und Kibana mit Docker nur zu Testzwecken. Wenn Elasticsearch und Kibana-Server bereits vorhanden sind, fahren Sie mit Schritt 5 fort.

1. Folgen Sie diesen Anweisungen "Docker-Installationsvorgang" So installieren Sie den Docker. Wir verwenden den "CentOS Docker Installationsverfahren" In diesem Setup.

```
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
```

   - Um den Docker nach dem Neustart zu starten, geben Sie Folgendes ein:

```
sudo systemctl enable docker
```

   - Stellen Sie die ein `vm.max_map_count` Wert für 262144:

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

   - Um die Einstellung nach dem Neustart zu behalten, geben Sie Folgendes ein:

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

2. Folgen Sie den "Elasticsearch Quick Start Guide" Selbstverwalteter Abschnitt zum Installieren und Ausführen der Elasticsearch- und Kibana-Docker. In diesem Beispiel wurde die Version 8.1 installiert.

Beachten Sie den Benutzernamen/das Kennwort und das Token, das Elasticsearch erstellt hat. Sie müssen diese zum Starten der Kibana UI und der StorageGRID-Plattform-Endpunktauthentifizierung verwenden.

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.

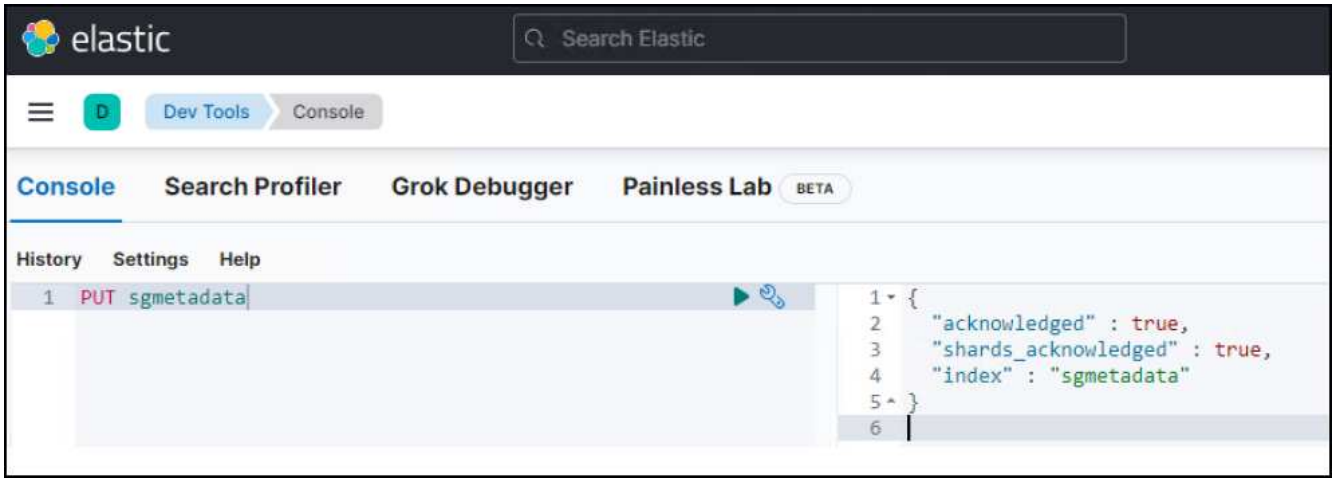
1. In a new terminal session, run:

```
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.

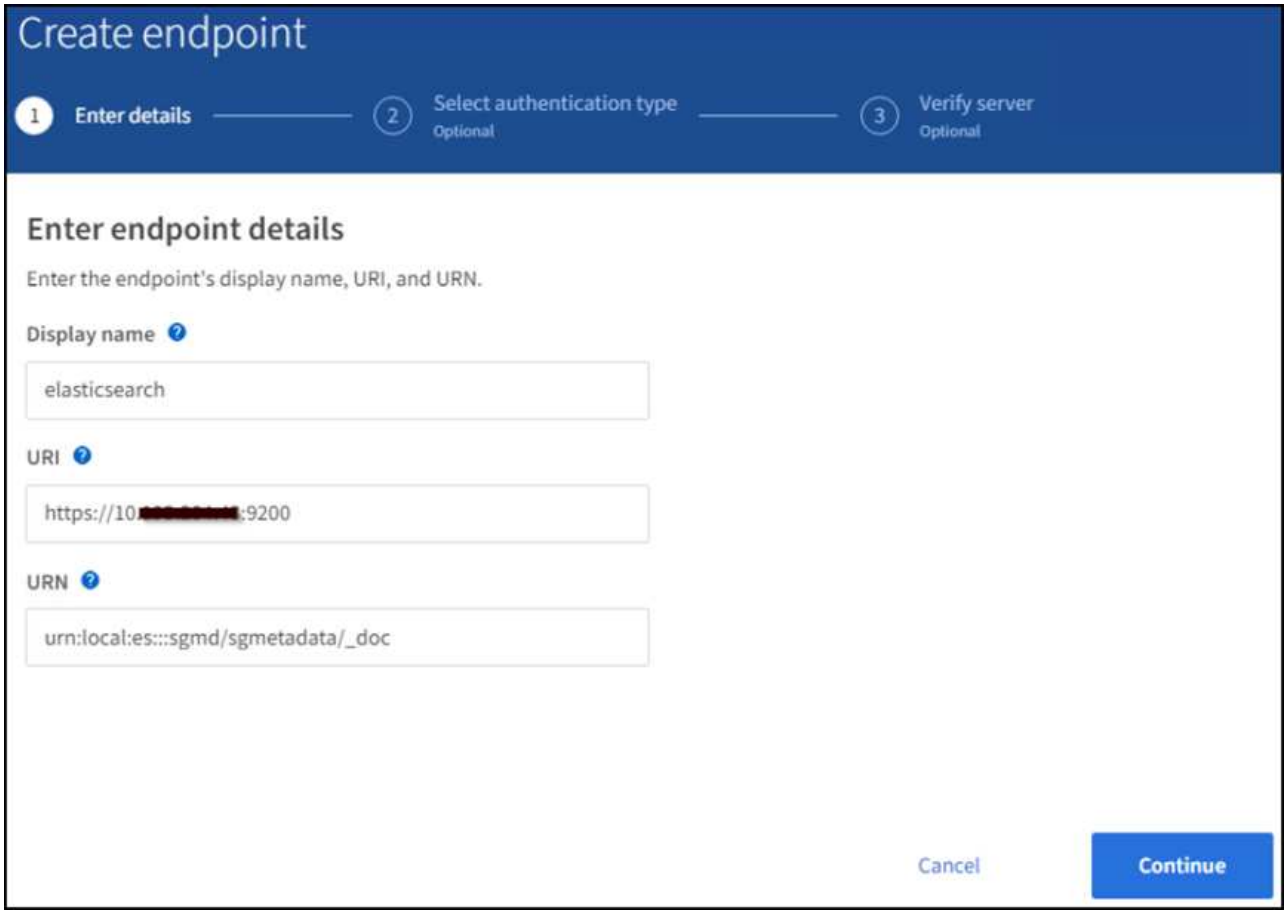
3. Nachdem der Kibana-Docker-Container gestartet wurde, wird der URL-Link aufgerufen `https://0.0.0.0:5601` Wird in der Konsole angezeigt. Ersetzen Sie 0.0.0.0 durch die Server-IP-Adresse in der URL.
4. Melden Sie sich mit dem Benutzernamen bei der Kibana-Benutzeroberfläche an `elastic` Und das Passwort, das im vorherigen Schritt von Elastic generiert wurde.
5. Wenn Sie sich zum ersten Mal anmelden möchten, wählen Sie auf der Begrüßungsseite „Explore“. Wählen Sie im Menü Verwaltung > Entwicklungstools.
6. Geben Sie auf dem Bildschirm Dev Tools Console die Eingabe ein `PUT <index>` Dort, wo Sie diesen Index zum Speichern von StorageGRID-Objektmetadaten verwenden. Wir verwenden den Indexnamen `sgmetadata` In diesem Beispiel. Klicken Sie auf das kleine Dreieck-Symbol, um den PUT-Befehl auszuführen. Das erwartete Ergebnis wird im rechten Bereich angezeigt, wie im folgenden Beispiel Screenshot dargestellt.



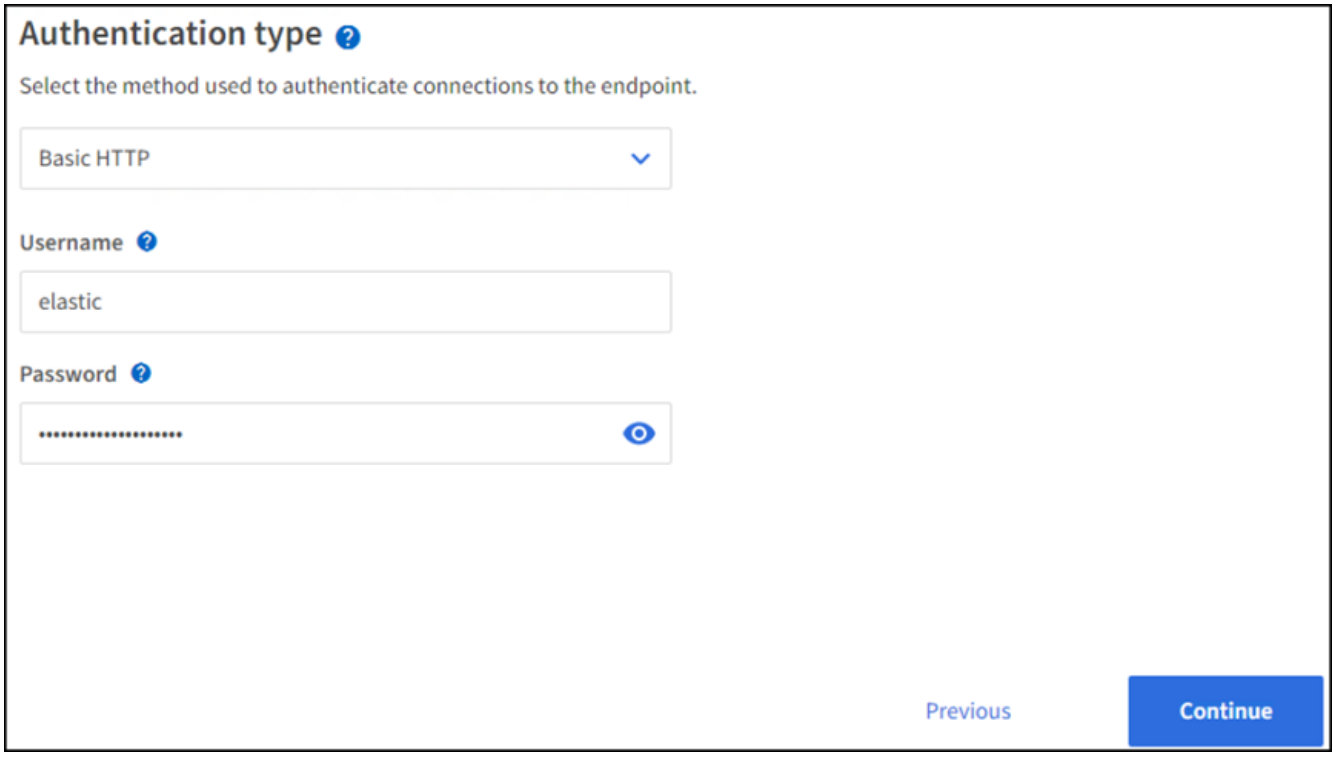
Endpoint-Konfiguration für Plattform-Services

Gehen Sie wie folgt vor, um Endpunkte für Plattformservices zu konfigurieren:

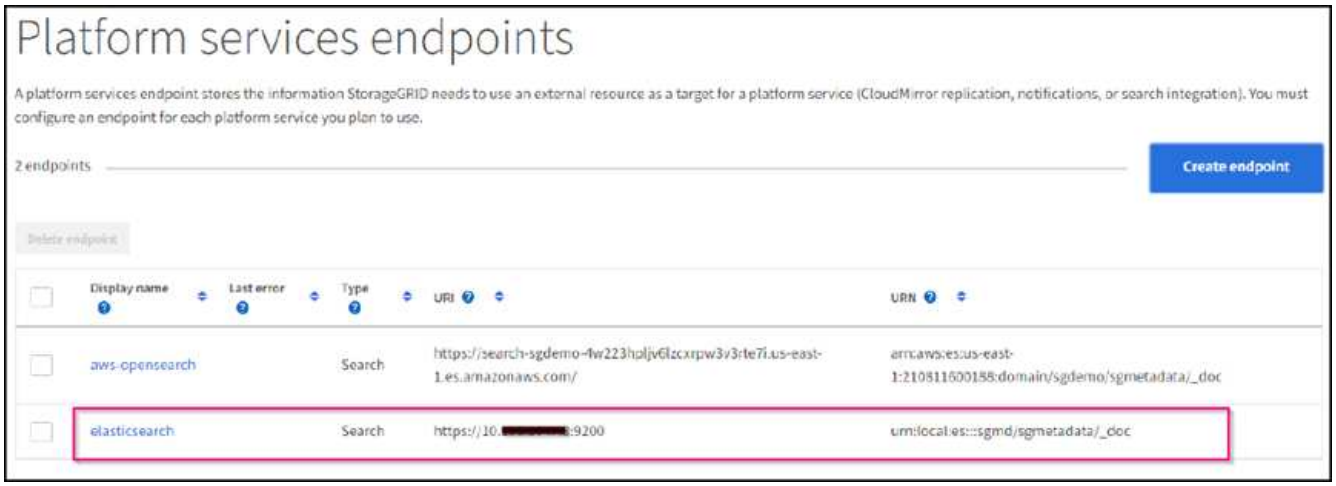
1. In Tenant Manager wechseln Sie zu STORAGE (S3) > Plattform-Services-Endpunkten
2. Klicken Sie auf Endpunkt erstellen, geben Sie Folgendes ein und klicken Sie dann auf Weiter:
   - Beispiel für Anzeigename: `elasticsearch`
   - URI: `https://<elasticsearch-server-ip or hostname>:9200`
   - URNE: `urn:<something>:es:::<some-unique-text>/<index-name>/_doc` Wobei der Indexname der Name ist, den Sie auf der Kibana-Konsole verwendet haben. Beispiel: `urn:local:es:::sgmd/sgmetadata/_doc`



3. Wählen Sie Basic HTTP als Authentifizierungstyp, geben Sie den Benutzernamen ein `elastic` Und das durch den Elasticsearch-Installationsprozess generierte Passwort. Um zur nächsten Seite zu gelangen, klicken Sie auf Weiter.



4. Wählen Sie Zertifikat nicht überprüfen und Endpunkt erstellen und testen, um den Endpunkt zu überprüfen. Wenn die Überprüfung erfolgreich ist, wird ein Endpunkt-Bildschirm angezeigt, der dem folgenden Screenshot ähnelt. Wenn die Überprüfung fehlschlägt, überprüfen Sie, ob die Einträge für URN, URI und Benutzername/Passwort korrekt sind.



Konfiguration des integrierten Service für die Bucket-Suche

Nachdem der Plattform-Service-Endpunkt erstellt wurde, besteht der nächste Schritt darin, diesen Service auf Bucket-Ebene zu konfigurieren, um Objektmetadaten an den definierten Endpunkt zu senden, sobald ein Objekt erstellt, gelöscht oder seine Metadaten oder Tags aktualisiert werden.

Sie können die Suchintegration mit Tenant Manager konfigurieren, um eine benutzerdefinierte StorageGRID-Konfigurations-XML auf einen Bucket anzuwenden wie folgt:

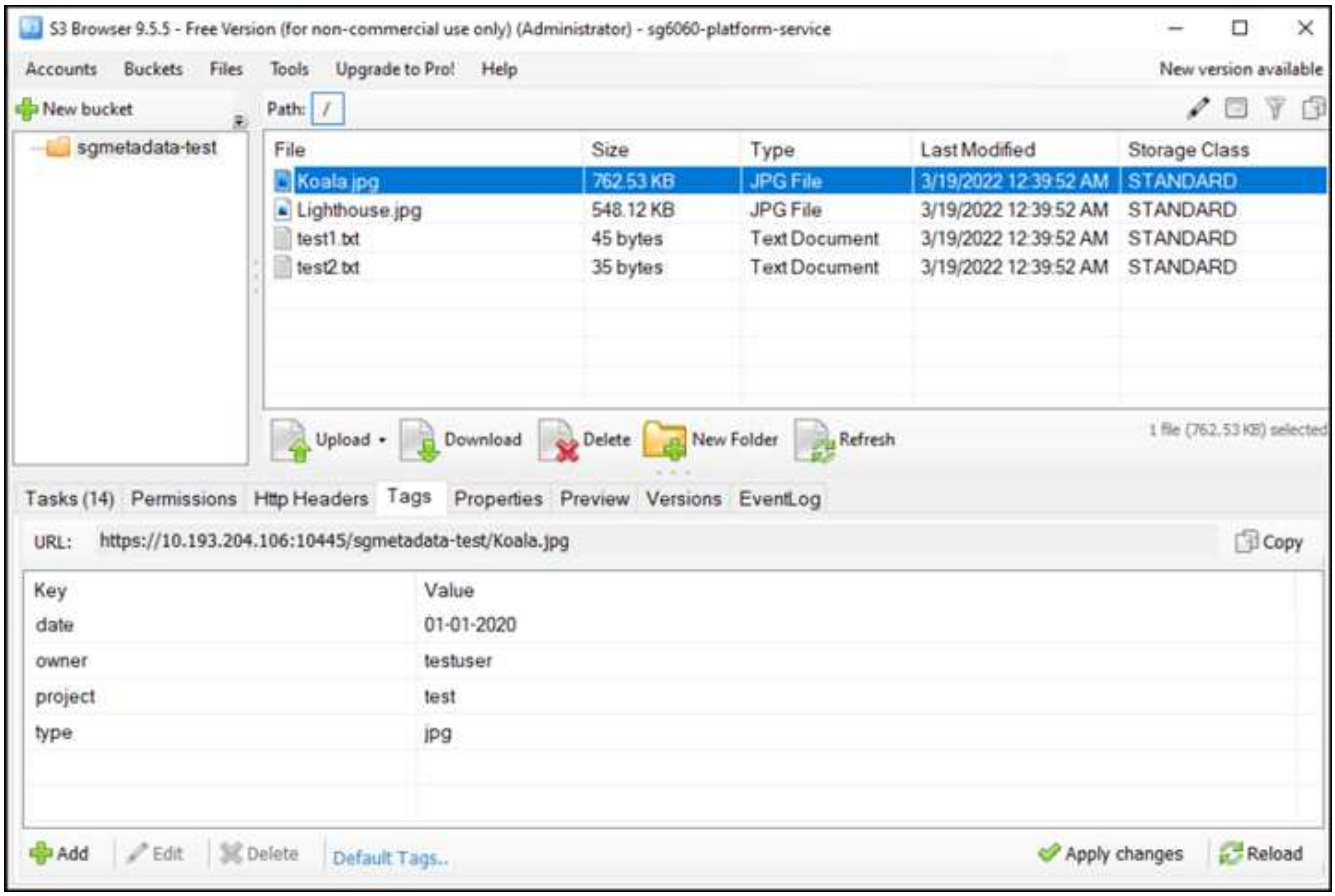
1. Wählen Sie in Tenant Manager „STORAGE(S3)“ > „Buckets“
2. Klicken Sie auf Create Bucket. Geben Sie den Bucket-Namen ein (z. B. `sgmetadata-test`) Und akzeptieren Sie die Standardeinstellung `us-east-1` Werden.
3. Klicken Sie Auf Weiter > Bucket Erstellen.
4. Um die Seite „Bucket-Übersicht“ aufzurufen, klicken Sie auf den Bucket-Namen und wählen Sie „Platform Services“ aus.
5. Wählen Sie das Dialogfeld Integration der Suche aktivieren aus. Geben Sie im angegebenen XML-Feld die Konfigurations-XML-XML-Datei unter Verwendung dieser Syntax ein.

   Der hervorgehobene URN muss mit dem von Ihnen definierten Endpunkt für Plattformservices übereinstimmen. Sie können eine weitere Browserregisterkarte öffnen, um auf den Mandantenmanager zuzugreifen und URN vom definierten Endpunkt der Plattformdienste zu kopieren.

   In diesem Beispiel haben wir kein Präfix verwendet, was bedeutet, dass die Metadaten für jedes Objekt in diesem Bucket an den zuvor definierten Elasticsearch-Endpunkt gesendet werden.

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

6. Verwenden Sie S3-Browser, um eine Verbindung zu StorageGRID mit dem Mandantenzugriff/geheimen Schlüssel herzustellen und Testobjekte in hochzuladen `sgmetadata-test` Bucket und fügen Sie Tags oder benutzerdefinierte Metadaten zu Objekten hinzu.



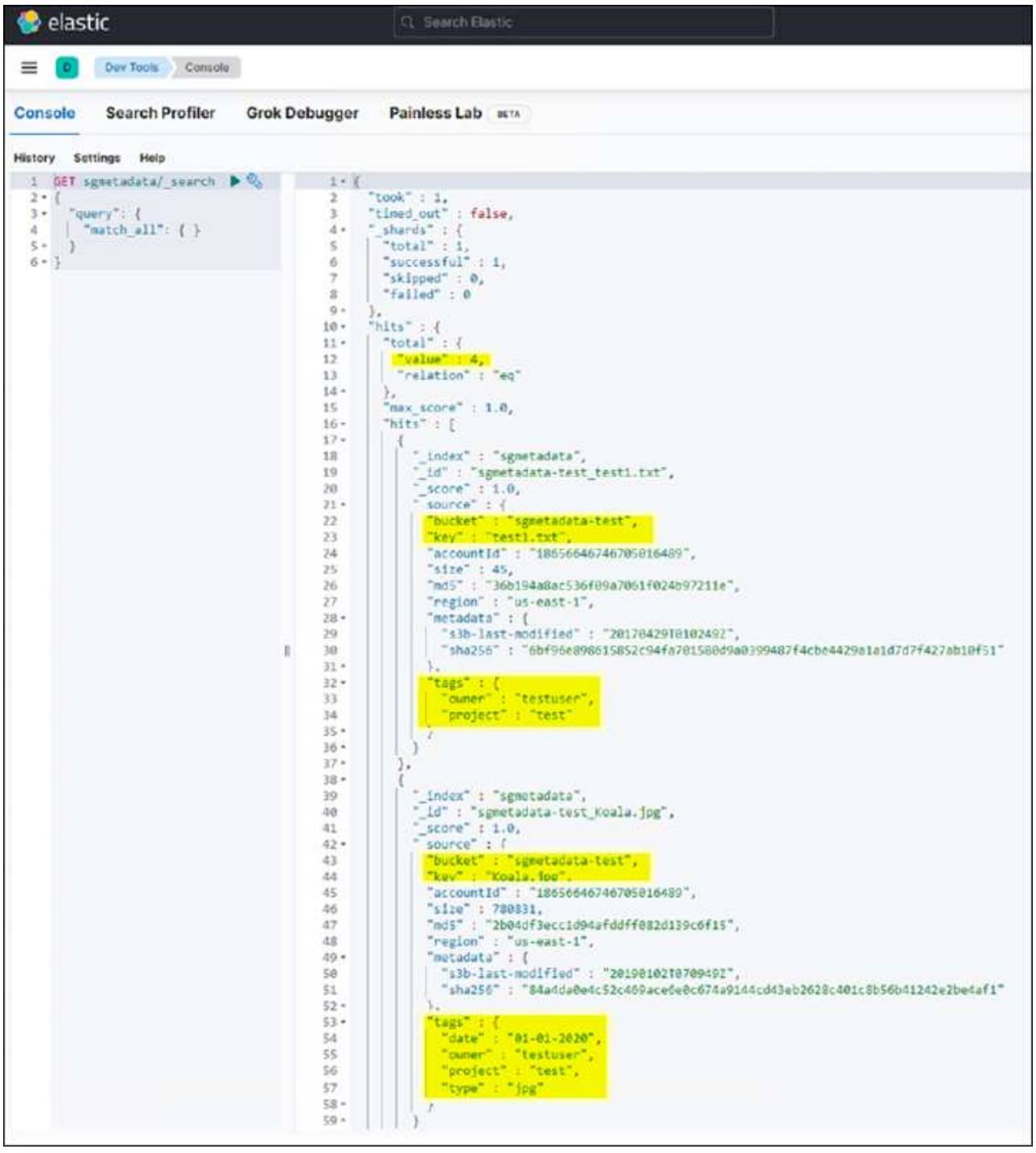
7. Verwenden Sie die Kibana UI, um zu überprüfen, ob die Objektmetadaten in den Index der sgmetadaten geladen wurden.

   a. Wählen Sie im Menü Verwaltung > Entwicklungstools.

   b. Fügen Sie die Beispielabfrage in das Konsolenfenster auf der linken Seite ein, und klicken Sie auf das Dreieckssymbol, um sie auszuführen.

      Das Beispielergebnis für die Abfrage 1 im folgenden Beispiel-Screenshot zeigt vier Datensätze. Dies entspricht der Anzahl der Objekte im Bucket.

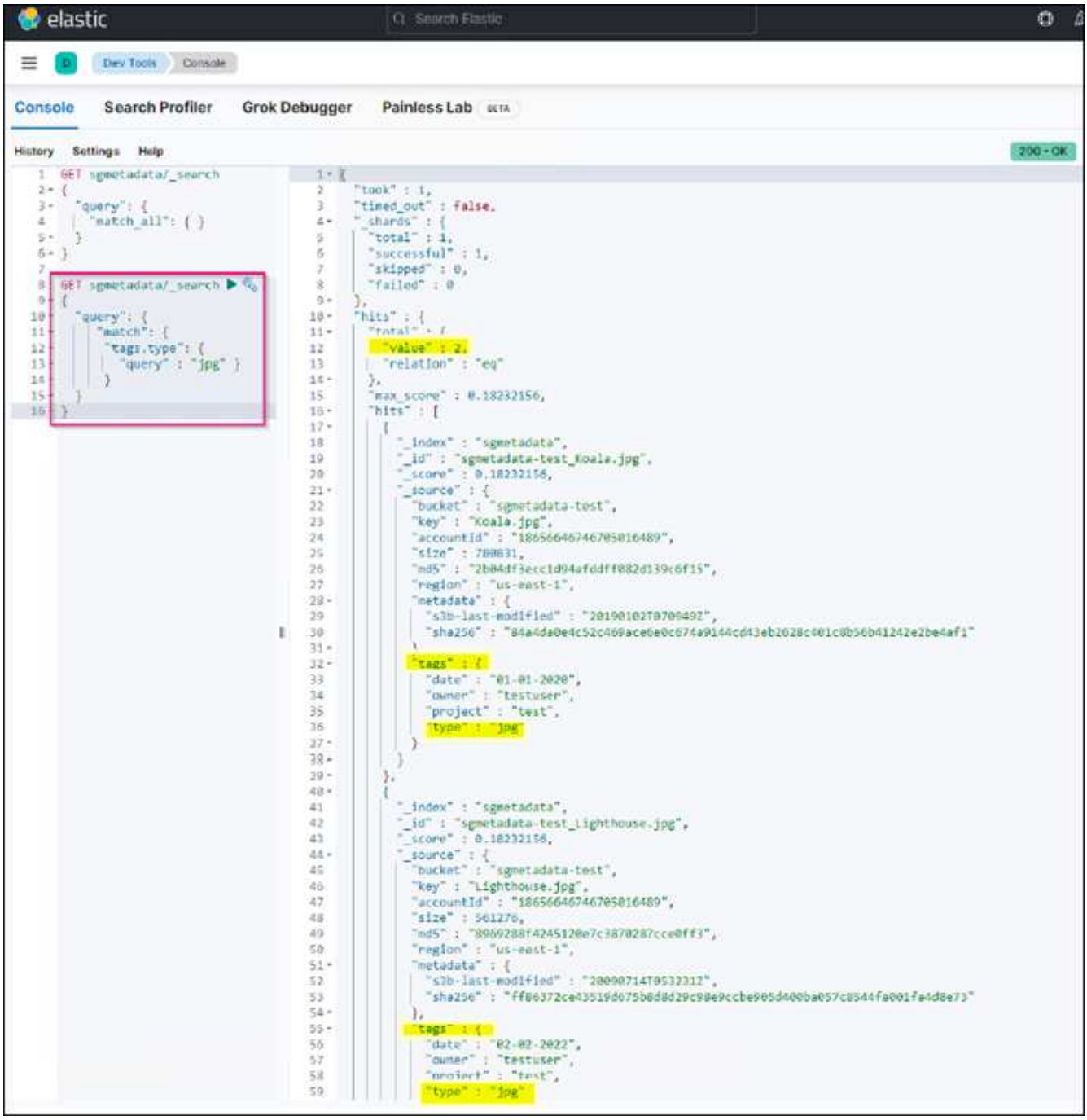
```
GET sgmetadata/_search
{
    "query": {
        "match_all": { }
}
}
```



Das Beispielergebnis für Abfrage 2 im folgenden Screenshot zeigt zwei Datensätze mit Tag-Typ jpg.

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

+



Wo Sie weitere Informationen finden

Sehen Sie sich die folgenden Dokumente und/oder Websites an, um mehr über die in diesem Dokument beschriebenen Informationen zu erfahren:

- "Was sind Plattform-Services"
- "StorageGRID 11.6-Dokumentation"

Von Angela Cheng

Node-Klonen

Überlegungen und Performance von Node-Klonen

Überlegungen zu Node-Klonen

Node-Klone können eine schnellere Methode zum Austausch vorhandener Appliance-Nodes für eine Technologieaktualisierung sein, die Kapazität erhöhen oder die Performance Ihres StorageGRID Systems steigern. Node-Klon kann auch für die Konvertierung in Node-Verschlüsselung mit einem KMS oder die Änderung eines Storage-Node von DDP8 zu DDP16 nützlich sein.

- Die genutzte Kapazität des Quell-Node ist nicht relevant für die Zeit, die für den Abschluss des Klonprozesses erforderlich ist. Node-Klon ist eine vollständige Kopie des Node, einschließlich freiem Speicherplatz im Node.
- Quell- und Ziel-Appliances müssen dieselbe PGE-Version aufweisen
- Der Zielknoten muss immer eine größere Kapazität als die Quelle haben
    - Stellen Sie sicher, dass die neue Ziel-Appliance eine größere Laufwerksgröße als die Quelle hat
    - Wenn das Zielgerät über Laufwerke gleicher Größe verfügt und für DDP8 konfiguriert ist, können Sie das Ziel für DDP16 konfigurieren. Wenn die Quelle bereits für DDP16 konfiguriert ist, ist ein Node-Klon nicht möglich.
    - Beachten Sie beim Wechsel von SG5660 oder SG5760 Appliances zu SG6060 Appliances, dass die SG5x60 60 Laufwerke mit Kapazität haben, bei denen die SG6060 nur 58 hat.
- Für den Klonprozess eines Node muss der Quell-Node für die Dauer des Klonens offline im Grid sein. Wenn ein zusätzlicher Knoten während dieser Zeit offline geht, sind möglicherweise die Client-Services betroffen.
- Ein Storage-Node kann nur 15 Tage lang offline sein. Wenn der Klonprozess fast 15 Tage beträgt oder 15 Tage überschreitet, können Sie das Erweiterungs- und Ausmusterung verwenden.
- Bei einem SG6060 mit Erweiterungs-Shelfs müssen Sie die Zeit für die richtige Shelf-Laufwerksgröße zur Zeit der Basis-Appliance hinzufügen, um die volle Klondauer zu erhalten.
- Die Anzahl der Volumes in einer Ziel-Storage-Appliance muss größer oder gleich der Anzahl der Volumes im Quell-Node sein. Sie können einen Quell-Node mit 16 Objektspeicher-Volumes (rangedb) nicht auf einer Ziel-Storage-Appliance mit 12 Objektspeicher-Volumes klonen, selbst wenn die Ziel-Appliance über eine größere Kapazität als der Quell-Node verfügt. Die meisten Storage Appliances verfügen über 16 Objektspeicher-Volumes, außer der SGF6112 Storage Appliance mit nur 12 Objektspeicher-Volumes. Sie können beispielsweise nicht von einem SG5760 in ein SGF6112 klonen.

Schätzungen der Performance von Node-Klonen

Die folgenden Tabellen enthalten berechnete Schätzungen für die Dauer von Node-Klonen. Die Bedingungen variieren, sodass Einträge in **BOLD** das 15-Tage-Limit für einen Knoten nach unten überschreiten können.

DDP8

SG5612 → beliebig

Geschwindigkeit der Netzwerkschnittstelle	Größe des 4-TB-Laufwerks	8-TB-Laufwerke	10-TB-Laufwerkgröße	12-TB-Laufwerksgröße	16-TB-Laufwerkgröße	18 TB Laufwerksgröße
10 GBIT	1 Tag	2 Tage	2.5 Tage	3 Tage	4 Tage	4.5 Tage
25 GB	1 Tag	2 Tage	2.5 Tage	3 Tage	4 Tage	4.5 Tage

SG5712 → beliebig

Geschwindigkeit der Netzwerkschnittstelle	Größe des 4-TB-Laufwerks	8-TB-Laufwerke	10-TB-Laufwerkgröße	12-TB-Laufwerksgröße	16-TB-Laufwerkgröße	18 TB Laufwerksgröße
10 GBIT	1 Tag	2 Tage	2.5 Tage	3 Tage	4 Tage	4.5 Tage
25 GB	1 Tag	2 Tage	2.5 Tage	3 Tage	4 Tage	4.5 Tage

SG5660 → SG5760

Geschwindigkeit der Netzwerkschnittstelle	Größe des 4-TB-Laufwerks	8-TB-Laufwerke	10-TB-Laufwerkgröße	12-TB-Laufwerksgröße	16-TB-Laufwerkgröße	18 TB Laufwerksgröße
10 GBIT	3 Tage	6 Tage	7 Tage	8.5 Tage	11.5 Tage	**13 Tage**
25 GB	3 Tage	6 Tage	7 Tage	8.5 Tage	11.5 Tage	**13 Tage**

SG5660 → SG6060

Geschwindigkeit der Netzwerkschnittstelle	Größe des 4-TB-Laufwerks	8-TB-Laufwerke	10-TB-Laufwerkgröße	12-TB-Laufwerksgröße	16-TB-Laufwerkgröße	18 TB Laufwerksgröße
10 GBIT	2.5 Tage	4.5 Tage	5.5 Tage	6.5 Tage	9 Tage	10 Tage
25 GB	2 Tage	4 Tage	5 Tage	6 Tage	8 Tage	9 Tage

SG5760 → SG5760

Geschwindigkeit der Netzwerkschnittstelle	Größe des 4-TB-Laufwerks	8-TB-Laufwerke	10-TB-Laufwerkgröße	12-TB-Laufwerksgröße	16-TB-Laufwerkgröße	18 TB Laufwerksgröße
10 GBIT	3 Tage	6 Tage	7 Tage	8.5 Tage	11.5 Tage	**13 Tage**
25 GB	3 Tage	6 Tage	7 Tage	8.5 Tage	11.5 Tage	**13 Tage**

SG5760 → SG6060

Geschwindigkeit der Netzwerkschnittstelle	Größe des 4-TB-Laufwerks	8-TB-Laufwerke	10-TB-Laufwerkgröße	12-TB-Laufwerksgröße	16-TB-Laufwerkgröße	18 TB Laufwerksgröße
10 GBIT	2.5 Tage	4.5 Tage	5.5 Tage	6.5 Tage	9 Tage	10 Tage
25 GB	1.5 Tage	3 Tage	3.5 Tage	4.5 Tage	6 Tage	6.5 Tage

SG6060 → SG6060

Geschwindigkeit der Netzwerkschnittstelle	Größe des 4-TB-Laufwerks	8-TB-Laufwerke	10-TB-Laufwerkgröße	12-TB-Laufwerksgröße	16-TB-Laufwerkgröße	18 TB Laufwerksgröße
10 GBIT	2.5 Tage	4.5 Tage	5.5 Tage	6.5 Tage	8.5 Tage	9.5 Tage
25 GB	1.5 Tage	3 Tage	3.5 Tage	4 Tage	5.5 Tage	6 Tage

DDP16

SG5760 → SG5760

Geschwindigkeit der Netzwerkschnittstelle	Größe des 4-TB-Laufwerks	8-TB-Laufwerke	10-TB-Laufwerkgröße	12-TB-Laufwerksgröße	16-TB-Laufwerkgröße	18 TB Laufwerksgröße
10 GBIT	3.5 Tage	6.5 Tage	8 Tage	9.5 Tage	12.5 Tage	**14 Tage**
25 GB	3.5 Tage	6.5 Tage	8 Tage	9.5 Tage	12.5 Tage	**14 Tage**

SG5760 → SG6060

Geschwindigkeit der Netzwerkschnittstelle	Größe des 4-TB-Laufwerks	8-TB-Laufwerke	10-TB-Laufwerkgröße	12-TB-Laufwerksgröße	16-TB-Laufwerkgröße	18 TB Laufwerksgröße
10 GBIT	2.5 Tage	5 Tage	6 Tage	7.5 Tage	10 Tage	11 Tage

Geschwindigkeit der Netzwerkschnittstelle	Größe des 4-TB-Laufwerks	8-TB-Laufwerke	10-TB-Laufwerkgröße	12-TB-Laufwerksgröße	16-TB-Laufwerkgröße	18 TB Laufwerksgröße
25 GB	2 Tage	3.5 Tage	4 Tage	5 Tage	6.5 Tage	7 Tage

SG6060 → SG6060

Geschwindigkeit der Netzwerkschnittstelle	Größe des 4-TB-Laufwerks	8-TB-Laufwerke	10-TB-Laufwerkgröße	12-TB-Laufwerksgröße	16-TB-Laufwerkgröße	18 TB Laufwerksgröße
10 GBIT	3.5 Tage	5 Tage	6 Tage	7 Tage	9.5 Tage	10.5 Tage
25 GB	2 Tage	3 Tage	4 Tage	4.5 Tage	6 Tage	7 Tage

Erweiterungs-Shelf (oberhalb von SG6060 für jedes Shelf in der Quell-Appliance hinzufügen)

Geschwindigkeit der Netzwerkschnittstelle	Größe des 4-TB-Laufwerks	8-TB-Laufwerke	10-TB-Laufwerkgröße	12-TB-Laufwerksgröße	16-TB-Laufwerkgröße	18 TB Laufwerksgröße
10 GBIT	3.5 Tage	5 Tage	6 Tage	7 Tage	9.5 Tage	10.5 Tage
25 GB	2 Tage	3 Tage	4 Tage	4.5 Tage	6 Tage	7 Tage

Von Aron Klein

So verwenden Sie die Port-Neuzuordnung

Möglicherweise müssen Sie einen eingehenden oder ausgehenden Port aus mehreren Gründen neu zuordnen. Möglicherweise wechseln Sie vom älteren CLB Load Balancer-Dienst zum aktuellen nginx Service Load Balancer-Endpunkt und behalten denselben Port bei, um die Auswirkungen auf Clients zu reduzieren. Sie möchten Port 443 für Client S3 in einem Client-Netzwerk des Admin-Knotens oder für Firewall-Einschränkungen verwenden.

Migrieren Sie S3-Clients von CLB auf NGINX mit Port-Neuzuordnung

In Versionen vor StorageGRID 11.3 ist der Verbindungs-Lastausgleich (CLB) der enthaltene Load Balancer auf den Gateway-Nodes. Im StorageGRID 11.3 stellt NetApp den NGINX-Service als funktionsreiche integrierte Lösung für den Lastausgleich von HTTP(s) Traffic vor. Da der CLB-Dienst in der aktuellen Version von StorageGRID verfügbar bleibt, können Sie Port 8082 nicht in der neuen Endpunktkonfiguration des Load Balancer wiederverwenden. Um dies zu umgehen, wird der eingehende Port 8082 erneut 10443 zugeordnet. Dadurch werden alle HTTPS-Anfragen an Port 8082 des Gateways an Port 10443 umgeleitet, wobei der CLB-Dienst umgangen und stattdessen eine Verbindung zum NGINX-Dienst hergestellt wird. Obwohl die folgenden Anweisungen für VMware gelten, ist die FUNKTION PORT_REMAP für alle Installationsmethoden vorhanden, und Sie können einen ähnlichen Prozess für Bare-Metal-Bereitstellungen und -Appliances verwenden.

Implementierung von VMware Virtual Machine Gateway Node

Die folgenden Schritte gelten für eine StorageGRID-Bereitstellung, bei der der Gateway-Knoten oder -Knoten in VMware vSphere 7 als VMs mit dem StorageGRID Open Virtualization Format (OVF) bereitgestellt werden. Der Prozess beinhaltet das zerstörerische Entfernen der VM und die erneute Bereitstellung der VM mit demselben Namen und derselben Konfiguration. Bevor Sie die VM einschalten, ändern Sie die vApp-Eigenschaft, um den Port neu zuzuordnen, schalten Sie die VM ein und folgen Sie dem Wiederherstellungsprozess für den Knoten.

Voraussetzungen

- Sie verwenden StorageGRID 11.3 oder höher
- Sie haben heruntergeladen und haben Zugriff auf die installierten VMware-Installationsdateien der StorageGRID-Version.
- Sie haben ein vCenter Konto mit Berechtigungen zum ein-/Ausschalten von VMs, Ändern der Einstellungen der VMs und vApps, Entfernen von VMs aus vCenter und Bereitstellen von VMs durch OVF.
- Sie haben einen Load Balancer-Endpunkt erstellt
  - Der Port ist für den gewünschten Umleitungsport konfiguriert
  - Das Endpunkt-SSL-Zertifikat ist dasselbe wie für den CLB-Dienst im Serverzertifikat für Konfiguration/Serverzertifikate/Objekt-Storage-API-Dienst installiert, oder der Client kann eine Änderung des Zertifikats akzeptieren.

> ⓘ
>
> ```
> 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.
> ```

Zerstören Sie den ersten Gateway-Node

Gehen Sie wie folgt vor, um den ersten Gateway-Node zu zerstören:

1. Wählen Sie den Gateway Node aus, mit dem Sie beginnen möchten, wenn das Grid mehr als einen enthält.
2. Entfernen Sie die Node-IPs von allen DNS-Round-Robin-Entitäten oder Load-Balancer-Pools, falls zutreffend.
3. Warten Sie, bis Time-to-Live (TTL) und geöffnete Sitzungen ablaufen.
4. Schalten Sie den VM-Knoten aus.
5. Entfernen Sie den VM-Node von der Festplatte.

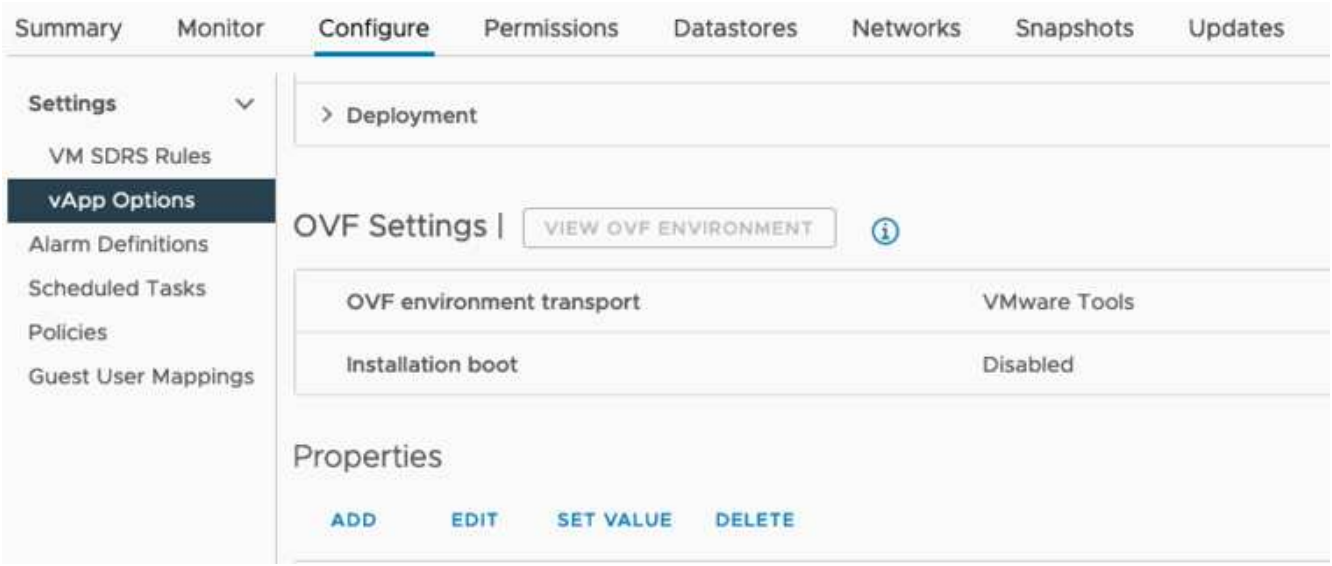
Implementieren Sie den Ersatz-Gateway-Node

Gehen Sie wie folgt vor, um den Ersatz-Gateway-Node bereitzustellen:

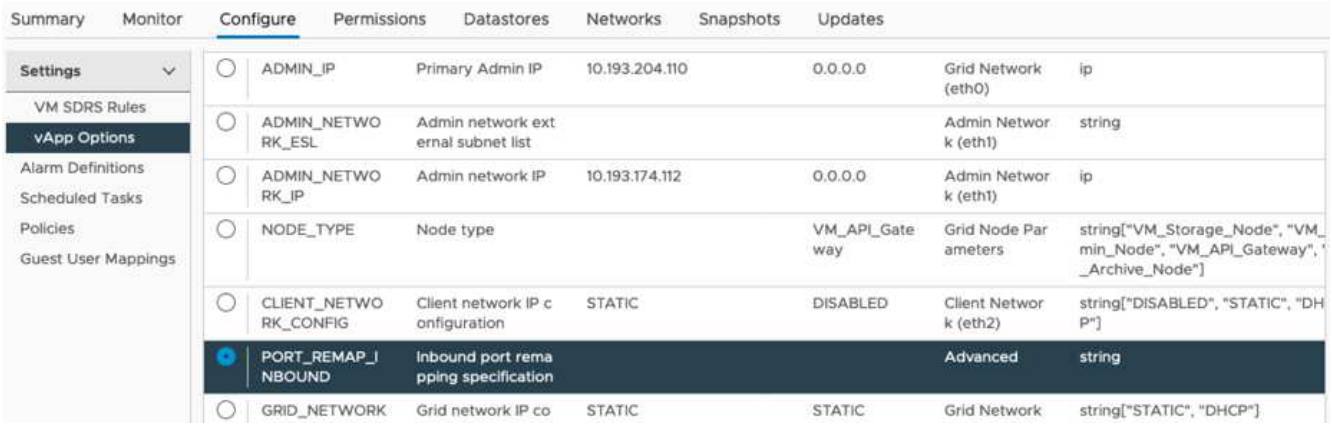
1. Implementieren Sie die neue VM über OVF, und wählen Sie die Dateien .ovf, .MF und .vmdk aus dem von der Support-Website heruntergeladenen Installationspaket aus:
   - vsphere-Gateway.MF
   - vsphere-Gateway.ovf

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

2. Nachdem die VM bereitgestellt wurde, wählen Sie sie aus der Liste der VMs aus und wählen Sie die Registerkarte Konfigurieren vApp Options aus.



3. Blättern Sie nach unten zum Abschnitt Eigenschaften, und wählen Sie die Eigenschaft PORT_REMAP_INBOUND aus

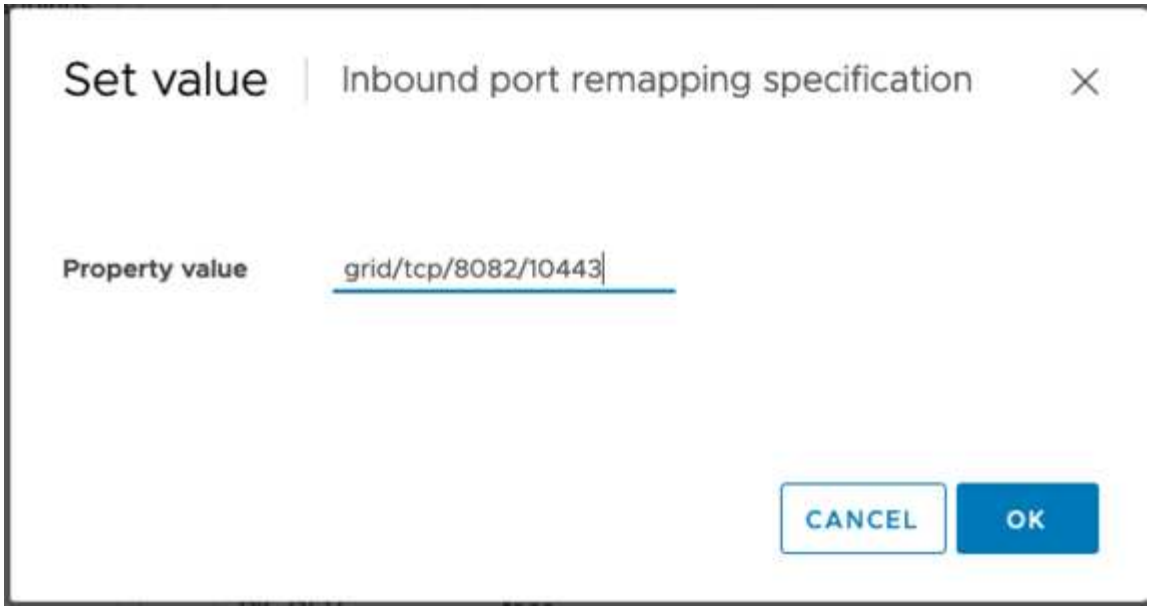


4. Blättern Sie nach oben in der Liste Eigenschaften, und klicken Sie auf Bearbeiten

5. Wählen Sie die Registerkarte Typ aus, bestätigen Sie, dass das Kontrollkästchen Benutzerkonfigurierbar aktiviert ist, und klicken Sie dann auf Speichern.

6. Klicken Sie oben in der Liste Eigenschaften, wenn die Eigenschaft „PORT_REMAP_INBOUND“ noch ausgewählt ist, auf Wert festlegen.

7. Geben Sie im Feld Eigenschaftswert das Netzwerk (Grid, admin oder Client), TCP, den ursprünglichen Port (8082) und den neuen Port (10443) mit „/“ zwischen den einzelnen Werten ein, wie nachfolgend dargestellt.

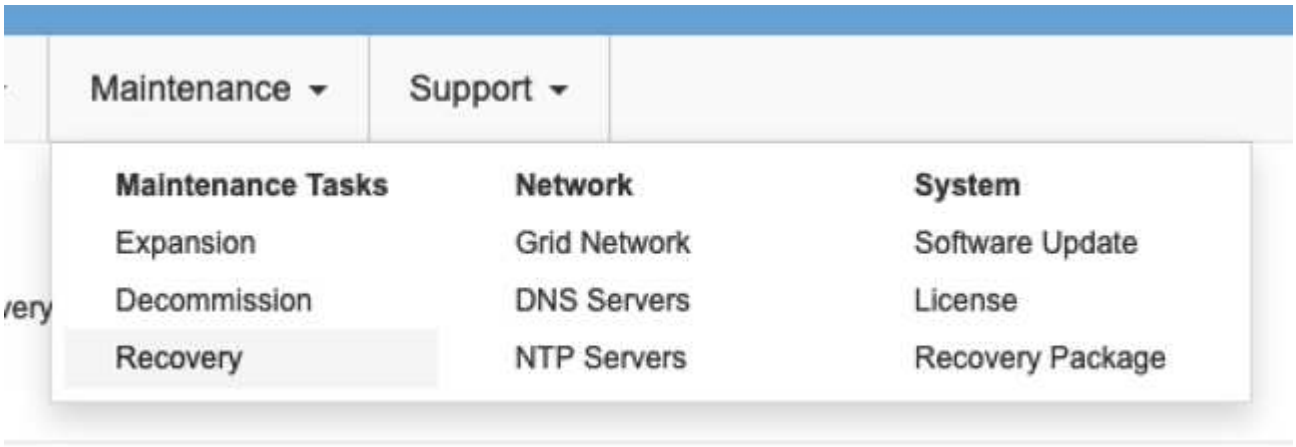


8. Wenn Sie mehrere Netzwerke verwenden, trennen Sie die Netzwerkzeichenfolgen mit einem Komma (,), z. B. GRID/tcp/8082/10443,admin/tcp/8082/10443,Client/tcp/8082/10443

Stellen Sie den Gateway-Node wieder her

Gehen Sie wie folgt vor, um den Gateway-Node wiederherzustellen:

1. Navigieren Sie zum Abschnitt Wartung/Wiederherstellung der Grid Management-Benutzeroberfläche.



2. Schalten Sie den VM-Knoten ein, und warten Sie, bis der Knoten im Abschnitt Wartung/Wiederherstellung ausstehender Knoten der Grid Management-Benutzeroberfläche angezeigt wird.

> 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. Nachdem der Node wiederhergestellt wurde, kann die IP in alle DNS-Round-Robin-Einheiten oder, falls zutreffend, in Load-Balancer-Pools enthalten sein.

   Jetzt gehen alle HTTPS-Sitzungen auf Port 8082 zu Port 10443

Port 443 für den Client-S3-Zugriff auf einen Admin-Node neu zuordnen

Die Standardkonfiguration im StorageGRID-System für einen Admin-Node oder eine HA-Gruppe mit einem Admin-Node lautet, dass Port 443 und 80 für die Management- und Mandantenmanager-UI reserviert werden und nicht für Load Balancer-Endpunkte verwendet werden können. Die Lösung hierfür besteht darin, die Funktion zur Portzuordnung zu verwenden und den eingehenden Port 443 an einen neuen Port weiterzuleiten, der als Load Balancer-Endpunkt konfiguriert wird. Sobald der Client-S3-Datenverkehr abgeschlossen ist, kann Port 443 verwendet werden, die Grid-Management-UI ist nur über Port 8443 zugänglich, und die Mandantenmanagement-UI ist nur über Port 9443 zugänglich. Die Neuzuordnungsfunktion kann nur zum Installationszeitpunkt des Node konfiguriert werden. Um eine Port-Neuzuordnung eines aktiven Node im Grid zu implementieren, muss dieser auf den vorinstallierten Status zurückgesetzt werden. Dies ist ein destruktives Verfahren, das nach Durchführung der Konfigurationsänderung eine Recovery des Node einschließt.

Backup-Protokolle und Datenbanken

Administrator-Nodes enthalten Audit-Protokolle, prometheus-Kennzahlen sowie Verlaufsinformationen zu Attributen, Alarmen und Alarmen. Bei mehreren Administrator-Nodes haben Sie mehrere Kopien dieser Daten. Wenn sich in dem Grid nicht mehrere Administrator-Nodes befinden, sollten Sie diese Daten zur Wiederherstellung beibehalten, nachdem der Node nach Abschluss dieses Prozesses wiederhergestellt wurde. Wenn sich in Ihrem Grid ein anderer Administrator-Node befindet, können Sie die Daten von diesem Node während des Recovery-Prozesses kopieren. Wenn sich kein weiterer Admin-Node im Raster befindet, können Sie die Daten vor dem Zerstören des Node anhand der folgenden Anweisungen kopieren.

Prüfprotokolle kopieren

1. Melden Sie sich beim Admin-Knoten an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
   b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`

d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

e. Fügen Sie den SSH-privaten Schlüssel zum SSH-Agenten hinzu. Geben Sie Ein: `ssh-add`

f. Geben Sie das SSH-Zugriffspasswort ein, das im aufgeführt ist `Passwords.txt` Datei:

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

2. Erstellen Sie das Verzeichnis, um alle Audit-Log-Dateien an einen temporären Speicherort auf einem separaten Grid-Knoten zu kopieren. Verwenden Sie *Storage_Node_01*:

a. `ssh admin@storage_node_01_IP`

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

3. Beenden Sie den AMS-Dienst wieder auf dem Admin-Knoten, um zu verhindern, dass er eine neue Protokolldatei erstellt: `service ams stop`

4. Benennen Sie die Datei audit.log um, damit sie die vorhandene Datei nicht überschreiben kann, wenn Sie sie in den wiederhergestellten Admin-Node kopieren.

a. Benennen Sie audit.log in einen eindeutigen nummerierten Dateinamen um, z. B. yyyy-mm-dd.txt.1. Sie können beispielsweise die Audit-Log-Datei in 2015-10-25.txt.1 umbenennen

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

5. AMS-Dienst neu starten: `service ams start`

6. Alle Audit-Log-Dateien kopieren: `scp * admin@storage_node_01_IP:/var/local/tmp/saved-audit-logs`

Kopieren Sie Prometheus Daten

Das Kopieren der Prometheus-Datenbank dauert möglicherweise ein Stunde oder länger. Einige Grid Manager-Funktionen sind nicht verfügbar, während Dienste auf dem Admin-Knoten angehalten werden.

1. Erstellen Sie das Verzeichnis, um die prometheus-Daten an einen temporären Speicherort auf einem separaten Grid-Knoten zu kopieren, auch hier wird *Storage_Node_01* verwendet:

a. Melden Sie sich beim Speicher-Node an:

i. Geben Sie den folgenden Befehl ein: `ssh admin@storage_node_01_IP`

ii. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

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

2. Melden Sie sich beim Admin-Knoten an:

a. Geben Sie den folgenden Befehl ein: `ssh admin@admin_node_IP`

b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`

d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

e. Fügen Sie den SSH-privaten Schlüssel zum SSH-Agenten hinzu. Geben Sie Ein: `ssh-add`

f. Geben Sie das SSH-Zugriffspasswort ein, das im aufgeführt ist `Passwords.txt` Datei:

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

3. Halten Sie vom Admin-Knoten den Prometheus-Service an: `service prometheus stop`

   a. Prometheus-Datenbank vom Quell-Admin-Node auf den Speicher-Node-Backup-Speicherort kopieren Knoten: `/rsync -azh --stats "/var/local/mysql_ibdata/prometheus/data" "`*`storage_node_01_IP`*`:/var/local/tmp/prometheus/"`

4. Starten Sie den Prometheus-Service auf dem Quell-Admin-Node neu.`service prometheus start`

Sichern Sie Verlaufsinformationen

Die historischen Informationen werden in einer mysql-Datenbank gespeichert. Um eine Kopie der Datenbank abzuladen, benötigen Sie den Benutzer und das Passwort von NetApp. Wenn sich in der Tabelle ein weiterer Admin-Node befindet, ist dieser Schritt nicht erforderlich. Die Datenbank kann während der Recovery von einem verbleibenden Admin-Node geklont werden.

1. Melden Sie sich beim Admin-Knoten an:

   a. Geben Sie den folgenden Befehl ein: `ssh admin@`*`admin_node_IP`*

   b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

   c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`

   d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

   e. Fügen Sie den SSH-privaten Schlüssel zum SSH-Agenten hinzu. Geben Sie Ein: `ssh-add`

   f. Geben Sie das SSH-Zugriffspasswort ein, das im aufgeführt ist `Passwords.txt` Datei:

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

2. Stoppen Sie StorageGRID-Dienste auf Admin-Knoten und starten sie ntp und mysql

   a. Beenden Sie alle Dienste: `service servermanager stop`

   b. Starten Sie den ntp-Service neu: `service ntp start`..Neustart mysql-Dienst: `service mysql start`

3. Dump mi-Datenbank in /var/local/tmp

   a. Geben Sie den folgenden Befehl ein: `mysqldump –u `*`username`*` –p `*`password`*` mi > /var/local/tmp/mysql-mi.sql`

4. Kopieren Sie die mysql Dump-Datei auf einen alternativen Knoten, wir verwenden *Storage_Node_01: `scp /var/local/tmp/mysql-mi.sql _storage_node_01_IP`:/var/local/tmp/mysql-mi.sql*

a. Wenn Sie keinen passwortlosen Zugriff auf andere Server mehr benötigen, entfernen Sie den privaten Schlüssel vom SSH-Agent. Geben Sie Ein: `ssh-add -D`

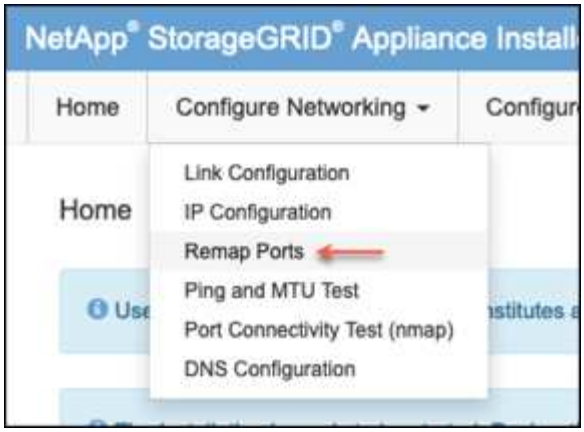
Erstellen Sie den Admin-Knoten neu

Nachdem Sie nun über eine Backup-Kopie aller gewünschten Daten und Protokolle verfügen, die sich entweder auf einem anderen Admin-Node im Grid oder an einem temporären Speicherort befinden, ist es an der Zeit, die Appliance zurückzusetzen, damit die Port-Neuzuordnung konfiguriert werden kann.

1. Wenn Sie eine Appliance zurücksetzen, wird sie in den vorinstallierten Zustand zurückversetzt, wobei nur der Hostname, die IP-Adressen und die Netzwerkkonfigurationen beibehalten werden. Alle Daten gehen verloren, weshalb wir dafür gesorgt haben, dass alle wichtigen Informationen gesichert sind.
   a. Geben Sie den folgenden Befehl ein: `sgareinstall`

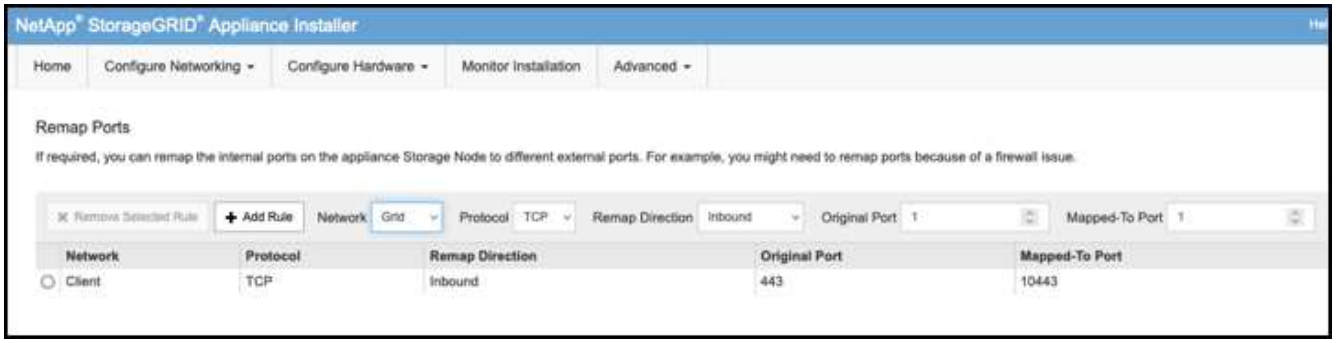
```
root@sg100-01:~ # sgareinstall
WARNING: All StorageGRID Webscale services on this node will be shut
down.
WARNING: Data stored on this node may be lost.
WARNING: You will have to reinstall StorageGRID Webscale to this
node.

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. Nach einiger Zeit wird die Appliance neu gestartet, und Sie können auf die Knoten-PGE-Benutzeroberfläche zugreifen.
3. Navigieren Sie zum Fenster Netzwerk konfigurieren



4. Wählen Sie das gewünschte Netzwerk, Protokoll, Richtung und Ports aus, und klicken Sie dann auf die Schaltfläche Regel hinzufügen.

> Die Neuzuordnung von eingehendem Port 443 auf dem GRID-Netzwerk bricht die Installation und die Erweiterungsverfahren ab. Es wird nicht empfohlen, Port 443 im NETZNETZWERK neu zuzuordnen.



5. Eine der gewünschten Port-Neuzuordnungen wurde hinzugefügt. Sie können zur Registerkarte „Home“ zurückkehren und auf die Schaltfläche „Installation starten“ klicken.

Sie können nun die Wiederherstellungsverfahren für den Admin-Knoten in befolgen "Produktdokumentation"

Wiederherstellung von Datenbanken und Protokollen

Nach der Wiederherstellung des Admin-Node können Sie nun die Metriken, Protokolle und Verlaufsinformationen wiederherstellen. Wenn sich ein anderer Administrator-Node im Raster befindet, folgen Sie den Anweisungen "Produktdokumentation" Verwenden der Skripte *prometheus-Clone-db.sh* und *mi-Clone-db.sh*. Wenn dies der einzige Admin-Node ist und Sie diese Daten sichern möchten, können Sie die folgenden Schritte ausführen, um die Informationen wiederherzustellen.

Kopieren Sie die Prüfprotokolle zurück

1. Melden Sie sich beim Admin-Knoten an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
   b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
   c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
   d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

e. Fügen Sie den SSH-privaten Schlüssel zum SSH-Agenten hinzu. Geben Sie Ein: `ssh-add`

f. Geben Sie das SSH-Zugriffspasswort ein, das im aufgeführt ist `Passwords.txt` Datei:

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

2. Kopieren Sie die erhaltenen Audit-Log-Dateien auf den wiederhergestellten Admin-Knoten: `scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY* .`
3. Löschen Sie aus Sicherheitsgründen die Prüfprotokolle vom fehlgeschlagenen Grid-Knoten, nachdem Sie überprüft haben, ob sie erfolgreich auf den wiederhergestellten Admin-Node kopiert wurden.
4. Aktualisieren Sie die Benutzer- und Gruppeneinstellungen der Audit-Log-Dateien auf dem wiederhergestellten Admin-Knoten: `chown ams-user:bycast *`

Sie müssen auch alle bereits vorhandenen Clientzugriffe auf die Revisionsfreigabe wiederherstellen. Weitere Informationen finden Sie in den Anweisungen zum Verwalten von StorageGRID.

Restore von Prometheus Kennzahlen

> Das Kopieren der Prometheus-Datenbank dauert möglicherweise ein Stunde oder länger. Einige Grid Manager-Funktionen sind nicht verfügbar, während Dienste auf dem Admin-Knoten angehalten werden.

1. Melden Sie sich beim Admin-Knoten an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
   b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
   c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
   d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
   e. Fügen Sie den SSH-privaten Schlüssel zum SSH-Agenten hinzu. Geben Sie Ein: `ssh-add`
   f. Geben Sie das SSH-Zugriffspasswort ein, das im aufgeführt ist `Passwords.txt` Datei:

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

2. Halten Sie vom Admin-Knoten den Prometheus-Service an: `service prometheus stop`
   a. Kopieren Sie die Prometheus Datenbank vom Speicherort für temporäre Backups auf den Admin-Node: `/rsync -azh --stats "backup_node:/var/local/tmp/prometheus/" "/var/local/mysql_ibdata/prometheus/"`
   b. Überprüfen Sie, ob sich die Daten im richtigen Pfad befinden und vollständig sind `ls /var/local/mysql_ibdata/prometheus/data/`
3. Starten Sie den Prometheus-Service auf dem Quell-Admin-Node neu.`service prometheus start`

Historische Informationen wiederherstellen

1. Melden Sie sich beim Admin-Knoten an:

a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`

b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`

d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

e. Fügen Sie den SSH-privaten Schlüssel zum SSH-Agenten hinzu. Geben Sie Ein: `ssh-add`

f. Geben Sie das SSH-Zugriffspasswort ein, das im aufgeführt ist `Passwords.txt` Datei:

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

2. Kopieren Sie die mysql-Dump-Datei vom alternativen Knoten: `scp grid_node_IP_:/var/local/tmp/mysql-mi.sql /var/local/tmp/mysql-mi.sql`
3. Stoppen Sie StorageGRID-Dienste auf Admin-Knoten und starten sie ntp und mysql
   a. Beenden Sie alle Dienste: `service servermanager stop`
   b. Starten Sie den ntp-Service neu: `service ntp start`..Neustart mysql-Dienst: `service mysql start`
4. Legen Sie die mi-Datenbank ab und erstellen Sie eine neue leere Datenbank: `mysql -u username -p password -A mi -e "drop database mi; create database mi;"`
5. Stellen Sie die mysql-Datenbank aus dem Datenbank-Dump wieder her: `mysql -u username -p password -A mi < /var/local/tmp/mysql-mi.sql`
6. Starten Sie alle anderen Dienste neu `service servermanager start`

Von Aron Klein

Standortverlagerung von Grid-Standorten und standortweites Netzwerkänderungsverfahren

Dieser Leitfaden beschreibt die Vorbereitung und das Verfahren für den Standortwechsel in einem Grid mit mehreren Standorten von StorageGRID. Sie sollten über ein vollständiges Verständnis dieser Vorgehensweise verfügen und im Voraus planen, um einen reibungslosen Prozess zu gewährleisten und Unterbrechungen für Kunden zu minimieren.

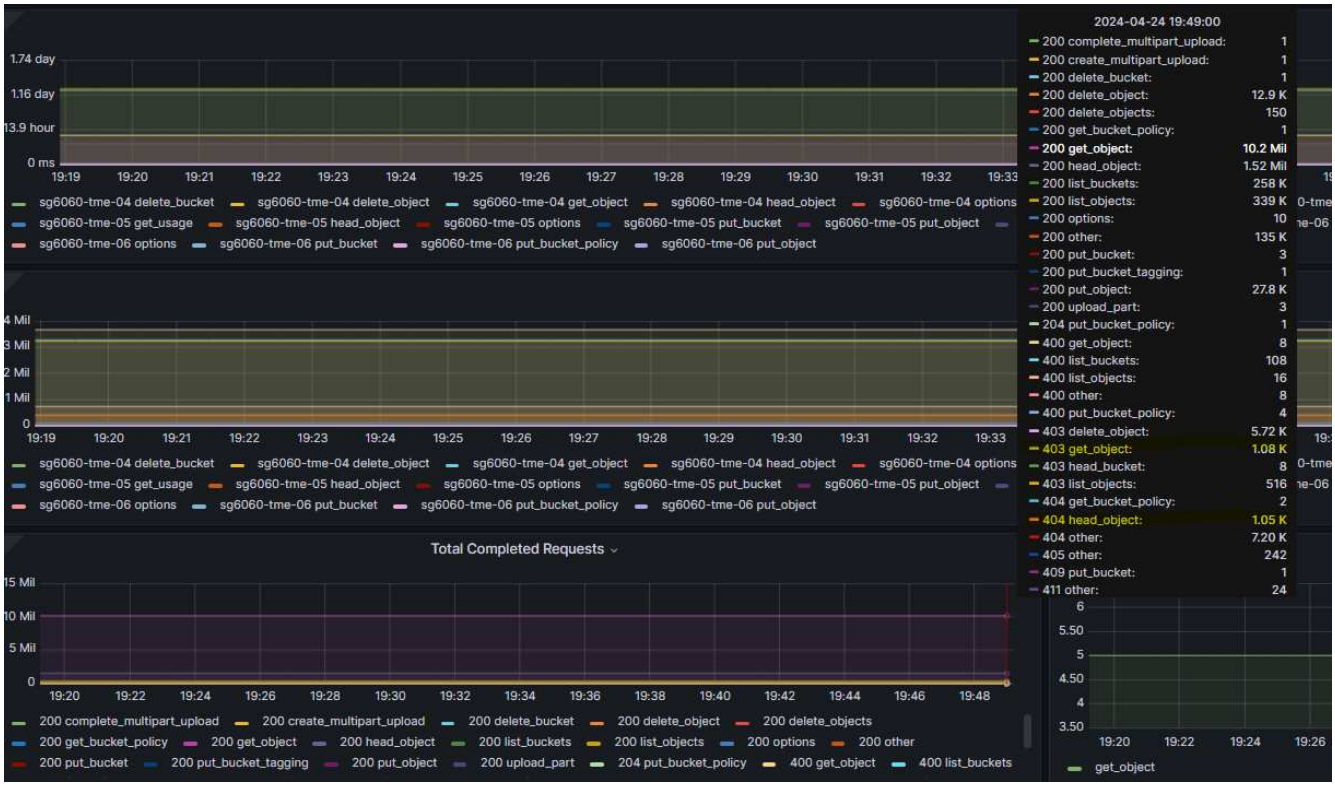
Informationen zum Ändern des Grid-Netzwerks des gesamten Grid finden Sie unter "Ändern Sie die IP-Adressen für alle Nodes im Grid".

Überlegungen vor Standortverlagerung

- Die Standortverschiebungen sollten abgeschlossen sein und alle Nodes innerhalb von 15 Tagen online sein, um eine Wiederherstellung der Cassandra-Datenbank zu vermeiden.
  "Stellen Sie Storage Node länger als 15 Tage wieder her"
- Wenn eine ILM-Regel in der aktiven Richtlinie striktes Aufnahmeverhalten verwendet, sollten Sie sie in Erwägung ziehen, um einen Ausgleich oder eine doppelte Provisionierung zu erreichen, wenn der Kunde

weiterhin Objekte im Grid bei der Standortverlagerung ABLEGEN möchte.

- Bei Storage Appliances mit 60 oder mehr Laufwerken: Verschieben Sie das Shelf niemals bei installierten Festplatten. Beschriften Sie die einzelnen Laufwerke, und entfernen Sie sie vor dem Verpacken/Verschieben aus dem Speichergehäuse.
- Ändern der StorageGRID-Appliance Grid-Netzwerk-VLAN kann Remote über das Admin-Netzwerk oder das Client-Netzwerk durchgeführt werden. Oder planen Sie, vor Ort zu sein, um die Änderung vor oder nach dem Umzug durchzuführen.
- Prüfen Sie, ob die Kundenanwendung vor dem PUT ein Objekt vom TYP HEAD oder GET Nonexistent verwendet. Wenn ja, ändern Sie die Bucket-Konsistenz in strong-site, um HTTP 500-Fehler zu vermeiden. Wenn Sie sich nicht sicher sind, überprüfen Sie die S3-Übersicht Grafana-Diagramme **Grid-Manager > Support > Metriken**, bewegen Sie die Maus über das Diagramm 'gesamte abgeschlossene Anfrage'. Wenn eine sehr hohe Anzahl von 404 get Object oder 404 Head Objects vorhanden ist, verwenden wahrscheinlich eine oder mehrere Anwendungen Head oder Get Nonexistence Objects. Die Zählung wird akkumuliert, Maus über verschiedene Zeitachse, um den Unterschied zu sehen.



Verfahren zum Ändern der Grid-IP-Adresse vor Standortverlagerung

Schritte

1. Wenn das neue Netznetz-Subnetz am neuen Standort verwendet wird, "Fügen Sie das Subnetz der Subnetzliste des Netznetzes hinzu"
2. Melden Sie sich beim primären Admin-Knoten an, verwenden Sie Change-IP, um Grid IP-Änderungen vorzunehmen, müssen Sie die Änderung * inszenieren*, bevor Sie den Knoten für die Verlagerung herunterfahren.
   a. Wählen Sie 2 und dann 1 für Grid IP-Änderung

```
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. Wählen Sie 5, um die Änderungen anzuzeigen

```
================================================================================
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
```

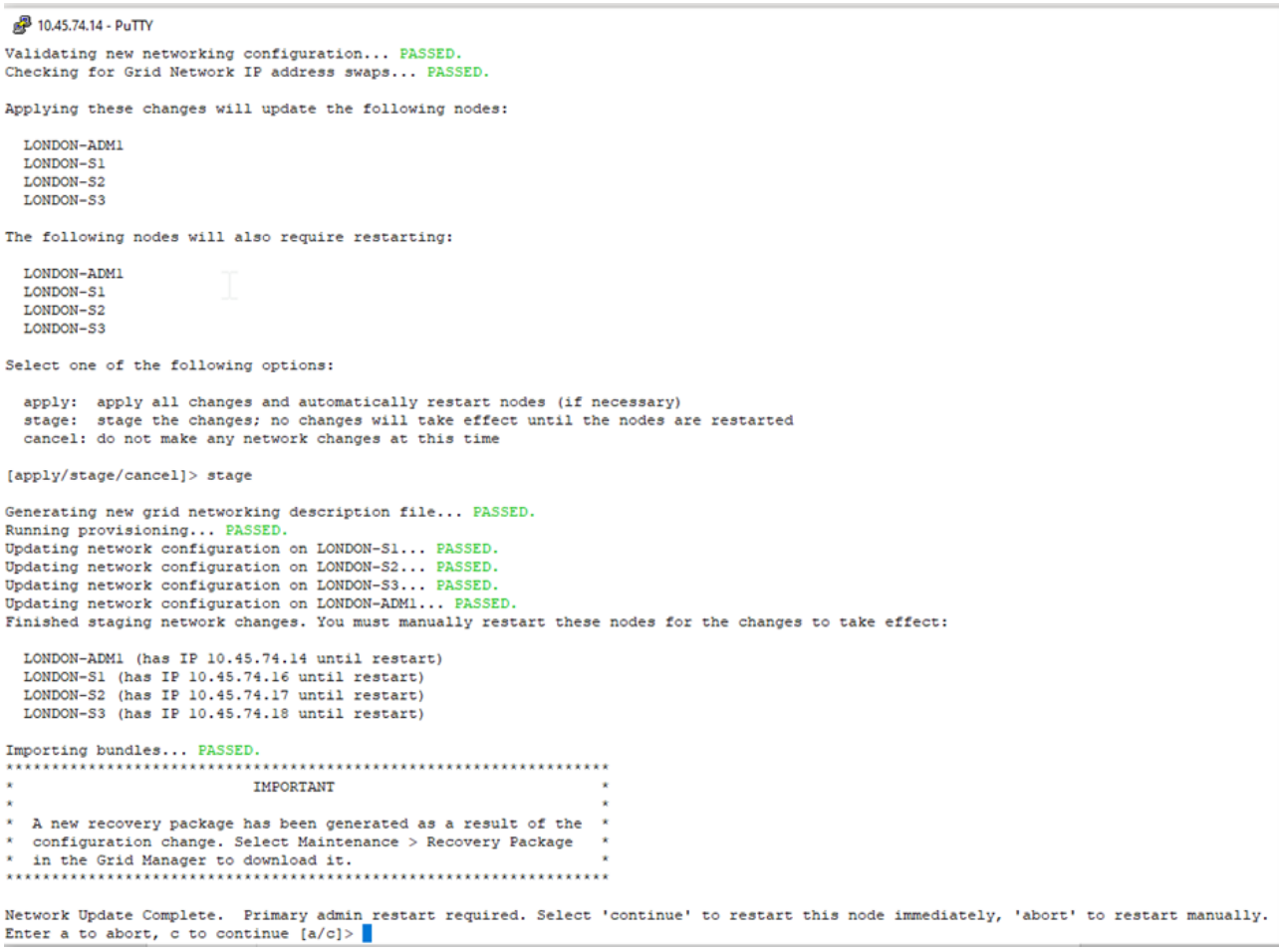
c. Wählen Sie 10, um die Änderung zu validieren und anzuwenden.

```
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
```

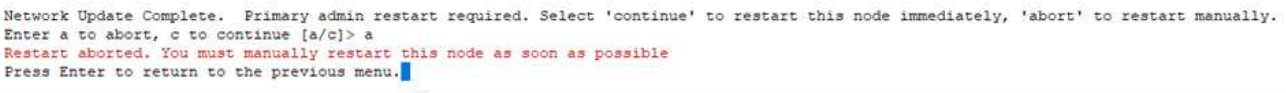
d. In diesem Schritt muss **Stufe** ausgewählt werden.

```
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. Wenn der primäre Admin-Knoten in der obigen Änderung enthalten ist, geben Sie **'a' ein, um den primären Admin-Knoten manuell neu zu starten**



f. Drücken Sie ENTER, um zum vorherigen Menü zurückzukehren und die Change-ip-Schnittstelle zu verlassen.



3. Laden Sie das neue Wiederherstellungspaket vom Grid Manager herunter. **Grid-Manager** > **Wartung** > **Recovery-Paket**
4. Wenn eine VLAN-Änderung auf der StorageGRID-Appliance erforderlich ist, lesen Sie den Abschnitt VLAN-Änderung der Appliance.
5. Fahren Sie alle Knoten und/oder Geräte am Standort herunter, kennzeichnen/entfernen Sie ggf. Festplattenlaufwerke, und entfernen Sie sie aus dem Rack, packen Sie sie aus, und verschieben Sie sie.
6. Wenn Sie die ip-Adresse des Admin-Netzwerks und/oder des Client-VLAN und der ip-Adresse ändern möchten, können Sie die Änderung nach der Verlagerung vornehmen.

VLAN-Änderung der Appliance

Bei der folgenden Vorgehensweise wird davon ausgegangen, dass Sie Remote-Zugriff auf das Admin- oder Client-Netzwerk der StorageGRID Appliance haben, um die Änderung Remote durchzuführen.

Schritte

1. Vor dem Herunterfahren des Geräts "Stellen Sie das Gerät in den Wartungsmodus".

2. Verwenden eines Browsers für den Zugriff auf die StorageGRID-Appliance-Installer-GUI mit https://<admin-or-client-network-ip>:8443. Grid IP kann nicht verwendet werden, da die neue Grid-IP bereits vorhanden ist, sobald die Appliance im Wartungsmodus gestartet wird.
3. Ändern Sie das VLAN für das Grid-Netzwerk. Wenn Sie über das Client-Netzwerk auf die Appliance zugreifen, können Sie das Client-VLAN derzeit nicht ändern. Sie können es nach dem Umzug ändern.
4. ssh zur Appliance und Herunterfahren des Node mit 'shutdoown -h now'
5. Sobald die Appliances an einem neuen Standort bereit sind, können Sie über die Benutzeroberfläche des StorageGRID-Appliance-Installationsprogramms auf zugreifen https://<grid-network-ip>:8443. Überprüfen Sie mithilfe der Ping/nmap-Tools in der GUI, ob sich der Speicher im optimalen Zustand und der Netzwerkverbindung zu anderen Grid-Nodes befindet.
6. Wenn Sie planen, die Client-Netzwerk-IP zu ändern, können Sie das Client-VLAN zu diesem Zeitpunkt ändern. Das Client-Netzwerk ist erst bereit, wenn Sie die Client-Netzwerk-ip-Adresse mit dem Change-ip-Tool in einem späteren Schritt aktualisieren.
7. Beenden Sie den Wartungsmodus. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option **Erweitert** > **Controller neu starten** aus, und wählen Sie dann **Neustart in StorageGRID** aus.
8. Wenn alle Nodes eingeschaltet sind und Grid kein Verbindungsproblem zeigt, aktualisieren Sie ggf. das Admin-Netzwerk und das Client-Netzwerk der Appliance mithilfe von Change-ip.