Guide alle funzionalità del prodotto

How to enable StorageGRID in your environment

NetApp
May 13, 2024

Sommario

Guide alle funzionalità del prodotto

Creazione di un pool di storage cloud per AWS o Google Cloud

È possibile utilizzare un pool di storage cloud se si desidera spostare gli oggetti StorageGRID in un bucket S3 esterno. Il bucket esterno può appartenere ad Amazon S3 (AWS) o Google Cloud.

Di cosa hai bisogno

- StorageGRID 11.6 è stato configurato.
- Hai già configurato un bucket S3 esterno su AWS o Google Cloud.

Fasi

1. In Grid Manager, selezionare **ILM** > **Storage Pools**.
2. Nella sezione Cloud Storage Pools della pagina, selezionare **Create**.

   Viene visualizzata la finestra a comparsa Create Cloud Storage Pool (Crea pool di storage cloud).

3. Inserire un nome visualizzato.
4. Selezionare **Amazon S3** dall'elenco a discesa Provider Type (tipo di provider).

   Questo tipo di provider funziona per AWS S3 o Google Cloud.

5. Immettere l'URI per il bucket S3 da utilizzare per il Cloud Storage Pool.

   Sono consentiti due formati:

   `https://host:port`

   `http://host:port`

6. Immettere il nome del bucket S3.

   Il nome specificato deve corrispondere esattamente al nome del bucket S3; in caso contrario, la creazione del pool di storage cloud non riesce. Non è possibile modificare questo valore dopo il salvataggio del Cloud Storage Pool.

7. Se si desidera, inserire l'ID della chiave di accesso e la chiave di accesso segreta.
8. Selezionare **non verificare certificato** dall'elenco a discesa.
9. Fare clic su **Save** (Salva).

Risultato previsto

Verificare che sia stato creato un Cloud Storage Pool per Amazon S3 o Google Cloud.

Di Jonathan Wong

Creazione di un pool di storage cloud per lo storage Azure Blob

È possibile utilizzare un pool di storage cloud se si desidera spostare gli oggetti StorageGRID in un container Azure esterno.

Di cosa hai bisogno

- StorageGRID 11.6 è stato configurato.
- Hai già configurato un container Azure esterno.

Fasi

1. In Grid Manager, selezionare **ILM** > **Storage Pools**.
2. Nella sezione Cloud Storage Pools della pagina, selezionare **Create**.

   Viene visualizzata la finestra a comparsa Create Cloud Storage Pool (Crea pool di storage cloud).

3. Inserire un nome visualizzato.
4. Selezionare **Azure Blob Storage** dall'elenco a discesa Provider Type (tipo di provider).
5. Immettere l'URI per il bucket S3 da utilizzare per il Cloud Storage Pool.

   Sono consentiti due formati:

   `https://host:port`

   `http://host:port`

6. Immettere il nome del container Azure.

   Il nome specificato deve corrispondere esattamente al nome del container Azure; in caso contrario, la creazione del pool di storage cloud non riesce. Non è possibile modificare questo valore dopo il salvataggio del Cloud Storage Pool.

7. Facoltativamente, inserire il nome account associato al container Azure e la chiave account per l'autenticazione.
8. Selezionare **non verificare certificato** dall'elenco a discesa.
9. Fare clic su **Save** (Salva).

Risultato previsto

Verificare che sia stato creato un pool di storage cloud per Azure Blob Storage.

Di Jonathan Wong

Utilizza un pool di storage cloud per il backup

È possibile creare una regola ILM per spostare gli oggetti in un Cloud Storage Pool per il backup.

Di cosa hai bisogno

- StorageGRID 11.6 è stato configurato.
- Hai già configurato un container Azure esterno.

Fasi

1. In Grid Manager, selezionare **ILM** > **Rules** > **Create**.
2. Inserire una descrizione.
3. Inserire un criterio per attivare la regola.
4. Fare clic su **Avanti**.
5. Replicare l'oggetto nei nodi di storage.
6. Aggiungere una regola di posizionamento.
7. Replicare l'oggetto nel Cloud Storage Pool
8. Fare clic su **Avanti**.
9. Fare clic su **Save** (Salva).

Risultato previsto

Verificare che il diagramma di conservazione mostri gli oggetti memorizzati localmente in StorageGRID e in un pool di storage cloud per il backup.

Verificare che, quando viene attivata la regola ILM, esista una copia nel Cloud Storage Pool ed è possibile recuperare l'oggetto localmente senza eseguire un ripristino dell'oggetto.

Di Jonathan Wong

Configurare il servizio di integrazione della ricerca StorageGRID

Questa guida fornisce istruzioni dettagliate per la configurazione del servizio di integrazione della ricerca di NetApp StorageGRID 11.6 con il servizio Amazon OpenSearch o on-premise Elasticsearch.

Introduzione

StorageGRID supporta tre tipi di servizi di piattaforma.

- **Replica di StorageGRID CloudMirror**. Eseguire il mirroring di oggetti specifici da un bucket StorageGRID a una destinazione esterna specificata.
- **Notifiche**. Notifiche di eventi per bucket per inviare notifiche su azioni specifiche eseguite su oggetti a un servizio Amazon Simple Notification Service (Amazon SNS) esterno specificato.
- **Ricerca servizio di integrazione**. Inviare metadati di oggetti Simple Storage Service (S3) a un indice Elasticsearch specificato, in cui è possibile cercare o analizzare i metadati utilizzando il servizio esterno.

I servizi della piattaforma vengono configurati dal tenant S3 tramite l'interfaccia utente di Tenant Manager. Per ulteriori informazioni, vedere "Considerazioni sull'utilizzo dei servizi della piattaforma".

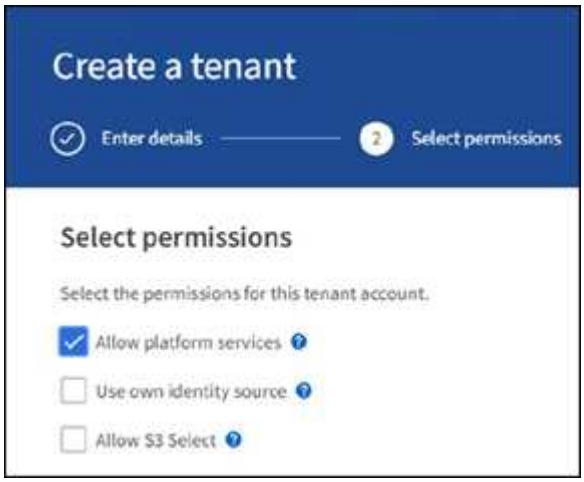
Il presente documento costituisce un'integrazione di "Guida al tenant di StorageGRID 11.6" inoltre, fornisce istruzioni dettagliate ed esempi per la configurazione di endpoint e bucket per i servizi di integrazione della ricerca. Le istruzioni di configurazione di Amazon Web Services (AWS) o on-premise Elasticsearch qui incluse

sono esclusivamente a scopo dimostrativo o di test di base.

Gli utenti devono avere familiarità con Grid Manager, il tenant manager, e avere accesso al browser S3 per eseguire operazioni di caricamento (PUT) e download (GET) di base per il test di integrazione della ricerca StorageGRID.

Creare tenant e abilitare i servizi della piattaforma

1. Creare un tenant S3 utilizzando Grid Manager, immettere un nome visualizzato e selezionare il protocollo S3.
2. Nella pagina Permission, selezionare l'opzione Allow Platform Services (Consenti servizi piattaforma). Se necessario, selezionare altre autorizzazioni.



3. Impostare la password iniziale dell'utente root tenant oppure, se l'opzione identifica federazione è attivata sulla griglia, selezionare il gruppo federated che dispone dell'autorizzazione di accesso root per configurare l'account tenant.
4. Fare clic su Accedi come root e selezionare bucket: Crea e gestisci bucket.

   Viene visualizzata la pagina del tenant manager.

5. Da Tenant Manager, selezionare My Access Keys (chiavi di accesso personali) per creare e scaricare la chiave di accesso S3 per i test successivi.

Cerca servizi di integrazione con Amazon OpenSearch

Configurazione del servizio Amazon OpenSearch (precedentemente chiamato Elasticsearch)

Utilizzare questa procedura per una configurazione rapida e semplice del servizio OpenSearch solo a scopo di test/demo. Se si utilizza on-premise Elasticsearch per i servizi di integrazione della ricerca, consultare la sezione Cerca servizi di integrazione con Elasticsearch on premise.

> Per iscriversi al servizio OpenSearch, è necessario disporre di un account di accesso alla console AWS valido, di una chiave di accesso, di una chiave di accesso segreta e dell'autorizzazione.

1. Creare un nuovo dominio utilizzando le istruzioni fornite da "Guida introduttiva al servizio AWS OpenSearch", ad eccezione di:

- Fase 4. Nome di dominio: Sgdemo
- Fase 10. Controllo degli accessi dettagliato: Deselezionare l'opzione Enable fine-Grained Access Control (attiva controllo degli accessi con grana fine).
- Fase 12. Access policy (criterio di accesso): Selezionare Configure Level Access Policy (Configura policy di accesso a livello), selezionare la scheda JSON per modificare la policy di accesso utilizzando il seguente esempio:
  - Sostituire il testo evidenziato con il proprio ID AWS Identity and Access Management (IAM) e il proprio nome utente.
  - Sostituire il testo evidenziato (l'indirizzo IP) con l'indirizzo IP pubblico del computer locale utilizzato per accedere alla console AWS.
  - Aprire una scheda del browser in "https://checkip.amazonaws.com" Per trovare l'IP pubblico.

```
{

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

Fine-grained access control

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

☐ Enable fine-grained access control

SAML authentication for OpenSearch Dashboards/Kibana

SAML authentication lets you use your existing identity provider for single sign-on for OpenSearch Dashboards/Kibana. Learn more

Prepare SAML authentication

ⓘ To use SAML authentication, you must first enable fine-grained access control.

Amazon Cognito authentication

Enable to use Amazon Cognito authentication for OpenSearch Dashboards/Kibana. Amazon Cognito supports a variety of identity providers for username-password authentication. Learn more

☐ Enable Amazon Cognito authentication

Access policy

Access policies control whether a request is accepted or rejected when it reaches the Amazon OpenSearch Service domain. If you specify an account, user, or role in this policy, you must sign your requests. Learn more

Domain access policy

○ Only use fine-grained access control
Allow open access to the domain.

○ Do not set domain level access policy
All requests to the domain will be denied.

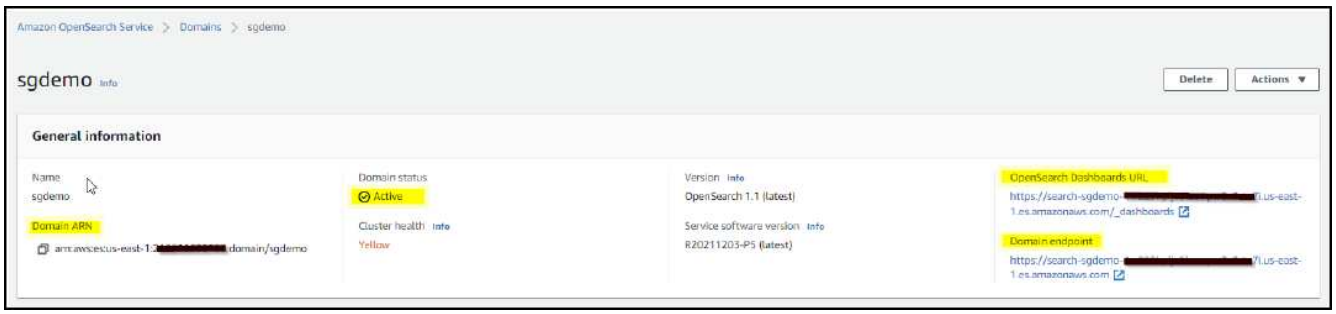
◉ Configure domain level access policy

Visual editor | JSON | Import policy

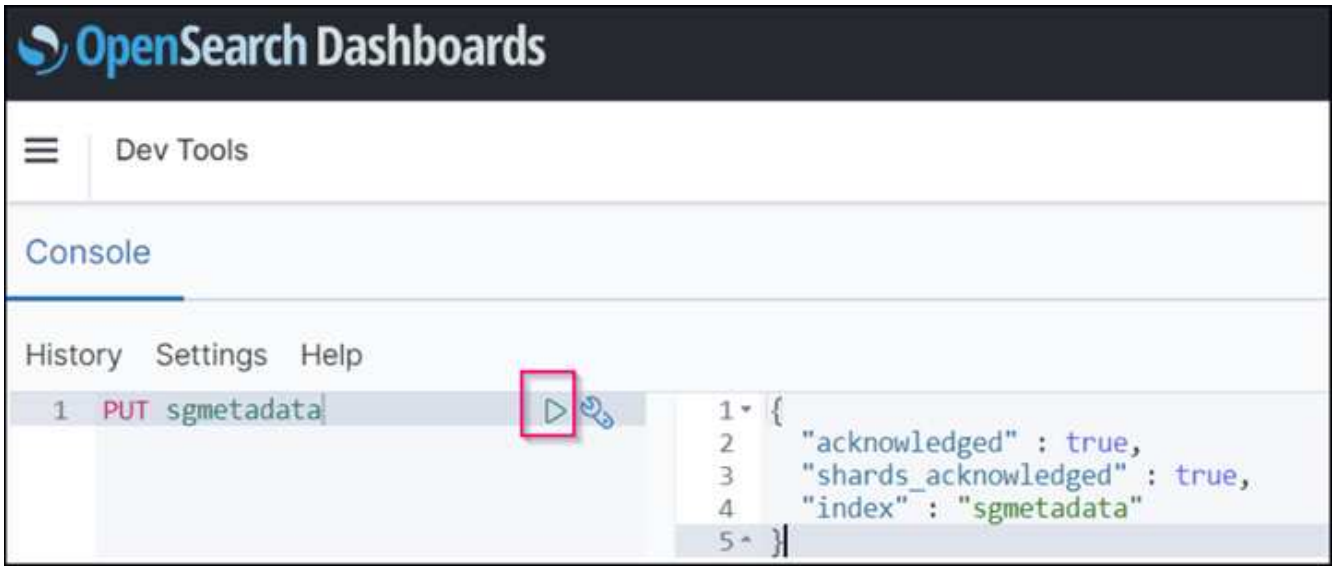
Access policy

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

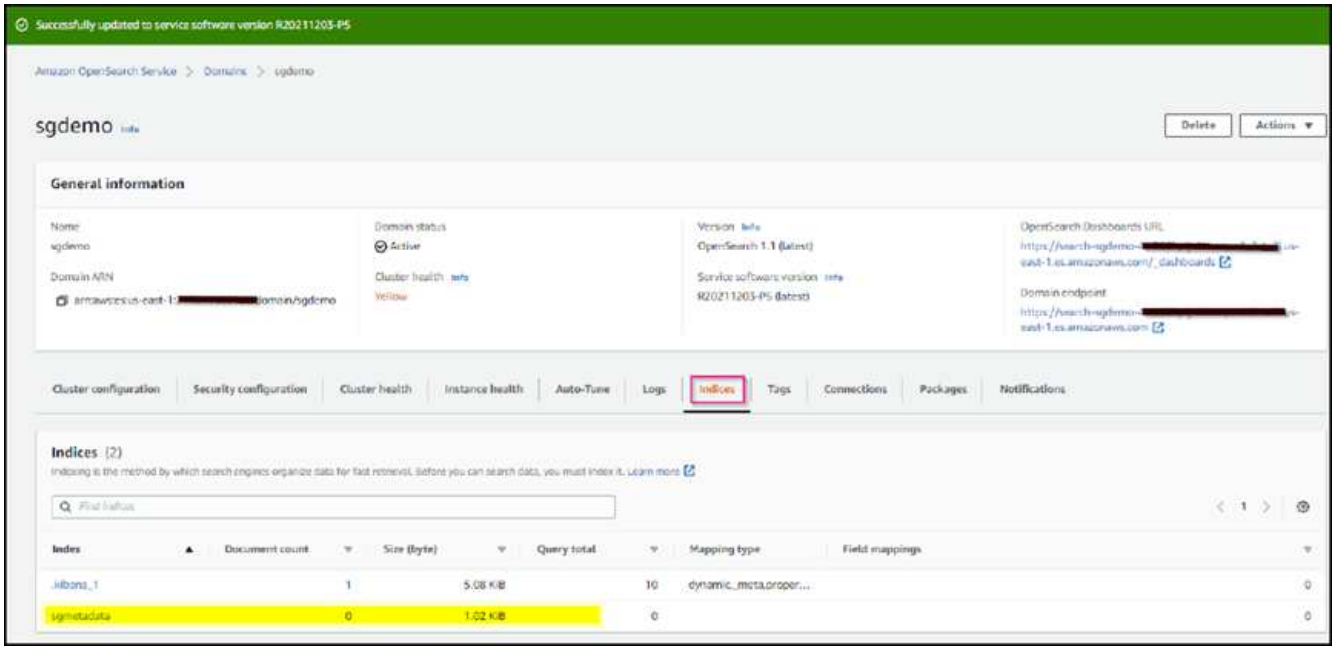
2. Attendere da 15 a 20 minuti per attivare il dominio.



3. Fare clic su OpenSearch Dashboards URL (URL dashboard OpenSearch) per aprire il dominio in una nuova scheda e accedere alla dashboard. Se viene visualizzato un errore di accesso negato, verificare che l'indirizzo IP di origine del criterio di accesso sia impostato correttamente sull'IP pubblico del computer per consentire l'accesso alla dashboard del dominio.
4. Nella pagina di benvenuto della dashboard, selezionare Esplora da solo. Dal menu, selezionare Management (Gestione) → Dev Tools (Strumenti di sviluppo)
5. In Strumenti di sviluppo → Console , immettere `PUT <index>` Dove si utilizza l'indice per memorizzare i metadati degli oggetti StorageGRID. Nell'esempio seguente viene utilizzato il nome dell'indice "sgmetadata". Fare clic sul piccolo simbolo del triangolo per eseguire IL comando PUT. Il risultato previsto viene visualizzato sul pannello di destra, come mostrato nella seguente schermata di esempio.



6. Verificare che l'indice sia visibile dall'interfaccia utente di Amazon OpenSearch in sgdomain > indici.

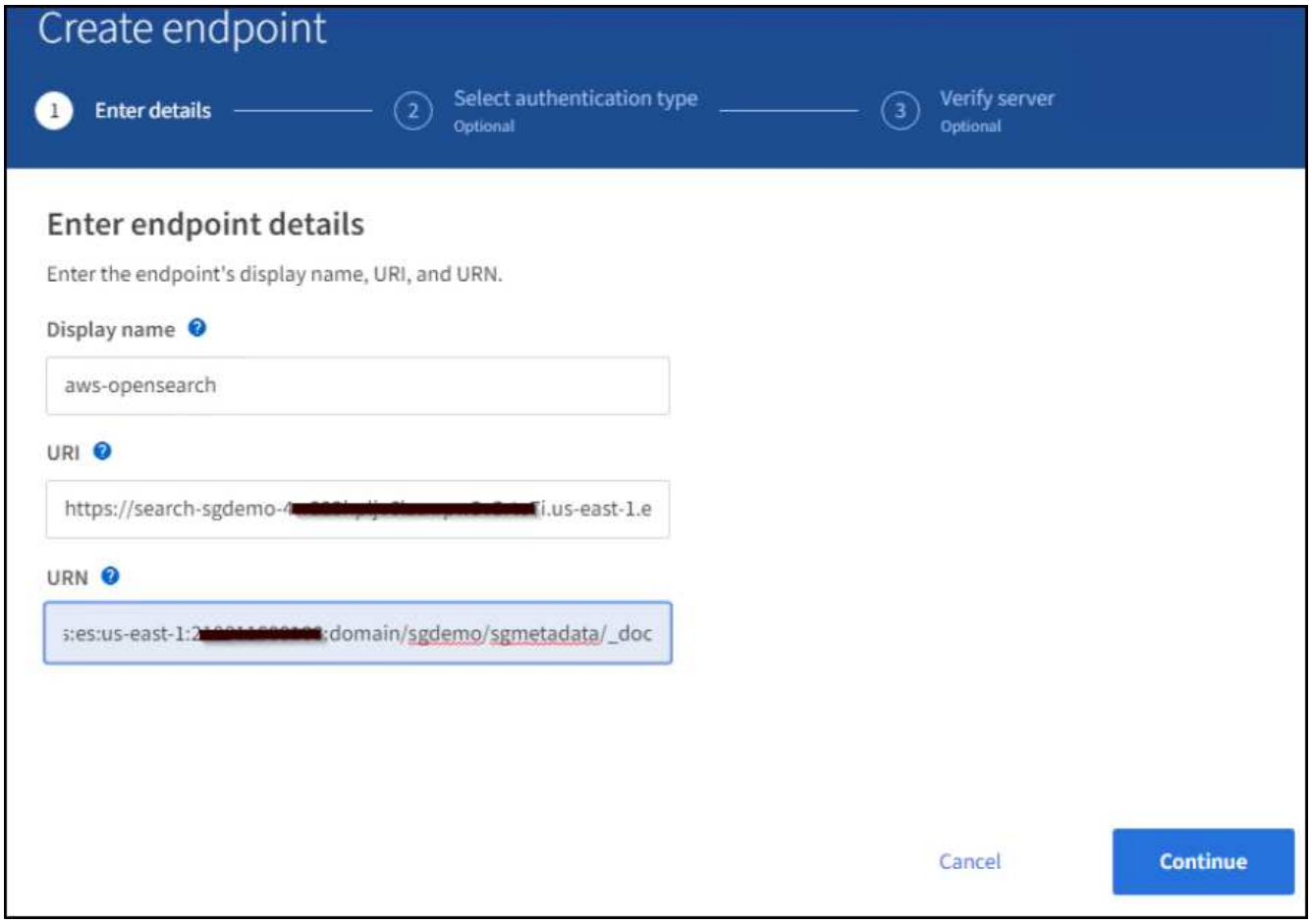


Configurazione degli endpoint dei servizi della piattaforma

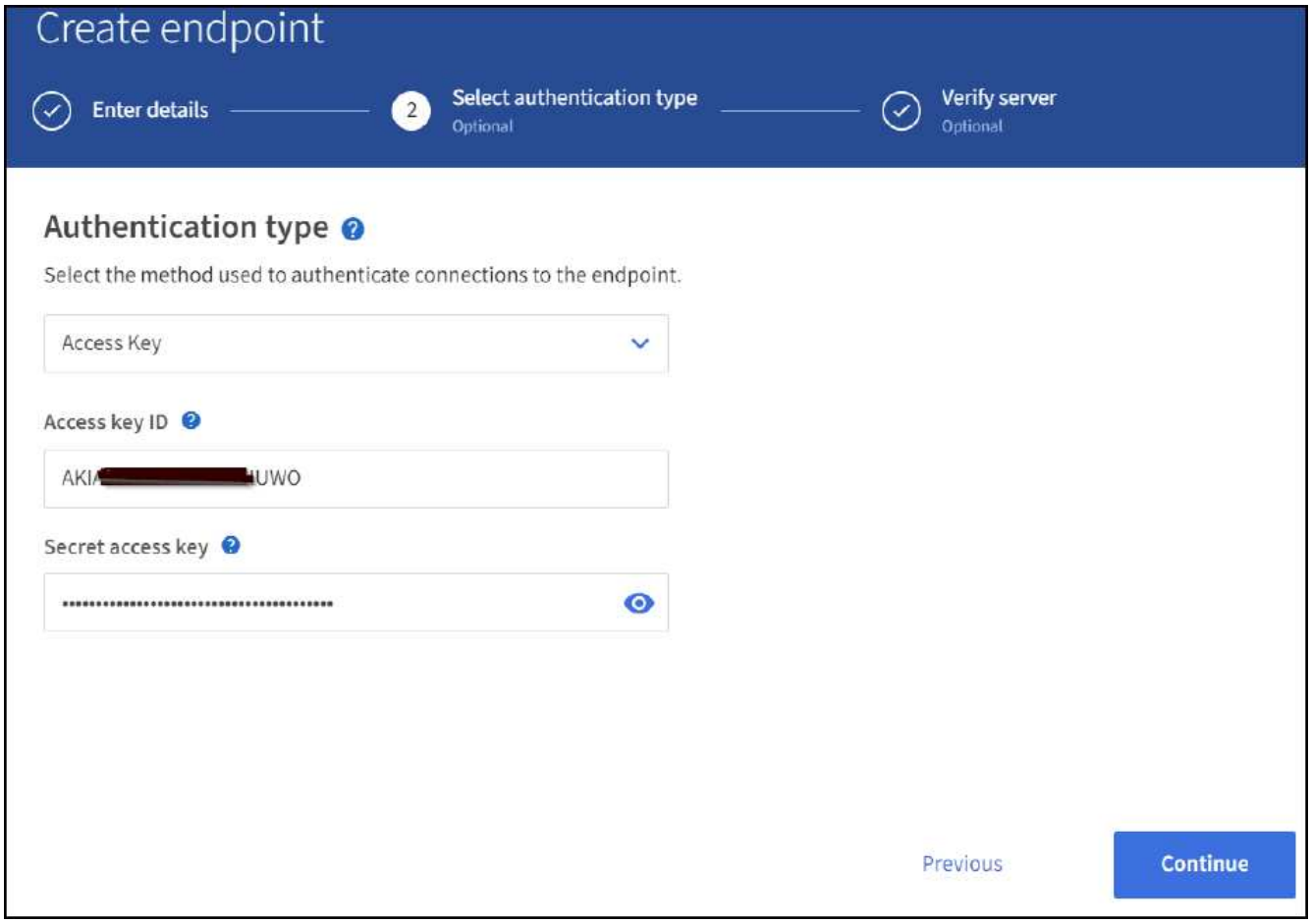
Per configurare gli endpoint dei servizi della piattaforma, attenersi alla seguente procedura:

1. In Tenant Manager, andare a STORAGE(S3) > Platform Services Endpoint.
2. Fare clic su Create Endpoint (Crea endpoint), immettere quanto segue, quindi fare clic su Continue (continua):
    - Esempio di nome visualizzato `aws-opensearch`
    - L'endpoint di dominio nella schermata di esempio nella fase 2 della procedura precedente nel campo URI.
    - Il dominio ARN utilizzato nella fase 2 della procedura precedente nel campo URN e aggiungere `/<index>/_doc` Alla fine di ARN.

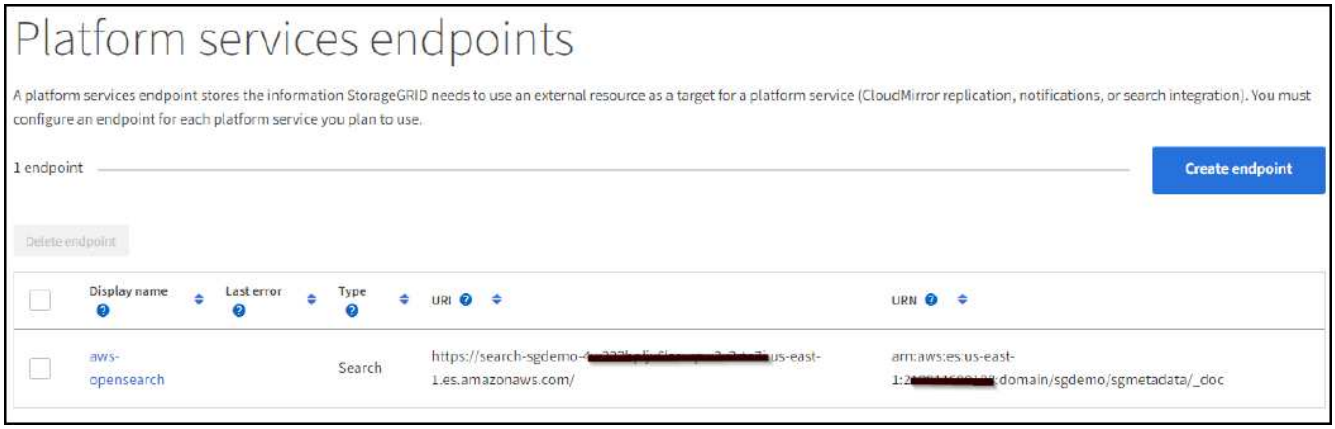
      In questo esempio, URN diventa `arn:aws:es:us-east-1:211234567890:domain/sgdemo/sgmedata/_doc`.



3. Per accedere a Amazon OpenSearch sgdomain, scegli Access Key come tipo di autenticazione, quindi inserisci la chiave di accesso Amazon S3 e la chiave segreta. Per passare alla pagina successiva, fare clic su Continue (continua).



4. Per verificare l'endpoint, selezionare Use Operating System CA Certificate and Test (Usa certificato CA del sistema operativo e test) e Create Endpoint (Crea endpoint). Se la verifica ha esito positivo, viene visualizzata una schermata dell'endpoint simile alla seguente figura. Se la verifica non riesce, verificare che l'URN includa `/<index>/_doc` Alla fine del percorso, la chiave di accesso AWS e la chiave segreta sono corrette.



Cerca servizi di integrazione con Elasticsearch on premise

Configurazione di Elasticsearch on premise

Questa procedura è per una rapida configurazione di on premise Elasticsearch e Kibana utilizzando docker solo a scopo di test. Se il server Elasticsearch e Kibana esiste già, passare alla fase 5.

1. Seguire questa procedura "Procedura di installazione di Docker" per installare docker. Utilizziamo il "Procedura di installazione di CentOS Docker" in questa configurazione.

```
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
```

   - Per avviare docker dopo il riavvio, immettere quanto segue:

```
sudo systemctl enable docker
```

   - Impostare `vm.max_map_count` valore 262144:

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

   - Per mantenere l'impostazione dopo il riavvio, immettere quanto segue:

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

2. Seguire la "Elasticsearch Guida introduttiva" Sezione autogestito per installare ed eseguire il docker Elasticsearch e Kibana. In questo esempio, è stata installata la versione 8.1.

> Annotare il nome utente/password e il token creati da Elasticsearch, necessari per avviare l'autenticazione dell'interfaccia utente Kibana e dell'endpoint della piattaforma StorageGRID.

Elasticsearch Service | Self-managed

Install and run Elasticsearch

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

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

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

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

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

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

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

Install and run Kibana

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

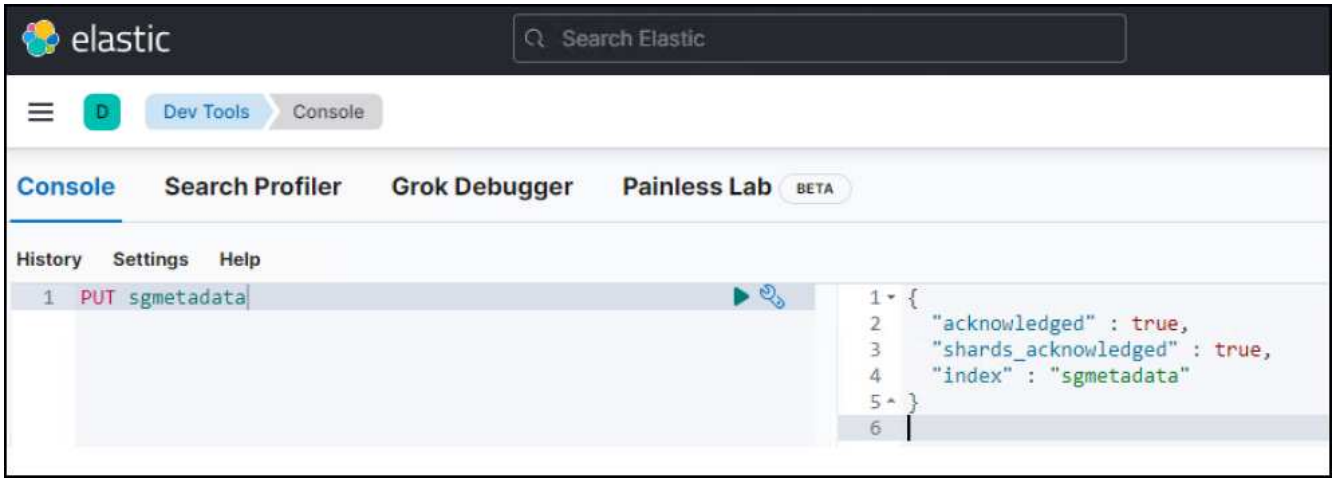
1. In a new terminal session, run:

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

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

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

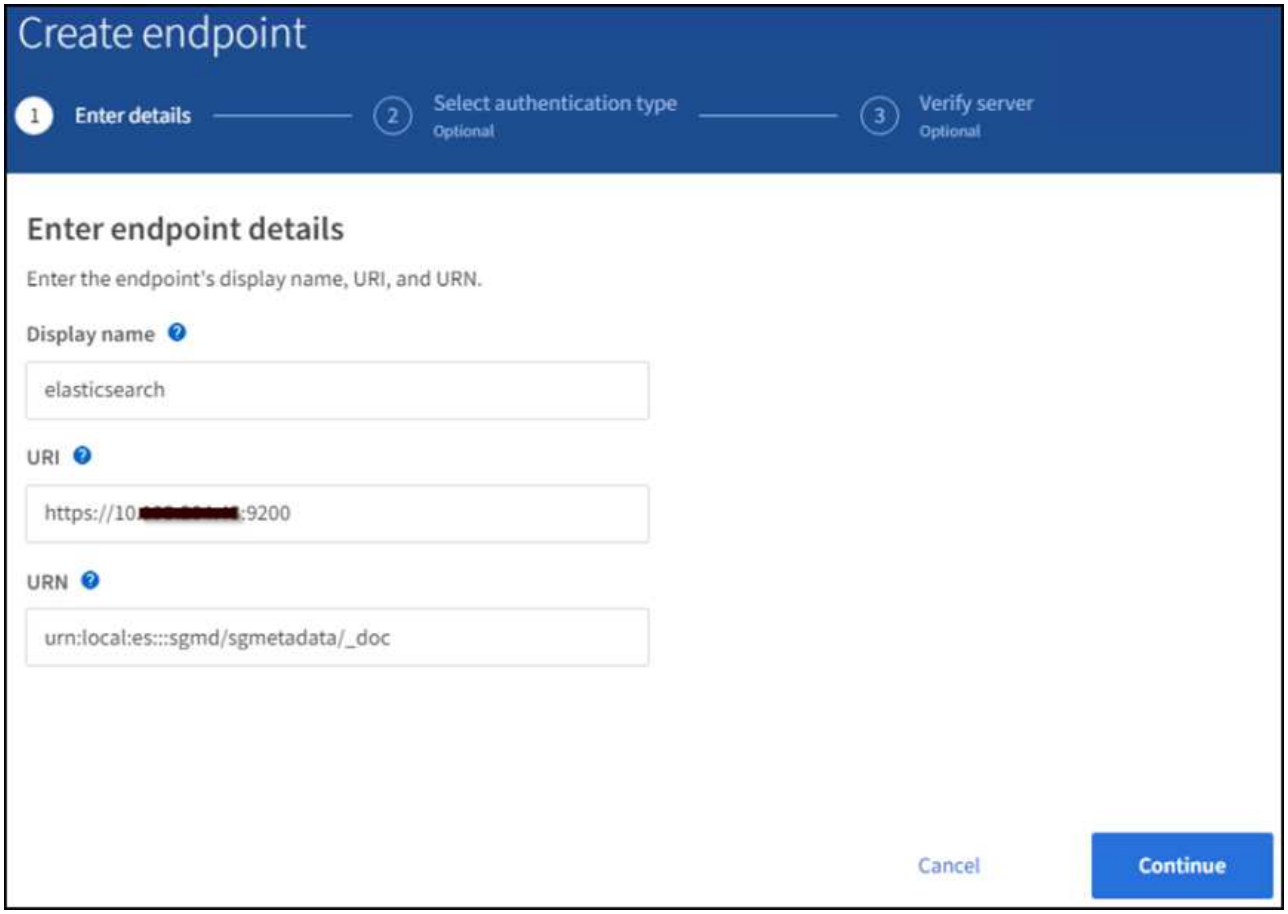
3. Una volta avviato il container Kibana docker, viene visualizzato il link URL `https://0.0.0.0:5601` viene visualizzato nella console. Sostituire 0.0.0.0 con l'indirizzo IP del server nell'URL.
4. Accedere all'interfaccia utente di Kibana utilizzando il nome utente `elastic` E la password generata da Elastic nel passaggio precedente.
5. Per il primo accesso, nella pagina di benvenuto della dashboard, selezionare Esplora da solo. Dal menu, selezionare Management (Gestione) > Dev Tools (Strumenti di sviluppo).
6. Nella schermata Console di Dev Tools, immettere `PUT <index>` Dove si utilizza questo indice per memorizzare i metadati degli oggetti StorageGRID. Utilizziamo il nome dell'indice `sgmetadata` in questo esempio. Fare clic sul piccolo simbolo del triangolo per eseguire IL comando PUT. Il risultato previsto viene visualizzato sul pannello di destra, come mostrato nella seguente schermata di esempio.



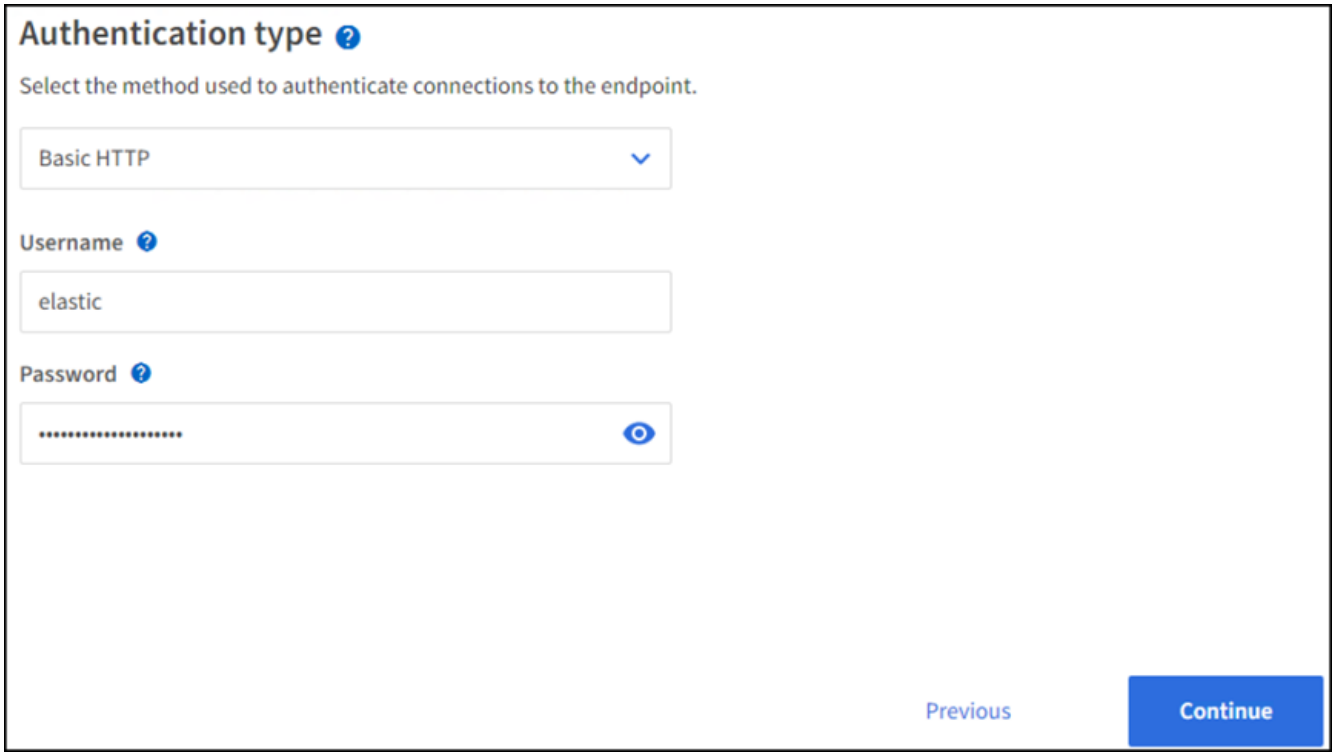
Configurazione degli endpoint dei servizi della piattaforma

Per configurare gli endpoint per i servizi della piattaforma, attenersi alla seguente procedura:

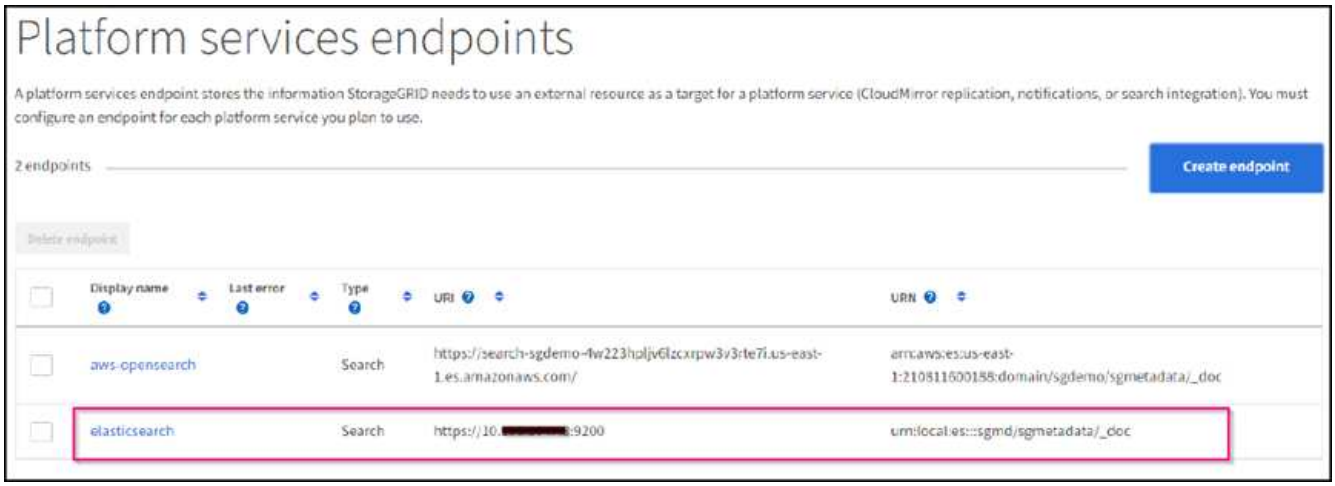
1. In Tenant Manager, andare a STORAGE(S3) > Platform Services Endpoint
2. Fare clic su Create Endpoint (Crea endpoint), immettere quanto segue, quindi fare clic su Continue (continua):
   - Esempio di nome visualizzato: `elasticsearch`
   - URI: `https://<elasticsearch-server-ip or hostname>:9200`
   - URNA: `urn:<something>:es:::<some-unique-text>/<index-name>/_doc` Dove index-name è il nome utilizzato sulla console Kibana. Esempio: `urn:local:es:::sgmd/sgmetadata/_doc`



3. Selezionare HTTP di base come tipo di autenticazione, quindi immettere il nome utente `elastic` E la password generata dal processo di installazione di Elasticsearch. Per passare alla pagina successiva, fare clic su Continue (continua).



4. Selezionare non verificare certificato e test e Crea endpoint per verificare l'endpoint. Se la verifica ha esito positivo, viene visualizzata una schermata dell'endpoint simile alla seguente schermata. Se la verifica non riesce, verificare che le voci URN, URI e nome utente/password siano corrette.



Configurazione del servizio di integrazione della ricerca nel bucket

Una volta creato l'endpoint del servizio della piattaforma, il passaggio successivo consiste nel configurare questo servizio a livello di bucket per inviare i metadati dell'oggetto all'endpoint definito ogni volta che un oggetto viene creato, cancellato o i relativi metadati o tag vengono aggiornati.

È possibile configurare l'integrazione della ricerca utilizzando Tenant Manager per applicare un XML di configurazione StorageGRID personalizzato a un bucket come segue:

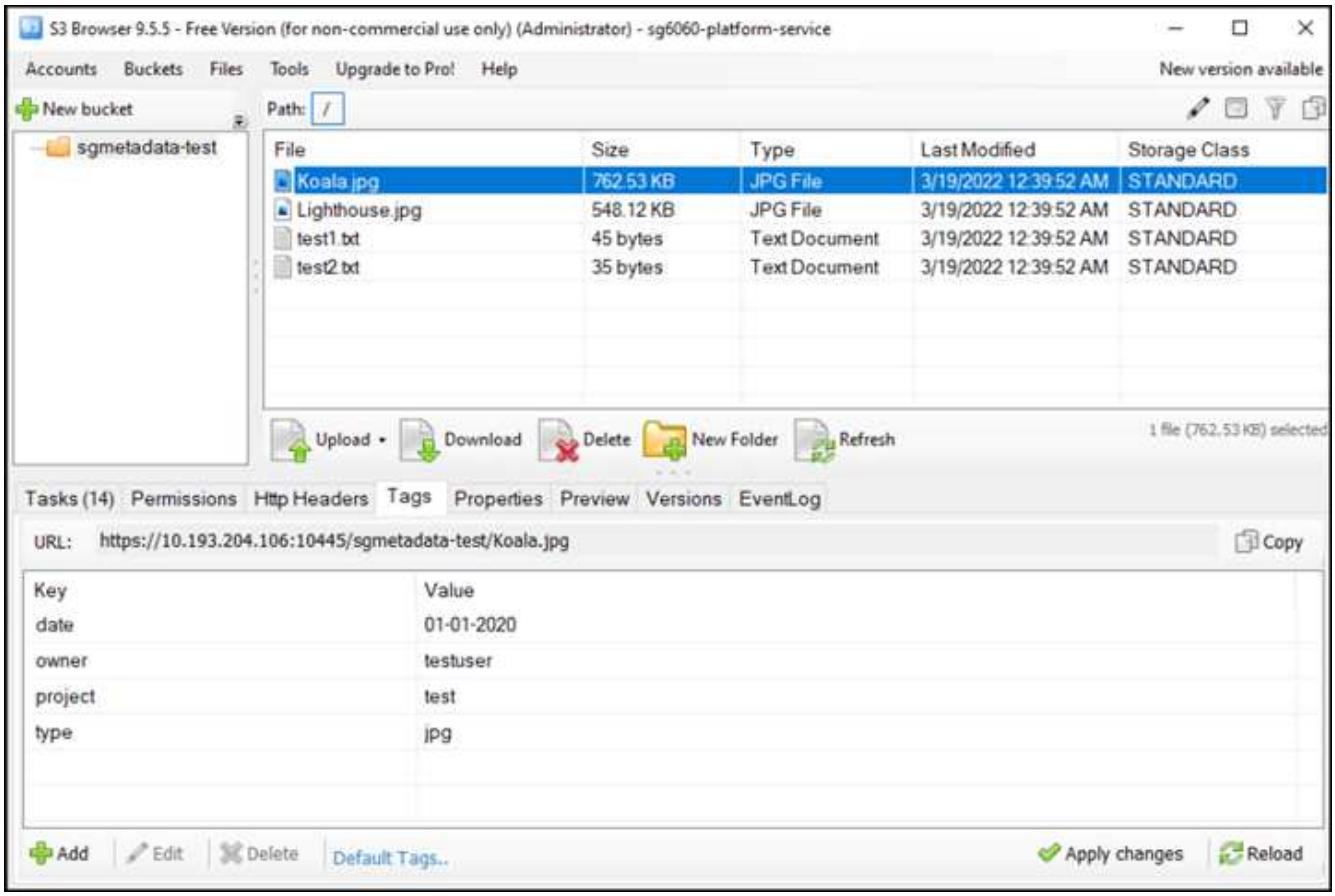
1. In Tenant Manager, andare a STORAGE(S3) > Bucket
2. Fare clic su Create bucket (Crea bucket), inserire il nome del bucket (ad esempio, `sgmetadata-test`) e accettare l'impostazione predefinita `us-east-1` regione.
3. Fare clic su continua > Crea bucket.
4. Per visualizzare la pagina Panoramica del bucket, fare clic sul nome del bucket, quindi selezionare Platform Services (servizi piattaforma).
5. Selezionare la finestra di dialogo Enable Search Integration (attiva integrazione ricerca). Nella casella XML fornita, immettere il file XML di configurazione utilizzando questa sintassi.

   L'URN evidenziato deve corrispondere all'endpoint dei servizi della piattaforma definito dall'utente. È possibile aprire un'altra scheda del browser per accedere a Tenant Manager e copiare l'URN dall'endpoint dei servizi della piattaforma definito.

   In questo esempio, non abbiamo utilizzato alcun prefisso, il che significa che i metadati per ogni oggetto in questo bucket vengono inviati all'endpoint Elasticsearch definito in precedenza.

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

6. Utilizzare S3 browser per connettersi a StorageGRID con la chiave di accesso/segreto del tenant e caricare gli oggetti di test in `sgmetadata-test` bucket e aggiunta di tag o metadati personalizzati agli oggetti.



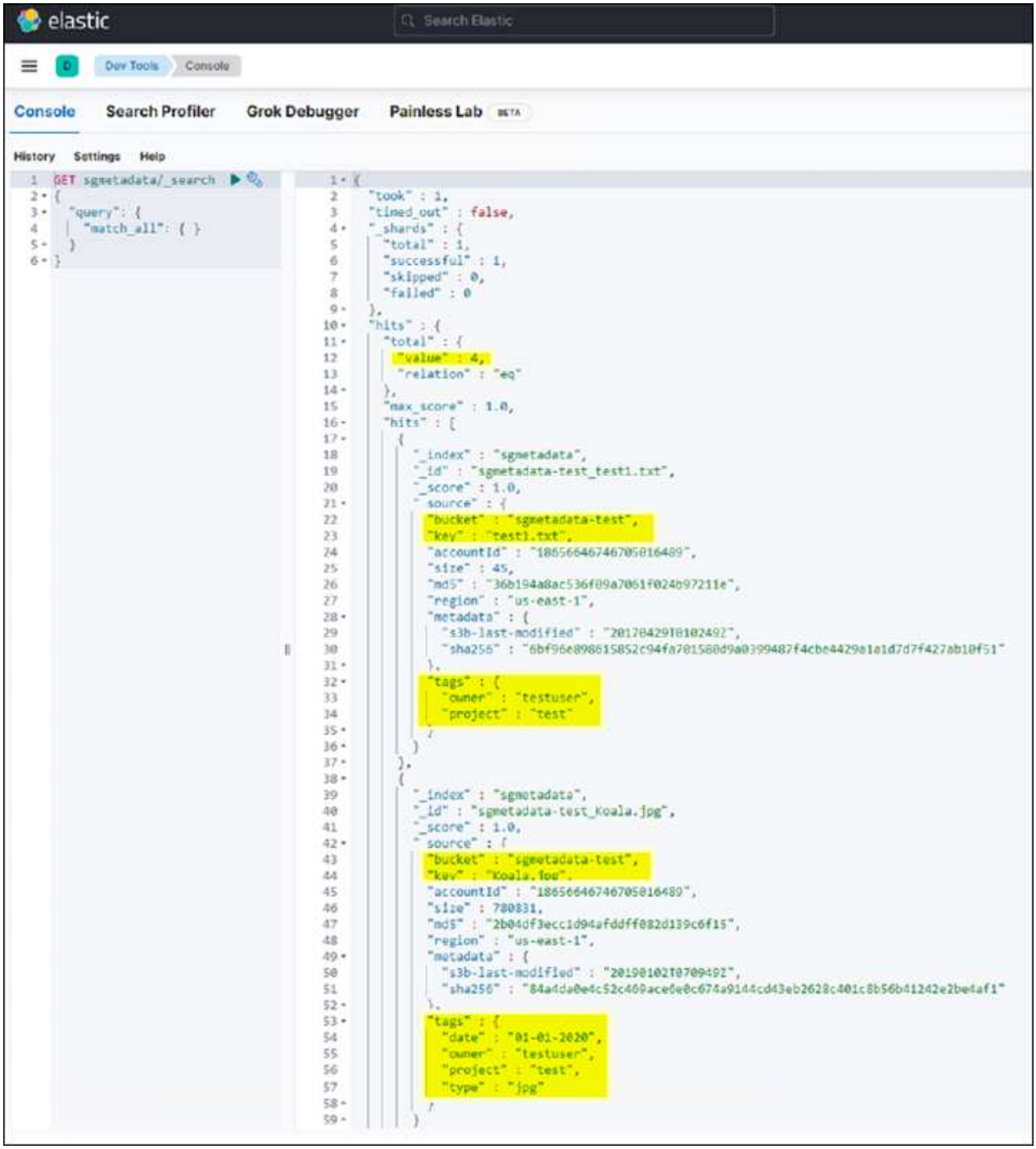
7. Utilizzare l'interfaccia utente di Kibana per verificare che i metadati dell'oggetto siano stati caricati nell'indice di sgmetadata.

   a. Dal menu, selezionare Management (Gestione) > Dev Tools (Strumenti di sviluppo).

   b. Incollare la query di esempio nel pannello della console a sinistra e fare clic sul simbolo del triangolo per eseguirla.

      Il risultato dell'esempio di query 1 nella seguente schermata di esempio mostra quattro record. Questo corrisponde al numero di oggetti nel bucket.

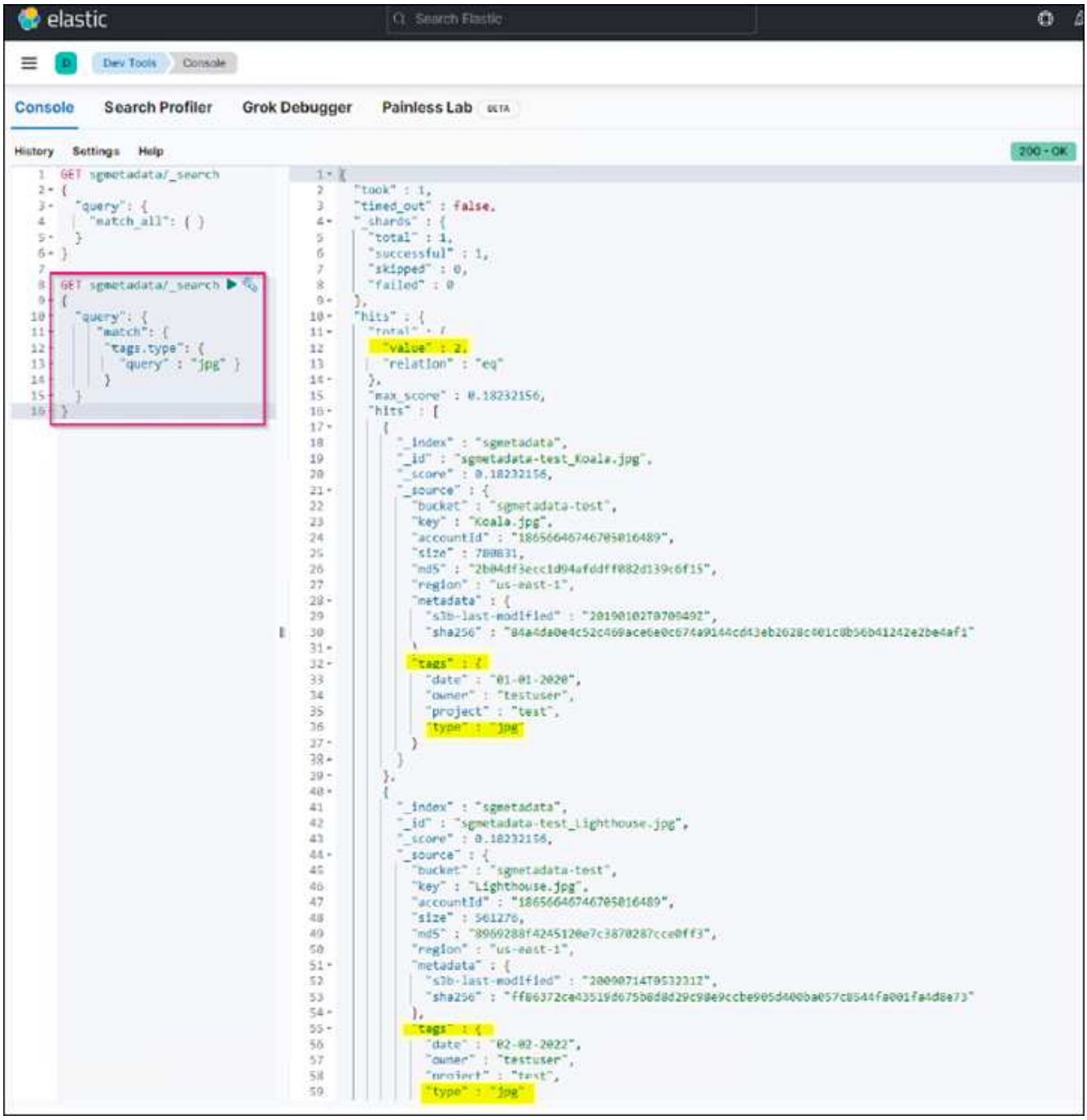
```
GET sgmetadata/_search
{
    "query": {
        "match_all": { }
}
}
```



Il risultato dell’esempio di query 2 nella seguente schermata mostra due record con il tipo di tag jpg.

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

+



Dove trovare ulteriori informazioni

Per ulteriori informazioni sulle informazioni descritte in questo documento, consultare i seguenti documenti e/o siti Web:

- "Cosa sono i servizi della piattaforma"
- "Documentazione di StorageGRID 11.6"

Di Angela Cheng

Clone del nodo

Considerazioni e performance sui cloni dei nodi.

Considerazioni sui cloni dei nodi

Il clone del nodo può essere un metodo più rapido per sostituire i nodi appliance esistenti per un aggiornamento tecnico, aumentare la capacità o aumentare le performance del sistema StorageGRID. Il clone del nodo può essere utile anche per la conversione alla crittografia del nodo con un KMS o per la modifica di un nodo di storage da DDP8 a DDP16.

- La capacità utilizzata del nodo di origine non è rilevante per il tempo richiesto per il completamento del processo di clonazione. Il clone del nodo è una copia completa del nodo che include spazio libero nel nodo.
- Le appliance di origine e di destinazione devono essere della stessa versione PGE
- Il nodo di destinazione deve avere sempre una capacità maggiore rispetto all'origine
  - Assicurarsi che il nuovo dispositivo di destinazione abbia un disco di dimensioni maggiori rispetto a quello di origine
  - Se il dispositivo di destinazione dispone di unità delle stesse dimensioni ed è configurato per il DDP8, è possibile configurare la destinazione per il DDP16. Se l'origine è già configurata per DDP16, non sarà possibile clonare il nodo.
  - Quando si passa dalle appliance SG5660 o SG5760 alle appliance SG6060, tenere presente che le unità SG5x60 dispongono di 60 dischi di capacità, mentre le unità SG6060 ne hanno solo 58.
- Il processo di clonazione del nodo richiede che il nodo di origine sia offline nella griglia per tutta la durata del processo di clonazione. Se un nodo aggiuntivo passa offline durante questo periodo di tempo, i servizi client potrebbero risentire.
- Un nodo di storage può essere offline solo per 15 giorni. Se la stima del processo di cloning è prossima a 15 giorni o supera i 15 giorni, utilizzare le procedure di espansione e decommissionamento.
- Per un sistema SG6060 con shelf di espansione, è necessario aggiungere il tempo necessario per la dimensione corretta del disco shelf al tempo di utilizzo dell'appliance di base per ottenere la durata completa del clone.
- Il numero di volumi in un dispositivo di storage di destinazione deve essere maggiore o uguale al numero di volumi nel nodo di origine. Non è possibile clonare un nodo di origine con volumi di archivi di oggetti 16 (rangedb) in un'appliance di storage di destinazione con volumi di archivi di oggetti 12, anche se l'appliance di destinazione ha una capacità maggiore rispetto al nodo di origine. La maggior parte delle appliance di storage dispone di 16 volumi di archivi di oggetti, ad eccezione dell'appliance di storage SGF6112 che ha solo 12 volumi di archivi di oggetti. Ad esempio, non è possibile clonare da SG5760 a SGF6112.

Stime delle performance dei cloni dei nodi

Le seguenti tabelle contengono stime calcolate per la durata del clone del nodo. Le condizioni variano, pertanto, le voci in **BOLD** potrebbero rischiare di superare il limite di 15 giorni per un nodo inattivo.

DDP8

SG5612 → qualsiasi

Velocità dell'interfaccia di rete	Dimensioni dell'unità 4 TB	Dimensioni disco 8 TB	Dimensioni disco 10 TB	12 TB di capacità dell'unità	Dimensioni dell'unità 16 TB	Dimensioni dell'unità 18 TB
10 GB	1 giorno	2 giorni	2.5 giorni	3 giorni	4 giorni	4.5 giorni
25 GB	1 giorno	2 giorni	2.5 giorni	3 giorni	4 giorni	4.5 giorni

SG5712 → qualsiasi

Velocità dell'interfaccia di rete	Dimensioni dell'unità 4 TB	Dimensioni disco 8 TB	Dimensioni disco 10 TB	12 TB di capacità dell'unità	Dimensioni dell'unità 16 TB	Dimensioni dell'unità 18 TB
10 GB	1 giorno	2 giorni	2.5 giorni	3 giorni	4 giorni	4.5 giorni
25 GB	1 giorno	2 giorni	2.5 giorni	3 giorni	4 giorni	4.5 giorni

SG5660 → SG5760

Velocità dell'interfaccia di rete	Dimensioni dell'unità 4 TB	Dimensioni disco 8 TB	Dimensioni disco 10 TB	12 TB di capacità dell'unità	Dimensioni dell'unità 16 TB	Dimensioni dell'unità 18 TB
10 GB	3 giorni	6 giorni	7 giorni	8.5 giorni	11.5 giorni	**13 giorni**
25 GB	3 giorni	6 giorni	7 giorni	8.5 giorni	11.5 giorni	**13 giorni**

SG5660 → SG6060

Velocità dell'interfaccia di rete	Dimensioni dell'unità 4 TB	Dimensioni disco 8 TB	Dimensioni disco 10 TB	12 TB di capacità dell'unità	Dimensioni dell'unità 16 TB	Dimensioni dell'unità 18 TB
10 GB	2.5 giorni	4.5 giorni	5.5 giorni	6.5 giorni	9 giorni	10 giorni
25 GB	2 giorni	4 giorni	5 giorni	6 giorni	8 giorni	9 giorni

SG5760 → SG5760

Velocità dell'interfaccia di rete	Dimensioni dell'unità 4 TB	Dimensioni disco 8 TB	Dimensioni disco 10 TB	12 TB di capacità dell'unità	Dimensioni dell'unità 16 TB	Dimensioni dell'unità 18 TB
10 GB	3 giorni	6 giorni	7 giorni	8.5 giorni	11.5 giorni	**13 giorni**
25 GB	3 giorni	6 giorni	7 giorni	8.5 giorni	11.5 giorni	**13 giorni**

SG5760 → SG6060

Velocità dell'interfaccia di rete	Dimensioni dell'unità 4 TB	Dimensioni disco 8 TB	Dimensioni disco 10 TB	12 TB di capacità dell'unità	Dimensioni dell'unità 16 TB	Dimensioni dell'unità 18 TB
10 GB	2.5 giorni	4.5 giorni	5.5 giorni	6.5 giorni	9 giorni	10 giorni
25 GB	1.5 giorni	3 giorni	3.5 giorni	4.5 giorni	6 giorni	6.5 giorni

SG6060 → SG6060

Velocità dell'interfaccia di rete	Dimensioni dell'unità 4 TB	Dimensioni disco 8 TB	Dimensioni disco 10 TB	12 TB di capacità dell'unità	Dimensioni dell'unità 16 TB	Dimensioni dell'unità 18 TB
10 GB	2.5 giorni	4.5 giorni	5.5 giorni	6.5 giorni	8.5 giorni	9.5 giorni
25 GB	1.5 giorni	3 giorni	3.5 giorni	4 giorni	5.5 giorni	6 giorni

DDP16

SG5760 → SG5760

Velocità dell'interfaccia di rete	Dimensioni dell'unità 4 TB	Dimensioni disco 8 TB	Dimensioni disco 10 TB	12 TB di capacità dell'unità	Dimensioni dell'unità 16 TB	Dimensioni dell'unità 18 TB
10 GB	3.5 giorni	6.5 giorni	8 giorni	9.5 giorni	12.5 giorni	**14 giorni**
25 GB	3.5 giorni	6.5 giorni	8 giorni	9.5 giorni	12.5 giorni	**14 giorni**

SG5760 → SG6060

Velocità dell'interfaccia di rete	Dimensioni dell'unità 4 TB	Dimensioni disco 8 TB	Dimensioni disco 10 TB	12 TB di capacità dell'unità	Dimensioni dell'unità 16 TB	Dimensioni dell'unità 18 TB
10 GB	2.5 giorni	5 giorni	6 giorni	7.5 giorni	10 giorni	11 giorni

Velocità dell'interfaccia di rete	Dimensioni dell'unità 4 TB	Dimensioni disco 8 TB	Dimensioni disco 10 TB	12 TB di capacità dell'unità	Dimensioni dell'unità 16 TB	Dimensioni dell'unità 18 TB
25 GB	2 giorni	3.5 giorni	4 giorni	5 giorni	6.5 giorni	7 giorni

SG6060 → SG6060

Velocità dell'interfaccia di rete	Dimensioni dell'unità 4 TB	Dimensioni disco 8 TB	Dimensioni disco 10 TB	12 TB di capacità dell'unità	Dimensioni dell'unità 16 TB	Dimensioni dell'unità 18 TB
10 GB	3.5 giorni	5 giorni	6 giorni	7 giorni	9.5 giorni	10.5 giorni
25 GB	2 giorni	3 giorni	4 giorni	4.5 giorni	6 giorni	7 giorni

Shelf di espansione (aggiungere a SG6060 per ogni shelf sull'appliance di origine)

Velocità dell'interfaccia di rete	Dimensioni dell'unità 4 TB	Dimensioni disco 8 TB	Dimensioni disco 10 TB	12 TB di capacità dell'unità	Dimensioni dell'unità 16 TB	Dimensioni dell'unità 18 TB
10 GB	3.5 giorni	5 giorni	6 giorni	7 giorni	9.5 giorni	10.5 giorni
25 GB	2 giorni	3 giorni	4 giorni	4.5 giorni	6 giorni	7 giorni

Di Aron Klein

Come utilizzare il remap delle porte

Potrebbe essere necessario rimappare una porta in entrata o in uscita per diversi motivi. È possibile passare dal servizio di bilanciamento del carico CLB legacy all'endpoint corrente di bilanciamento del carico del servizio nginx e mantenere la stessa porta per ridurre l'impatto sui client, utilizzare la porta 443 per il client S3 su una rete client con nodo di amministrazione o per le restrizioni del firewall.

Migrare i client S3 da CLB a NGINX con il remap della porta

Nelle release precedenti a StorageGRID 11.3, il servizio bilanciamento del carico incluso nei nodi gateway è il bilanciamento del carico di connessione (CLB). In StorageGRID 11.3, NetApp introduce il servizio NGINX come soluzione integrata ricca di funzionalità per il bilanciamento del carico del traffico HTTP. Poiché il servizio CLB rimane disponibile nella release corrente di StorageGRID, non è possibile riutilizzare la porta 8082 nella nuova configurazione dell'endpoint del bilanciamento del carico. Per risolvere questo problema, la porta in entrata 8082 viene rimappata a 10443. In questo modo, tutte le richieste HTTPS inviate alla porta 8082 del gateway vengono reindirizzate alla porta 10443, ignorando il servizio CLB e connettendosi invece al servizio NGINX. Sebbene le seguenti istruzioni siano per VMware, la funzionalità PORT_REMAP esiste per tutti i metodi di installazione ed è possibile utilizzare un processo simile per le implementazioni e le appliance bare metal.

Implementazione di VMware Virtual Machine Gateway Node

I seguenti passaggi riguardano un'implementazione StorageGRID in cui il nodo gateway o i nodi vengono implementati in VMware vSphere 7 come macchine virtuali utilizzando il formato di virtualizzazione aperta (OVF) di StorageGRID. Il processo comporta la rimozione distruttiva della macchina virtuale e la ridistribuzione della macchina virtuale con lo stesso nome e configurazione. Prima di accendere la macchina virtuale, modificare la proprietà vApp per rimappare la porta, quindi accendere la macchina virtuale e seguire il processo di ripristino del nodo.

Prerequisiti

- Si utilizza StorageGRID 11.3 o versione successiva
- È stato scaricato e si dispone dell'accesso ai file di installazione della versione di StorageGRID installata.
- Si dispone di un account vCenter con autorizzazioni per accendere/spegnere le macchine virtuali, modificare le impostazioni delle macchine virtuali e delle applicazioni, rimuovere le macchine virtuali da vCenter e implementare le macchine virtuali tramite OVF.
- È stato creato un endpoint per il bilanciamento del carico
  - La porta è configurata sulla porta di reindirizzamento desiderata
  - Il certificato SSL dell'endpoint è uguale a quello installato per il servizio CLB nel certificato server di configurazione/certificati server/servizio API di archiviazione oggetti o il client è in grado di accettare una modifica del certificato.

```
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.
```

Distruggere il primo nodo gateway

Per distruggere il primo nodo gateway, attenersi alla seguente procedura:

1. Scegliere il nodo gateway con cui iniziare se la griglia contiene più di uno.
2. Rimuovere gli IP dei nodi da tutte le entità round robin DNS o dai pool di bilanciamento del carico, se applicabile.
3. Attendere la scadenza del TTL (Time-to-Live) e delle sessioni aperte.
4. Spegnere il nodo VM.
5. Rimuovere il nodo VM dal disco.

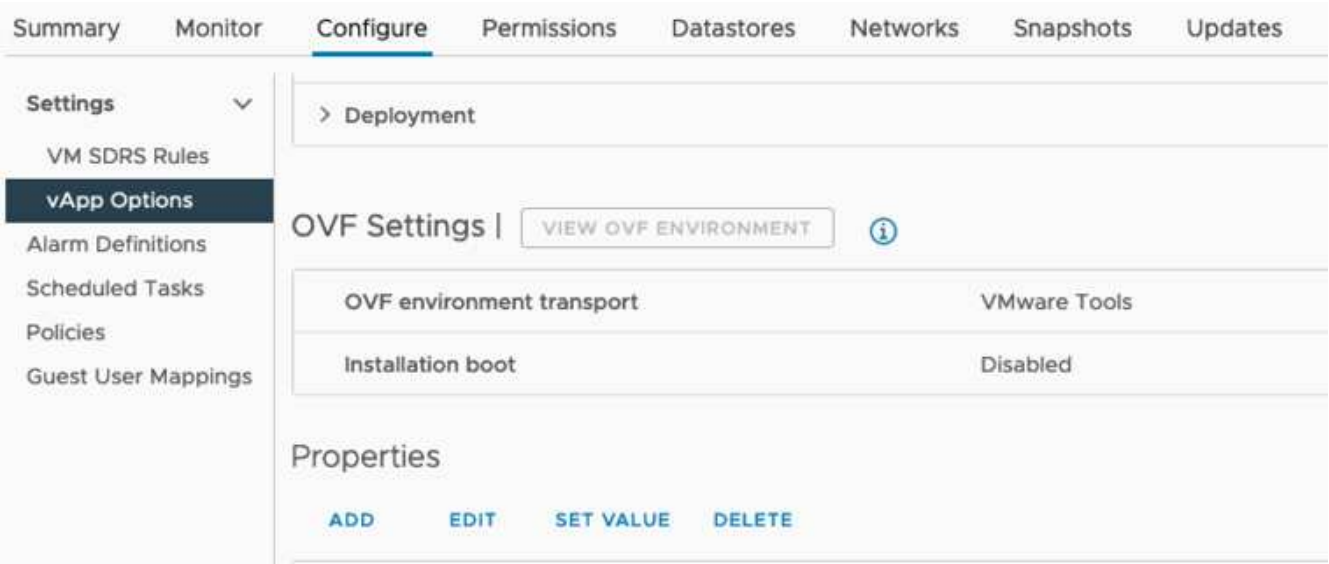
Implementare il nodo gateway sostitutivo

Per implementare il nodo gateway sostitutivo, attenersi alla seguente procedura:

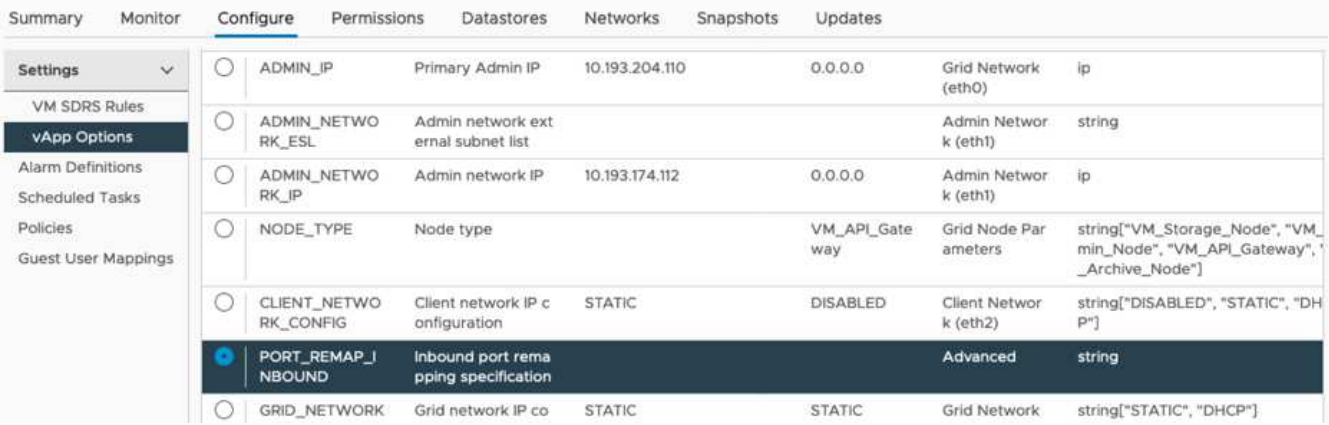
1. Implementare la nuova macchina virtuale da OVF, selezionando i file .ovf, .mf e .vmdk dal pacchetto di installazione scaricato dal sito di supporto:
   - vsphere-gateway.mf
   - vsphere-gateway.ovf

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

2. Una volta implementata la macchina virtuale, selezionarla dall'elenco delle macchine virtuali e selezionare la scheda Configura opzioni vApp.



3. Scorrere fino alla sezione Proprietà e selezionare LA proprietà PORT_REMAP_INBOUND

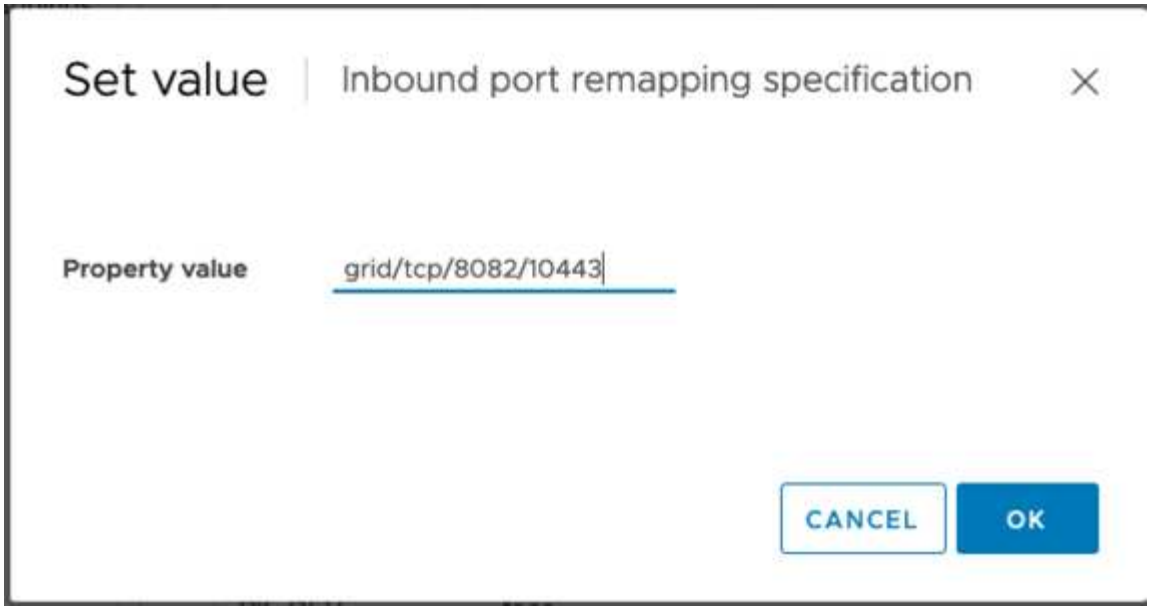


4. Scorrere fino all'inizio dell'elenco Proprietà e fare clic su Modifica

5. Selezionare la scheda tipo, verificare che la casella di controllo configurabile dall'utente sia selezionata, quindi fare clic su Salva.

6. Nella parte superiore dell’elenco Proprietà, con la proprietà "PORT_REMAP_INBOUND" ancora selezionata, fare clic su Imposta valore.

7. Nel campo Property Value (valore proprietà), inserire la rete (griglia, amministratore o client), il TCP, la porta originale (8082) e la nuova porta (10443) con "/" tra ciascun valore, come illustrato di seguito.

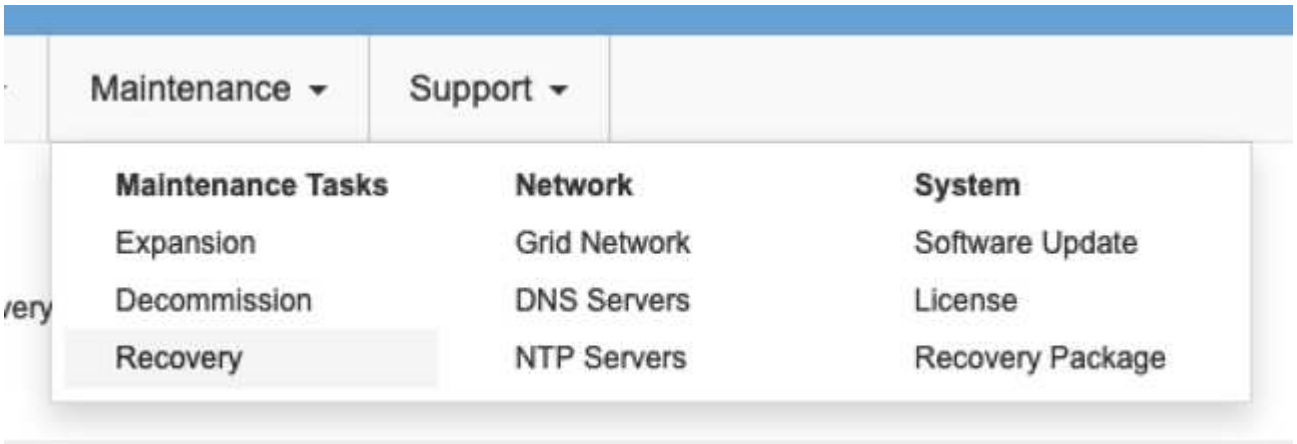


8. Se si utilizzano più reti, utilizzare una virgola (,) per separare le stringhe di rete, ad esempio Grid/tcp/8082/10443,admin/tcp/8082/10443,client/tcp/8082/10443

Ripristinare il nodo gateway

Per ripristinare il nodo gateway, attenersi alla seguente procedura:

1. Accedere alla sezione manutenzione/Ripristino dell'interfaccia utente di Grid Management.



2. Accendere il nodo VM e attendere che venga visualizzato nella sezione Maintenance/Recovery Pending Nodes dell'interfaccia utente Grid Management.


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

3. Una volta ripristinato il nodo, l'IP può essere incluso in tutte le entità round robin DNS o nei pool di bilanciamento del carico, se applicabile.

   A questo punto, tutte le sessioni HTTPS sulla porta 8082 vanno alla porta 10443

Rimappare la porta 443 per l'accesso al client S3 su un nodo Admin

La configurazione predefinita nel sistema StorageGRID per un nodo admin o un gruppo ha contenente un nodo Admin prevede che le porte 443 e 80 siano riservate alle interfacce utente di gestione e di gestione del tenant e non possano essere utilizzate per gli endpoint di bilanciamento del carico. La soluzione consiste nell'utilizzare la funzione di remap delle porte e reindirizzare la porta in entrata 443 a una nuova porta che verrà configurata come endpoint del bilanciamento del carico. Una volta completato il traffico del client S3, sarà possibile utilizzare la porta 443, l'interfaccia utente di gestione della griglia sarà accessibile solo tramite la porta 8443 e l'interfaccia utente di gestione del tenant sarà accessibile solo sulla porta 9443. La funzione di remap port può essere configurata solo al momento dell'installazione del nodo. Per implementare un remap di porta di un nodo attivo nella griglia, è necessario ripristinarlo allo stato preinstallato. Si tratta di una procedura distruttiva che include un ripristino del nodo una volta apportata la modifica alla configurazione.

Log e database di backup

I nodi di amministrazione contengono registri di audit, metriche prometheus e informazioni storiche su attributi, allarmi e avvisi. Avere più nodi di amministrazione significa avere più copie di questi dati. Se non si dispone di più nodi di amministrazione nella griglia, assicurarsi di conservare questi dati per il ripristino dopo che il nodo è stato ripristinato al termine di questo processo. Se si dispone di un altro nodo admin nella griglia, è possibile copiare i dati da tale nodo durante il processo di ripristino. Se non si dispone di un altro nodo admin nella griglia, è possibile seguire queste istruzioni per copiare i dati prima di distruggere il nodo.

Copia dei registri di audit

1. Accedere al nodo di amministrazione:
   a. Immettere il seguente comando: `ssh admin@grid_node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`

d. Immettere la password elencata in `Passwords.txt` file.

e. Aggiungere la chiave privata SSH all'agente SSH. Inserire: `ssh-add`

f. Inserire la password di accesso SSH elencata in `Passwords.txt` file.

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

2. Creare la directory per copiare tutti i file di log di audit in una posizione temporanea su un nodo griglia separato. Utilizzare *storage_node_01*:

   a. `ssh admin@storage_node_01_IP`

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

3. Tornare al nodo admin, arrestare il servizio AMS per impedire la creazione di un nuovo file di log: `service ams stop`

4. Rinominare il file audit.log in modo che non sovrascriva il file esistente quando lo si copia nel nodo di amministrazione recuperato.

   a. Rinominare il file audit.log con un nome di file univoco numerato, ad esempio yyyy-mm-dd.txt.1. Ad esempio, è possibile rinominare il file di log di audit in 2015-10-25.txt.1

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

5. Riavviare il servizio AMS: `service ams start`

6. Copia tutti i file di log di audit: `scp * admin@storage_node_01_IP:/var/local/tmp/saved-audit-logs`

Copia dei dati Prometheus

> La copia del database Prometheus potrebbe richiedere un'ora o più. Alcune funzionalità di Grid Manager non saranno disponibili mentre i servizi vengono arrestati sul nodo di amministrazione.

1. Creare la directory per copiare i dati prometheus in una posizione temporanea su un nodo griglia separato, ancora una volta utilizzeremo *storage_node_01*:

   a. Accedere al nodo di storage:

      i. Immettere il seguente comando: `ssh admin@storage_node_01_IP`

      ii. Immettere la password elencata in `Passwords.txt` file.

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

2. Accedere al nodo di amministrazione:

   a. Immettere il seguente comando: `ssh admin@admin_node_IP`

   b. Immettere la password elencata in `Passwords.txt` file.

   c. Immettere il seguente comando per passare a root: `su -`

d. Immettere la password elencata in `Passwords.txt` file.

e. Aggiungere la chiave privata SSH all'agente SSH. Inserire: `ssh-add`

f. Inserire la password di accesso SSH elencata in `Passwords.txt` file.

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

3. Dal nodo di amministrazione, arrestare il servizio Prometheus: `service prometheus stop`

   a. Copiare il database Prometheus dal nodo di amministrazione di origine al nodo di storage percorso di backup nodo: `/rsync -azh --stats "/var/local/mysql_ibdata/prometheus/data" "`*`storage_node_01_IP`*`:/var/local/tmp/prometheus/"`

4. Riavviare il servizio Prometheus sul nodo di amministrazione di origine.`service prometheus start`

Backup delle informazioni cronologiche

Le informazioni storiche sono memorizzate in un database mysql. Per eseguire il dump di una copia del database, sono necessari l'utente e la password di NetApp. Se si dispone di un altro nodo admin nella griglia, questo passaggio non è necessario e il database può essere clonato da un nodo admin rimanente durante il processo di recovery.

1. Accedere al nodo di amministrazione:

   a. Immettere il seguente comando: `ssh admin@`*`admin_node_IP`*

   b. Immettere la password elencata in `Passwords.txt` file.

   c. Immettere il seguente comando per passare a root: `su -`

   d. Immettere la password elencata in `Passwords.txt` file.

   e. Aggiungere la chiave privata SSH all'agente SSH. Inserire: `ssh-add`

   f. Inserire la password di accesso SSH elencata in `Passwords.txt` file.

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

2. Arrestare i servizi StorageGRID sul nodo di amministrazione e avviare ntp e mysql

   a. Arrestare tutti i servizi: `service servermanager stop`

   b. riavviare il servizio ntp: `service ntp start`..riavviare il servizio mysql: `service mysql start`

3. Dump del database mi in /var/local/tmp

   a. immettere il seguente comando: `mysqldump -u `*`username`*` -p `*`password`*` mi > /var/local/tmp/mysql-mi.sql`

4. Copiare il file dump mysql in un nodo alternativo, verrà utilizzato *storage_node_01:* *`scp /var/local/tmp/mysql-mi.sql _storage_node_01_IP`*:*/var/local/tmp/mysql-mi.sql*

   a. Se non si richiede più l'accesso senza password ad altri server, rimuovere la chiave privata dall'agente SSH. Inserire: `ssh-add -D`

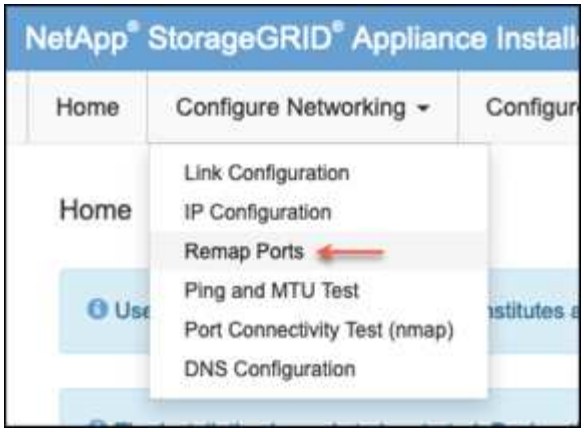
Ricostruire il nodo Admin

Ora che si dispone di una copia di backup di tutti i dati e i registri desiderati su un altro nodo admin nella griglia o memorizzati in una posizione temporanea, è il momento di ripristinare l'appliance in modo da poter configurare il rimap della porta.

1. La reimpostazione di un'appliance riporta l'appliance allo stato preinstallato, dove conserva solo il nome host, gli IP e le configurazioni di rete. Tutti i dati andranno persi, motivo per cui ci siamo assicurati di avere un backup di tutte le informazioni importanti.
   a. immettere il seguente comando: `sgareinstall`

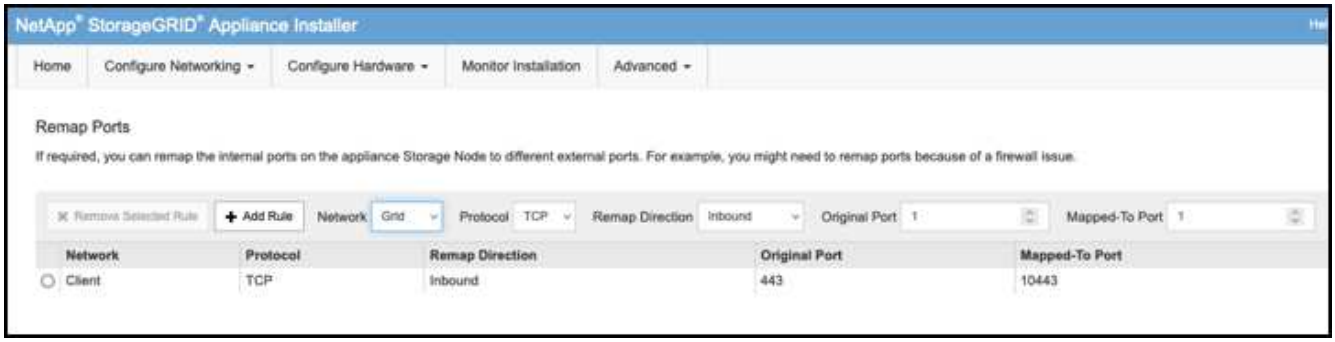
```
root@sg100-01:~ # sgareinstall
WARNING: All StorageGRID Webscale services on this node will be shut
down.
WARNING: Data stored on this node may be lost.
WARNING: You will have to reinstall StorageGRID Webscale to this
node.

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. Dopo un certo periodo di tempo, l'appliance si riavvierà e sarà possibile accedere all'interfaccia utente PGE del nodo.
3. Accedere alla scheda Configure Networking (Configura rete)



4. Selezionare la rete, il protocollo, la direzione e le porte desiderate, quindi fare clic sul pulsante Add Rule (Aggiungi regola).

> Il rimappamento della porta in entrata 443 sulla rete GRID interromperà l'installazione e le procedure di espansione. Si sconsiglia di rimappare la porta 443 sulla rete GRID.



5. Una volta aggiunti i rimap di porta desiderati, è possibile tornare alla scheda home e fare clic sul pulsante Start Installation (Avvia installazione).

A questo punto, è possibile seguire le procedure di ripristino del nodo Admin in "documentazione del prodotto"

Ripristinare database e registri

Una volta ripristinato il nodo admin, è possibile ripristinare le metriche, i registri e le informazioni storiche. Se si dispone di un altro nodo admin nella griglia, seguire la "documentazione del prodotto" utilizzando gli script *prometheus-clone-db.sh* e *mi-clone-db.sh*. Se si tratta dell'unico nodo admin e si è scelto di eseguire il backup di questi dati, attenersi alla procedura riportata di seguito per ripristinare le informazioni.

Copia dei log di audit

1. Accedere al nodo di amministrazione:
   a. Immettere il seguente comando: `ssh admin@grid_node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.
   e. Aggiungere la chiave privata SSH all'agente SSH. Inserire: `ssh-add`

f. Inserire la password di accesso SSH elencata in `Passwords.txt` file.

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

2. Copiare i file di log di controllo conservati nel nodo di amministrazione recuperato: `scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY* .`
3. Per motivi di sicurezza, eliminare i registri di controllo dal nodo Grid guasto dopo aver verificato che siano stati copiati correttamente nel nodo Admin ripristinato.
4. Aggiornare le impostazioni di utente e gruppo dei file di log di controllo sul nodo di amministrazione recuperato: `chown ams-user:bycast *`

È inoltre necessario ripristinare qualsiasi accesso client preesistente alla condivisione di controllo. Per ulteriori informazioni, consultare le istruzioni per l'amministrazione di StorageGRID.

Ripristinare le metriche Prometheus

> La copia del database Prometheus potrebbe richiedere un'ora o più. Alcune funzionalità di Grid Manager non saranno disponibili mentre i servizi vengono arrestati sul nodo di amministrazione.

1. Accedere al nodo di amministrazione:
   a. Immettere il seguente comando: `ssh admin@grid_node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.
   e. Aggiungere la chiave privata SSH all'agente SSH. Inserire: `ssh-add`
   f. Inserire la password di accesso SSH elencata in `Passwords.txt` file.

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

2. Dal nodo di amministrazione, arrestare il servizio Prometheus: `service prometheus stop`
   a. Copiare il database Prometheus dalla posizione di backup temporaneo al nodo admin: `/rsync -azh --stats "backup_node:/var/local/tmp/prometheus/" "/var/local/mysql_ibdata/prometheus/"`
   b. verificare che i dati siano nel percorso corretto e che siano completi `ls /var/local/mysql_ibdata/prometheus/data/`
3. Riavviare il servizio Prometheus sul nodo di amministrazione di origine.`service prometheus start`

Ripristinare le informazioni cronologiche

1. Accedere al nodo di amministrazione:
   a. Immettere il seguente comando: `ssh admin@grid_node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.

c. Immettere il seguente comando per passare a root: `su -`

d. Immettere la password elencata in `Passwords.txt` file.

e. Aggiungere la chiave privata SSH all'agente SSH. Inserire: `ssh-add`

f. Inserire la password di accesso SSH elencata in `Passwords.txt` file.

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

2. Copiare il file dump mysql dal nodo alternativo: `scp grid_node_IP_:/var/local/tmp/mysql-mi.sql /var/local/tmp/mysql-mi.sql`
3. Arrestare i servizi StorageGRID sul nodo di amministrazione e avviare ntp e mysql
   a. Arrestare tutti i servizi: `service servermanager stop`
   b. riavviare il servizio ntp: `service ntp start`..riavviare il servizio mysql: `service mysql start`
4. Rilasciare il database mi e creare un nuovo database vuoto: `mysql -u *username* -p *password* -A mi -e "drop database mi; create database mi;"`
5. ripristinare il database mysql dal dump del database: `mysql -u *username* -p *password* -A mi < /var/local/tmp/mysql-mi.sql`
6. Riavviare tutti gli altri servizi `service servermanager start`

Di Aron Klein

Procedura di trasferimento del sito a griglia e di modifica della rete a livello di sito

Questa guida descrive la preparazione e la procedura per il trasferimento del sito StorageGRID in una griglia multisito. È necessario avere una conoscenza completa di questa procedura e pianificare in anticipo per garantire un processo senza problemi e ridurre al minimo le interruzioni per i clienti.

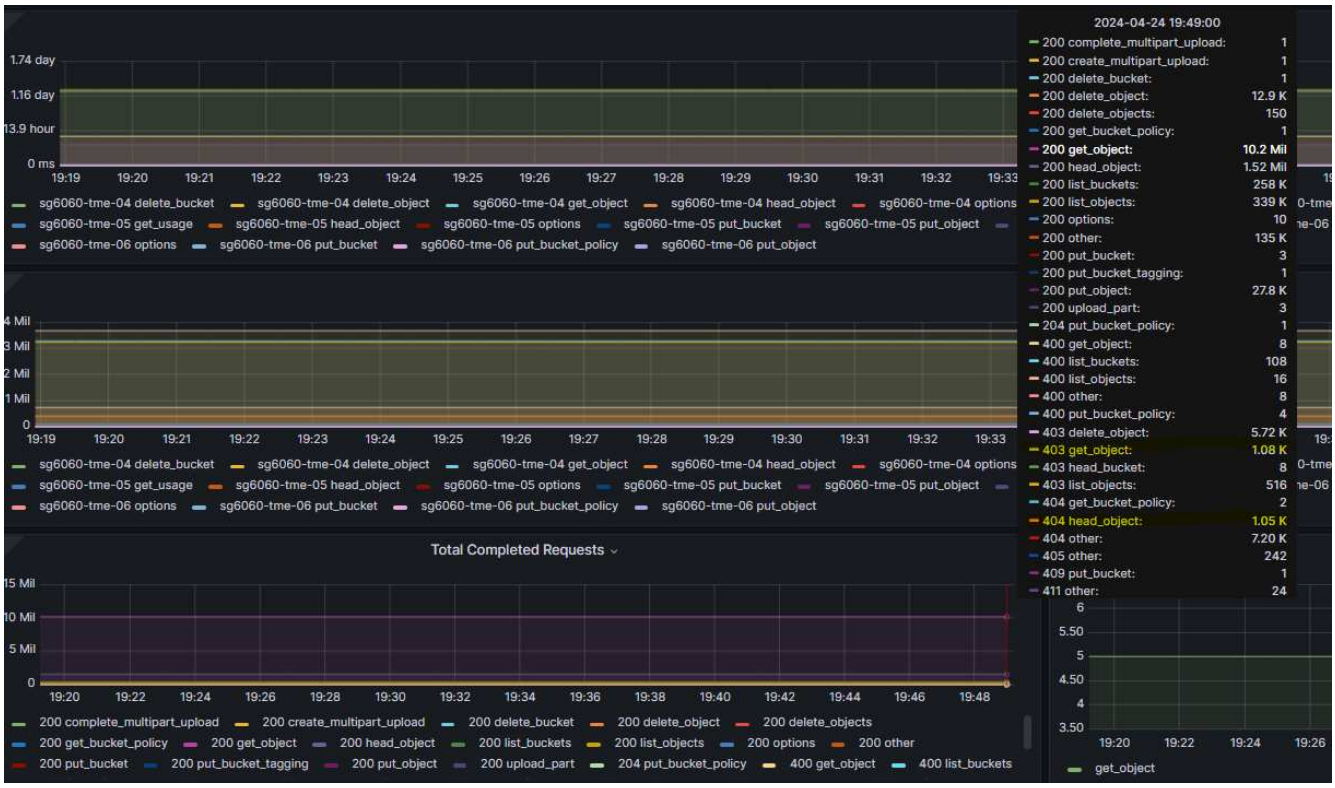
Se è necessario modificare la rete Grid di tutta la griglia, vedere "Modificare gli indirizzi IP per tutti i nodi nella griglia".

Considerazioni prima del trasferimento del sito

- Lo spostamento del sito deve essere completato e tutti i nodi online entro 15 giorni per evitare la ricostruzione del database Cassandra.
  "Recovery Storage Node Down per più di 15 giorni"
- Se una regola ILM delle policy attive utilizza un comportamento di acquisizione rigoroso, considerare la possibilità di cambiarlo in modo da bilanciarlo o in dual commit se il cliente desidera continuare a INSERIRE gli oggetti nel Grid durante il trasferimento del sito.
- Per le appliance storage con 60 dischi o più, non spostare mai lo shelf con i dischi installati. Etichettare ciascuna unità disco e rimuoverla dal contenitore di archiviazione prima di imballarla/spostarla.
- Modifica appliance StorageGRID la rete VLAN può essere eseguita in remoto tramite rete di amministrazione o rete client. Oppure si prevede di essere in loco per eseguire la modifica prima o dopo il

trasferimento.

- Verificare se l'applicazione cliente sta utilizzando HEAD o OTTENERE l'oggetto di non esistenza prima di METTERE. In caso affermativo, modificare la coerenza del bucket in strong-site per evitare l'errore HTTP 500. In caso di dubbi, consultare la panoramica S3 grafici Grafana **Grid manager > supporto > metriche**, passare il mouse sul grafico "richiesta totale completata". Se il conteggio è molto elevato di 404 oggetti GET o 404 oggetti Head, probabilmente una o più applicazioni utilizzano l'oggetto Head o Get nonexistence. Il conteggio è cumulativo, passare il mouse su una timeline diversa per vedere la differenza.



Procedura di modifica dell'indirizzo IP della griglia prima del trasferimento del sito

Fasi

1. Se la nuova subnet di rete della griglia viene utilizzata nella nuova posizione, "Aggiungere la subnet all'elenco delle subnet di rete della griglia"
2. Accedere al nodo di amministrazione primario, utilizzare change-ip per modificare l'IP della griglia, deve **stage** la modifica prima di arrestare il nodo per il trasferimento.
   a. Selezionare 2 quindi 1 per la modifica dell'IP della griglia

```
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. selezionare 5 per visualizzare le modifiche

```
================================================================================
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. selezionare 10 per convalidare e applicare la modifica.

```
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 questa fase è necessario selezionare **fase**.

```
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. Se il nodo di amministrazione primario è incluso nella modifica precedente, immettere **'A' per riavviare manualmente il nodo di amministrazione primario**

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

Applying these changes will update the following nodes:

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

The following nodes will also require restarting:

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

Select one of the following options:

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

[apply/stage/cancel]> stage

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

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

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

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

f. Premere invio per tornare al menu precedente e uscire dall'interfaccia change-ip.

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

3. Da Grid Manager, scaricare il nuovo pacchetto di ripristino. **Grid manager** > **Maintenance** > **Recovery package**
4. Se è necessario modificare la VLAN sull'appliance StorageGRID, vedere la sezione Modifica VLAN dell'appliance.
5. Arrestare tutti i nodi e/o le appliance in sede, etichettare/rimuovere le unità disco se necessario, disimballare, imballare e spostare.
6. Se si prevede di modificare l'indirizzo ip della rete amministrativa e/o la VLAN e l'indirizzo ip del client, è possibile eseguire la modifica dopo il trasferimento.

Modifica VLAN dell'appliance

La procedura riportata di seguito presuppone l'accesso remoto alla rete client o di amministrazione dell'appliance StorageGRID per eseguire la modifica in remoto.

Fasi

1. Prima di spegnere l'apparecchio, "impostare l'apparecchio in modalità di manutenzione".

2. Utilizzando un browser per accedere alla GUI del programma di installazione dell'appliance StorageGRID utilizzando https://<admin-or-client-network-ip>:8443. Non è possibile utilizzare Grid IP come nuovo Grid IP già in uso dopo l'avvio dell'appliance in modalità di manutenzione.
3. Modificare la VLAN per la rete Grid. Se si accede all'appliance tramite la rete client, non è possibile modificare la VLAN client in questo momento, è possibile modificarla dopo lo spostamento.
4. ssh per l'appliance e spegnere il nodo utilizzando 'hutdoown -h now'
5. Dopo che le appliance sono pronte presso il nuovo sito, accedere alla GUI del programma di installazione dell'appliance StorageGRID utilizzando https://<grid-network-ip>:8443. Verificare che lo storage sia in uno stato ottimale e la connettività di rete agli altri nodi Grid utilizzando gli strumenti ping/nmap nella GUI.
6. Se si prevede di modificare l'IP della rete client, è possibile modificare la VLAN client in questa fase. La rete client non è pronta finché non si aggiorna l'ip della rete client utilizzando lo strumento change-ip nel passaggio successivo.
7. Uscire dalla modalità di manutenzione. Dal programma di installazione dell'appliance StorageGRID, selezionare **Avanzate** > **Riavvia controller**, quindi selezionare **Riavvia in StorageGRID**.
8. Dopo che tutti i nodi sono attivi e Grid non mostra alcun problema di connettività, utilizzare change-ip per aggiornare la rete di amministrazione dell'appliance e la rete client, se necessario.