Come abilitare StorageGRID nel tuo ambiente

How to enable StorageGRID in your environment

NetApp
April 26, 2024

Sommario

Come abilitare StorageGRID nel tuo ambiente

Soluzioni di terze parti validate

Soluzioni validate di terze parti: Panoramica

NetApp, in collaborazione con i nostri partner, ha validato queste soluzioni per l'utilizzo con StorageGRID. Consultare le informazioni contenute in questa sezione per scoprire quali soluzioni sono state validate e per ottenere istruzioni aggiuntive, se applicabili.

Unisci le forze con NetApp per accelerare l'innovazione del portfolio, espandere la consapevolezza del mercato e aumentare le vendite quando crei soluzioni NetApp collaudate e Best-of-breed. "Diventa un partner Alliance oggi stesso".

Soluzioni validate di terze parti StorageGRID 11,8

Le seguenti soluzioni di terze parti sono state convalidate per l'utilizzo con StorageGRID 11,8.
Se la soluzione che stai cercando non è presente nell'elenco, contatta il tuo rappresentante commerciale NetApp.

Soluzioni di terze parti validate su StorageGRID

Queste soluzioni sono state testate in collaborazione con i rispettivi partner.

- Actifio
- Alluxio
- Apache Kafka
- Punto di montaggio AWS
- Bridgestor
- Cantemo
- Citrix Content Collaboration
- Collibra (qualità minima dei dati Collibra versione 2024,02)
- CommVault 11
- Portale Ctera 6
- Dal
- Datadobi
- Storage di Data Dynamics X
- DefendX
- Dati di diskover
- Dremio
- EMAM
- Archivio di oggetti Fujifilm
- Server aziendale GitHub

- IBM FileNet
- IBM Spectrum Protect Plus
- Interica
- Impresa
- Cluster di big data Microsoft SQL Server
- Model9
- Modzy
- Moonwalk universale
- BELLO
- Nasuni
- Documento OpenText 16.4
- Documento OpenText 21.4
- OpenText InfoArchive 16 EP7
- OpenText Media Management 16.5 con CyanGate Cloud
- Panzura
- PixitMedia ngenea
- Point Archival Gateway 2.0
- Point Storage Manager 6.4
- Primestream
- Quantum StorNext 5.4.0.1
- Reveille v10 build 220706 o superiore
- Rubrik CDM
- s3a
- Signiant
- Fiocco di neve
- Ghiacciaio on-premise di Spectra Logic
- Smartstore Splunk
- Lo storage diventa semplice
- Trino
- Verniciare Enterprise 6.0.4
- Veeeam 12
- Veritas Enterprise Vault 14
- Veritas NetBackup 8.0
- Verticale 10.x
- Visoline
- Virtalica StorageFabric
- Weka v3.10 o versione successiva

Soluzioni di terze parti validate su StorageGRID con blocco a oggetti

Queste soluzioni sono state testate in collaborazione con i rispettivi partner.

- CommVault 11 Feature Release 26
- IBM FileNet
- Documento OpenText 21.4
- Veeeam 12
- Veritas Enterprise Vault 14.2.2
- Veritas NetBackup 10.1.1 e versioni successive

Soluzioni di terze parti supportate su StorageGRID

Queste soluzioni sono state testate.

- Archiviware
- Comunicazioni Axis
- Congruità360
- DataFrameworks
- Piattaforma EcoDigital DIVA
- Encoding.com
- Archivio di oggetti Fujifilm
- Archivio GE Centricity Enterprise
- Gitlab
- Hyland Acuo
- IBM Aspera
- Sistemi Milestone
- OnSSI
- Motore Reach
- SilverTrak
- SoftNAS
- QStar
- Velasea

Soluzioni di terze parti validate da StorageGRID 11.7

Le seguenti soluzioni di terze parti sono state validate per l'utilizzo con StorageGRID 11.7. + se la soluzione che stai cercando non è presente nell'elenco, contatta il tuo rappresentante commerciale NetApp.

Soluzioni di terze parti validate su StorageGRID

Queste soluzioni sono state testate in collaborazione con i rispettivi partner.

- Actifio
- Alluxio
- Apache Kafka
- Punto di montaggio AWS
- Bridgestor
- Cantemo
- Citrix Content Collaboration
- Collibra (qualità minima dei dati Collibra versione 2024,02)
- CommVault 11
- Portale Ctera 6
- Dal
- Datadobi
- Storage di Data Dynamics X
- DefendX
- Dati di diskover
- Dremio
- EMAM
- Archivio di oggetti Fujifilm
- Server aziendale GitHub
- IBM FileNet
- IBM Spectrum Protect Plus
- Interica
- Impresa
- Cluster di big data Microsoft SQL Server
- Model9
- Modzy
- Moonwalk universale
- BELLO
- Nasuni
- Documento OpenText 16.4
- Documento OpenText 21.4
- OpenText InfoArchive 16 EP7
- OpenText Media Management 16.5 con CyanGate Cloud
- Panzura

- PixitMedia ngenea
- Point Archival Gateway 2.0
- Point Storage Manager 6.4
- Primestream
- Quantum StorNext 5.4.0.1
- Reveille v10 build 220706 o superiore
- Rubrik CDM
- s3a
- Signiant
- Fiocco di neve
- Ghiacciaio on-premise di Spectra Logic
- Smartstore Splunk
- Lo storage diventa semplice
- Trino
- Verniciare Enterprise 6.0.4
- Veeeam 12
- Veritas Enterprise Vault 14
- Veritas NetBackup 8.0
- Verticale 10.x
- Visoline
- Virtalica StorageFabric
- Weka v3.10 o versione successiva

Soluzioni di terze parti validate su StorageGRID con blocco a oggetti

Queste soluzioni sono state testate in collaborazione con i rispettivi partner.

- CommVault 11 Feature Release 26
- IBM FileNet
- Documento OpenText 21.4
- Veeeam 12
- Veritas Enterprise Vault 14.2.2
- Veritas NetBackup 10.1.1 e versioni successive

Soluzioni di terze parti supportate su StorageGRID

Queste soluzioni sono state testate.

- Archiviware
- Comunicazioni Axis
- Congruità360

- DataFrameworks
- Piattaforma EcoDigital DIVA
- Encoding.com
- Archivio di oggetti Fujifilm
- Archivio GE Centricity Enterprise
- Gitlab
- Hyland Acuo
- IBM Aspera
- Sistemi Milestone
- OnSSI
- Motore Reach
- SilverTrak
- SoftNAS
- QStar
- Velasea

Soluzioni di terze parti validate da StorageGRID 11.6

Le seguenti soluzioni di terze parti sono state validate per l'utilizzo con StorageGRID 11.6. + se la soluzione che stai cercando non è presente nell'elenco, contatta il tuo rappresentante commerciale NetApp.

Soluzioni di terze parti validate su StorageGRID

Queste soluzioni sono state testate in collaborazione con i rispettivi partner.

- Actifio
- Alluxio
- Apache Kafka
- Bridgestor
- Cantemo
- Citrix Content Collaboration
- CommVault 11
- Portale Ctera 6
- Dal
- Datadobi
- Storage di Data Dynamics X
- DefendX
- Dati di diskover
- Dremio

- EMAM
- Archivio di oggetti Fujifilm
- Server aziendale GitHub
- IBM FileNet
- IBM Spectrum Protect Plus
- Interica
- Impresa
- Cluster di big data Microsoft SQL Server
- Model9
- Modzy
- Moonwalk universale
- BELLO
- Nasuni
- Documento OpenText 16.4
- Documento OpenText 21.4
- OpenText InfoArchive 16 EP7
- OpenText Media Management 16.5 con CyanGate Cloud
- Panzura
- PixitMedia ngenea
- Point Archival Gateway 2.0
- Point Storage Manager 6.4
- Primestream
- Quantum StorNext 5.4.0.1
- Reveille v10 build 220706 o superiore
- Rubrik CDM
- s3a
- Signiant
- Fiocco di neve
- Ghiacciaio on-premise di Spectra Logic
- Smartstore Splunk
- Lo storage diventa semplice
- Trino
- Verniciare Enterprise 6.0.4
- Veeeam 12
- Veritas Enterprise Vault 14
- Veritas NetBackup 8.0
- Verticale 10.x

- Visoline
- Virtalica StorageFabric
- Weka v3.10 o versione successiva

Soluzioni di terze parti validate su StorageGRID con blocco a oggetti

Queste soluzioni sono state testate in collaborazione con i rispettivi partner.

- CommVault 11 Feature Release 26
- IBM FileNet
- Documento OpenText 21.4
- Veeeam 12
- Veritas Enterprise Vault 14.2.2
- Veritas NetBackup 10.1.1 e versioni successive

Soluzioni di terze parti supportate su StorageGRID

Queste soluzioni sono state testate.

- Archiviware
- Comunicazioni Axis
- Congruità360
- DataFrameworks
- Piattaforma EcoDigital DIVA
- Encoding.com
- Archivio di oggetti Fujifilm
- Archivio GE Centricity Enterprise
- Gitlab
- Hyland Acuo
- IBM Aspera
- Sistemi Milestone
- OnSSI
- Motore Reach
- SilverTrak
- SoftNAS
- QStar
- Velasea

Soluzioni di terze parti validate da StorageGRID 11.5

Le seguenti soluzioni di terze parti sono state validate per l'utilizzo con StorageGRID 11.5. + se la soluzione che stai cercando non è presente nell'elenco, contatta il tuo

rappresentante commerciale NetApp.

Soluzioni di terze parti validate su StorageGRID

Queste soluzioni sono state testate in collaborazione con i rispettivi partner.

- Actifio
- Alluxio
- Bridgestor
- Cantemo
- Citrix Content Collaboration
- CommVault 11
- Portale Ctera 6
- Dal
- Datadobi
- Storage di Data Dynamics X
- DefendX
- Interica
- Impresa
- Moonwalk universale
- BELLO
- Nasuni
- Documento OpenText 16.4
- Documento OpenText 21.4
- OpenText InfoArchive 16 EP7
- OpenText Media Management 16.5 con CyanGate Cloud
- Panzura
- Point Archival Gateway 2.0
- Point Storage Manager 6.4
- Primestream
- Quantum StorNext 5.4.0.1
- Rubrik CDM
- s3a
- Signiant
- Smartstore Splunk
- Trino
- Verniciare Enterprise 6.0.4
- Veeeam 11
- Veritas Enterprise Vault 11

- Veritas Enterprise Vault 12
- Veritas NetBackup 8.0
- Verticale 10.x
- Visoline
- Virtalica StorageFabric

Soluzioni di terze parti validate su StorageGRID con blocco a oggetti

Queste soluzioni sono state testate in collaborazione con i rispettivi partner.

- Documento OpenText 21.4
- Veeeam 11

Soluzioni di terze parti supportate su StorageGRID

Queste soluzioni sono state testate.

- Archiviware
- Comunicazioni Axis
- Congruità360
- DataFrameworks
- Piattaforma EcoDigital DIVA
- Encoding.com
- Archivio di oggetti Fujifilm
- Archivio GE Centricity Enterprise
- Gitlab
- Hyland Acuo
- IBM Aspera
- Sistemi Milestone
- OnSSI
- Motore Reach
- SilverTrak
- SoftNAS
- QStar
- Velasea

Soluzioni di terze parti validate da StorageGRID 11.4

Le seguenti soluzioni di terze parti sono state validate per l'utilizzo con StorageGRID 11.4. + se la soluzione che stai cercando non è presente nell'elenco, contatta il tuo rappresentante commerciale NetApp.

Soluzioni di terze parti validate su StorageGRID

Queste soluzioni sono state testate in collaborazione con i rispettivi partner.

- Actifio
- Bridgestor
- Cantemo
- Citrix Content Collaboration
- CommVault 11
- Portale Ctera 6
- Dal
- Datadobi
- Storage di Data Dynamics X
- DefendX
- Interica
- Impresa
- BELLO
- Nasuni
- Documento OpenText 16.4
- OpenText InfoArchive 16 EP7
- OpenText Media Management 16.5 con CyanGate Cloud
- Panzura
- Point Archival Gateway 2.0
- Point Storage Manager 6.4
- Primestream
- Quantum StorNext 5.4.0.1
- Rubrik CDM
- Signiant
- Smartstore Splunk
- Verniciare Enterprise 6.0.4
- Veeeam 9.5.4
- Veritas Enterprise Vault 11
- Veritas Enterprise Vault 12
- Veritas NetBackup 8.0
- Verticale 10.x
- Visoline

Soluzioni di terze parti supportate su StorageGRID

Queste soluzioni sono state testate.

- Archiviware
- Comunicazioni Axis
- Congruità360
- DataFrameworks
- Piattaforma EcoDigital DIVA
- Encoding.com
- Archivio di oggetti Fujifilm
- Archivio GE Centricity Enterprise
- Hyland Acuo
- IBM Aspera
- Sistemi Milestone
- OnSSI
- Motore Reach
- SilverTrak
- SoftNAS
- QStar
- Velasea

Soluzioni di terze parti validate da StorageGRID 11.3

Le seguenti soluzioni di terze parti sono state validate per l'utilizzo con StorageGRID 11.3. + se la soluzione che stai cercando non è presente nell'elenco, contatta il tuo rappresentante commerciale NetApp.

Soluzioni di terze parti validate su StorageGRID

Queste soluzioni sono state testate in collaborazione con i rispettivi partner.

- Actifio
- Bridgestor
- Cantemo
- Citrix Content Collaboration
- CommVault 11
- Portale Ctera 6
- Dal
- Datadobi
- Storage di Data Dynamics X

- DefendX
- Interica
- Impresa
- BELLO
- Nasuni
- Documento OpenText 16.4
- OpenText Media Management 16.5 con CyanGate Cloud
- Panzura
- Point Archival Gateway 2.0
- Point Storage Manager 6.4
- Primestream
- Quantum StorNext 5.4.0.1
- Rubrik CDM 5.0.1 p1-1342
- Signiant
- Smartstore Splunk
- Verniciare Enterprise 6.0.4
- Veeeam 9.5.4
- Veritas Enterprise Vault 11
- Veritas Enterprise Vault 12
- Veritas NetBackup 8.0
- Visoline

Soluzioni di terze parti supportate su StorageGRID

Queste soluzioni sono state testate.

- Archiviware
- Comunicazioni Axis
- Congruità360
- DataFrameworks
- Piattaforma EcoDigital DIVA
- Encoding.com
- Archivio di oggetti Fujifilm
- Archivio GE Centricity Enterprise
- Hyland Acuo
- IBM Aspera
- Sistemi Milestone
- OnSSI
- Motore Reach

- SilverTrak
- SoftNAS
- QStar
- Velasea

Soluzioni di terze parti validate da StorageGRID 11.2

Le seguenti soluzioni di terze parti sono state validate per l'utilizzo con StorageGRID 11.2. + se la soluzione che stai cercando non è presente nell'elenco, contatta il tuo rappresentante commerciale NetApp.

Soluzioni di terze parti validate su StorageGRID

Queste soluzioni sono state testate in collaborazione con i rispettivi partner.

- Actifio
- Bridgestor
- Cantemo
- Citrix Content Collaboration
- CommVault 11
- Portale Ctera 6
- Dal
- Datadobi
- Storage di Data Dynamics X
- DefendX
- Interica
- Impresa
- BELLO
- Nasuni
- Documento OpenText 16.4
- OpenText Media Management 16.5 con CyanGate Cloud
- Panzura
- Point Archival Gateway 2.0
- Point Storage Manager 6.4
- Primestream
- Quantum StorNext 5.4.0.1
- Rubrik CDM 5.0.1 p1-1342
- Signiant
- Smartstore Splunk
- Verniciare Enterprise 6.0.4

- Veeeam 9.5.4
- Veritas Enterprise Vault 11
- Veritas Enterprise Vault 12
- Veritas NetBackup 8.0
- Visoline

Soluzioni di terze parti supportate su StorageGRID

Queste soluzioni sono state testate.

- Archiviware
- Comunicazioni Axis
- Congruità360
- DataFrameworks
- Piattaforma EcoDigital DIVA
- Encoding.com
- Archivio di oggetti Fujifilm
- Archivio GE Centricity Enterprise
- Hyland Acuo
- IBM Aspera
- Sistemi Milestone
- OnSSI
- Motore Reach
- SilverTrak
- SoftNAS
- QStar
- Velasea

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".

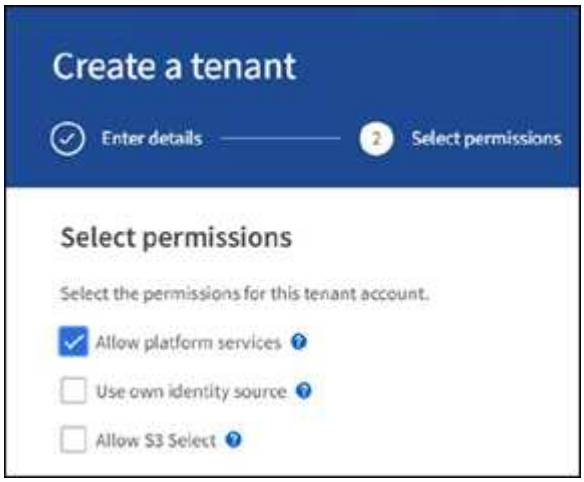
Il presente documento costituisce un'integrazione di "Guida al tenant di StorageGRID 11.6" inoltre, fornisce istruzioni dettagliate ed esempi per la configurazione di endpoint e bucket per i servizi di integrazione della ricerca. Le istruzioni di configurazione di Amazon Web Services (AWS) o on-premise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

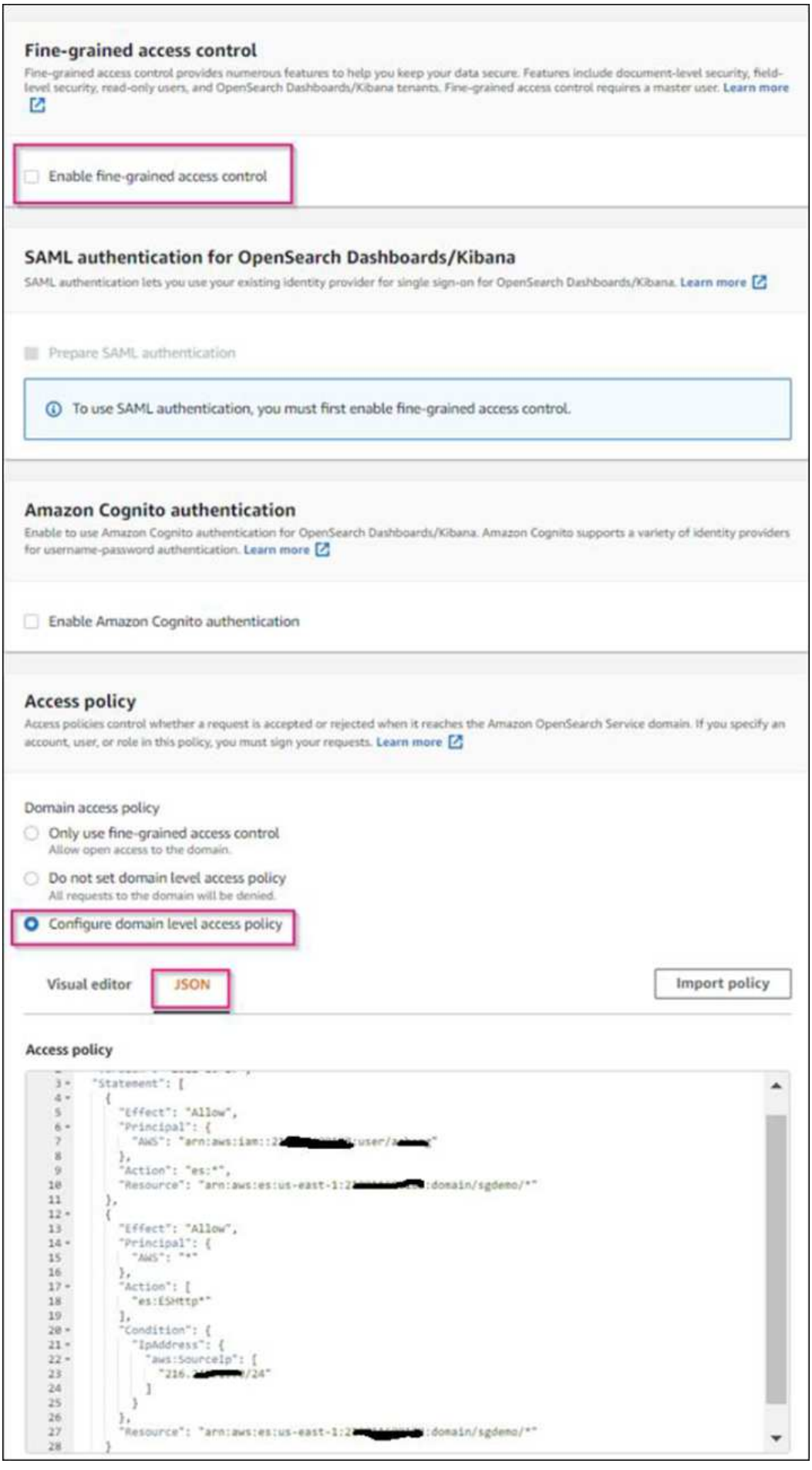
Utilizzare questa procedura per una configurazione rapida e semplice del servizio OpenSearch solo a scopo di test/demo. Se si utilizza on-premise Elasticsearch per i servizi di integrazione della ricerca, consultare la sezione Cerca servizi di integrazione con Elasticsearch on premise.

> 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:

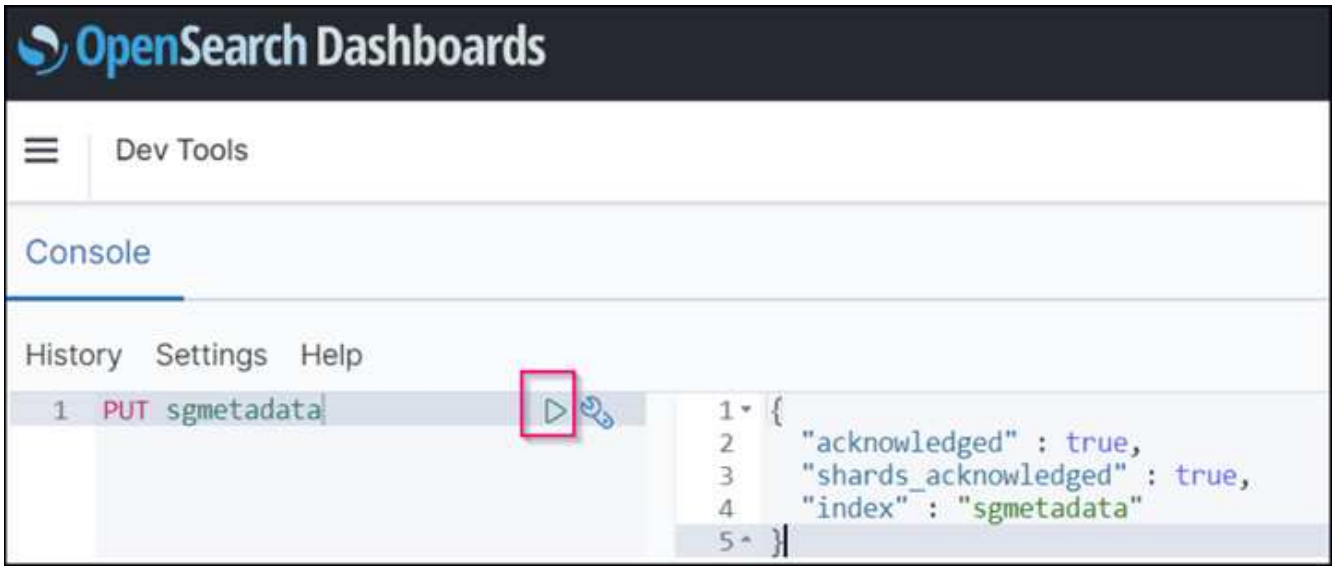
- Fase 4. Nome di dominio: Sgdemo
- Fase 10. Controllo degli accessi dettagliato: Deselezionare l'opzione Enable fine-Grained Access Control (attiva controllo degli accessi con grana fine).
- Fase 12. Access policy (criterio di accesso): Selezionare Configure Level Access Policy (Configura policy di 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/*"
        }
    ]
}
```

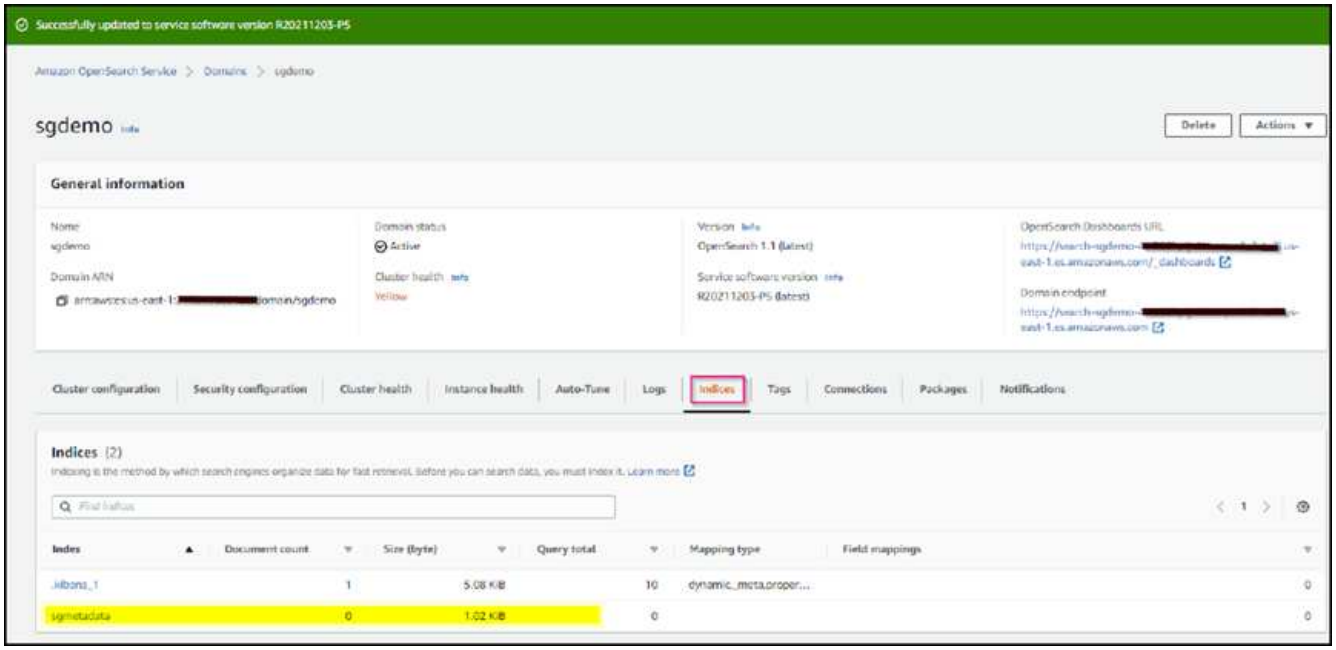

Fine-grained access control
Fine-grained access control provides numerous features to help you keep your data secure. Features include document-level security, field-level security, read-only users, and OpenSearch Dashboards/Kibana tenants. Fine-grained access control requires a master user. Learn more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



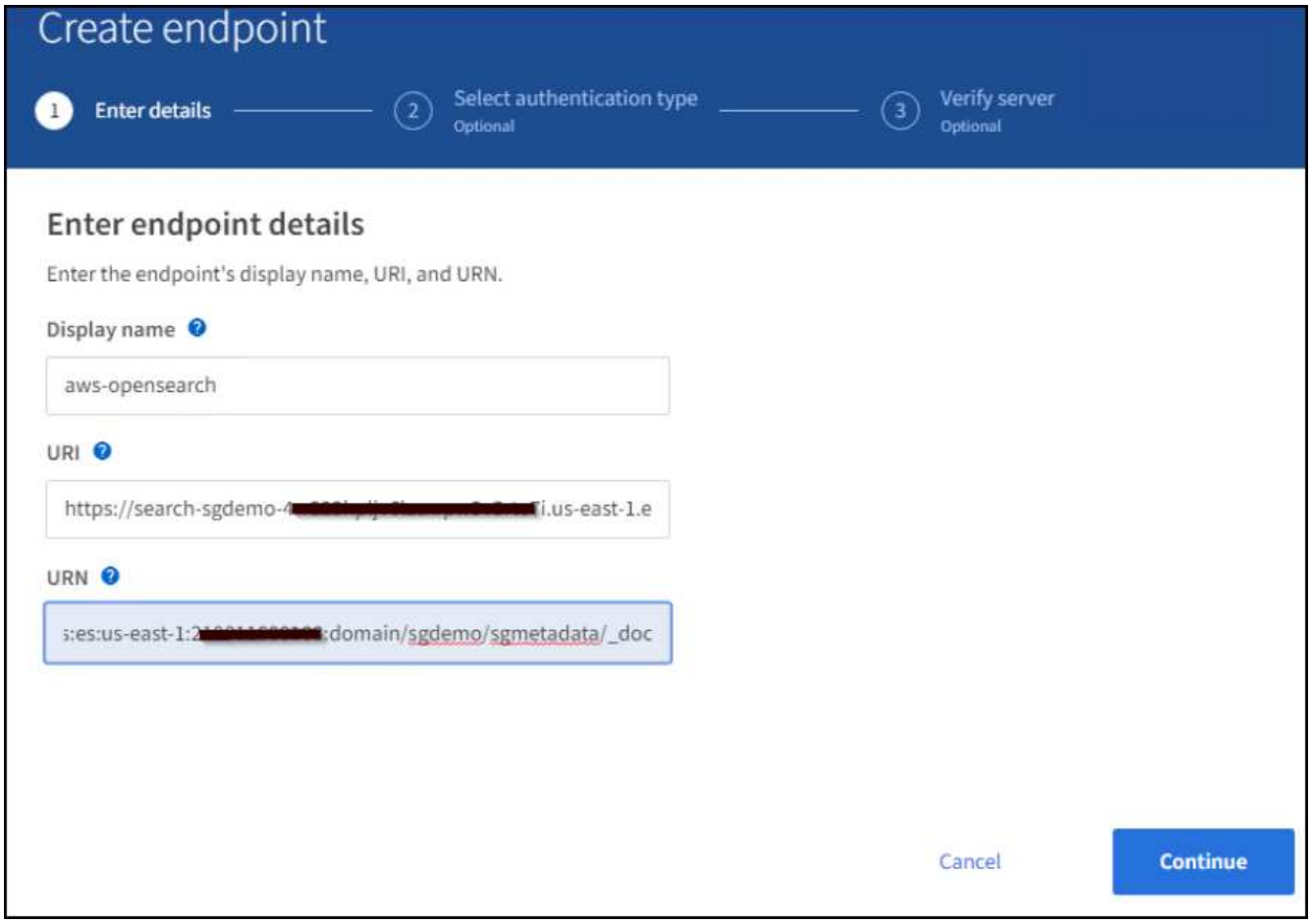
Configurazione degli endpoint dei servizi della piattaforma

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

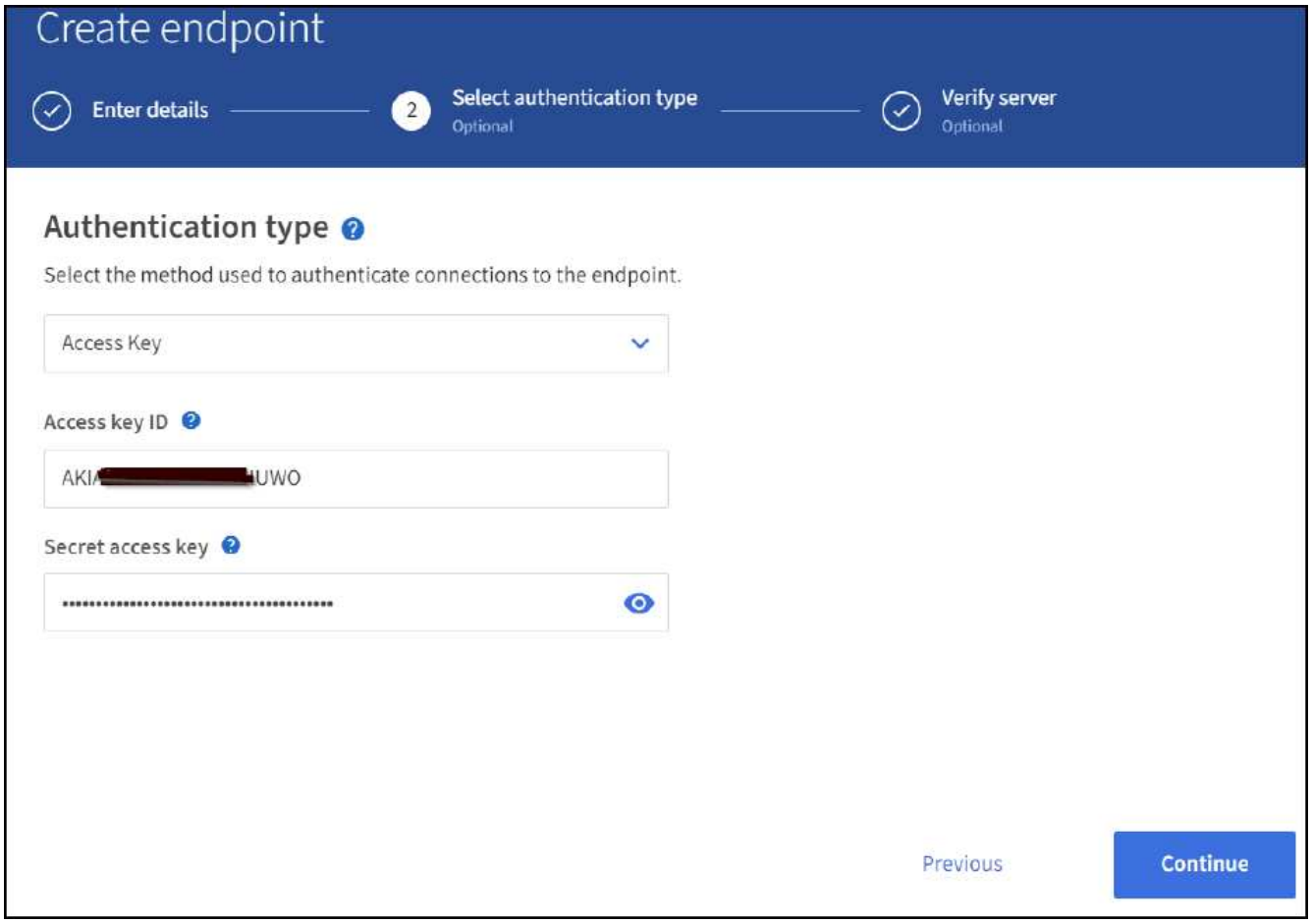
1. In Tenant Manager, andare a STORAGE(S3) > Platform Services Endpoint.
2. Fare clic su Create Endpoint (Crea endpoint), immettere quanto segue, quindi fare clic su Continue (continua):

   - 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.

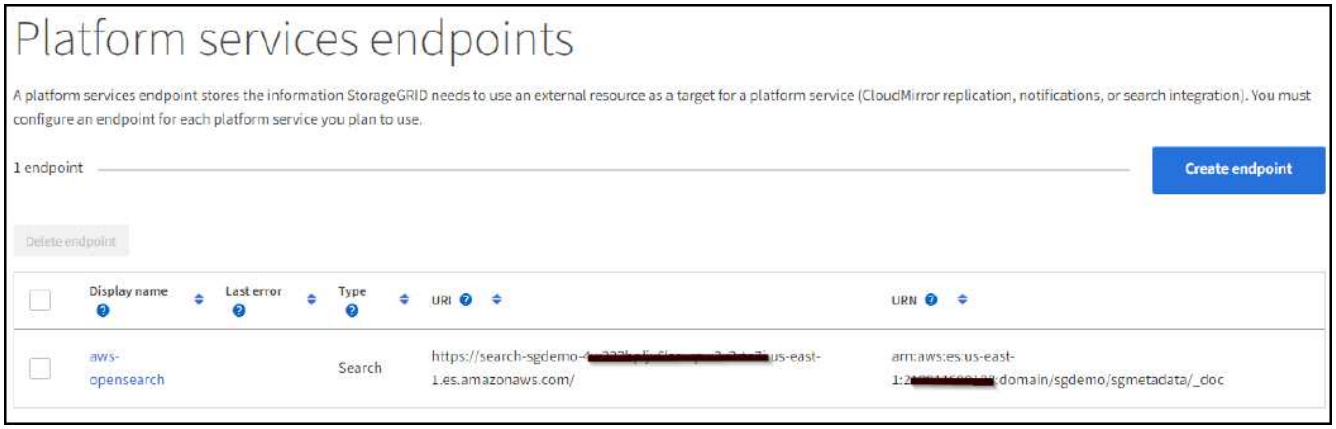
     In questo esempio, URN diventa `arn:aws:es:us-east-1:211234567890:domain/sgdemo /sgmedata/_doc`.



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.

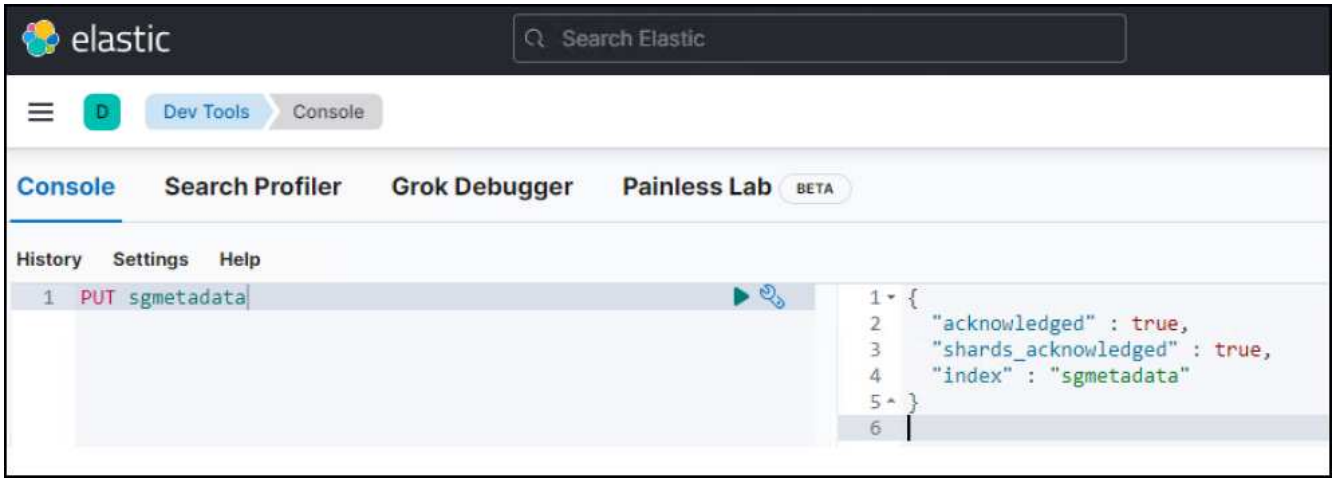
1. In a new terminal session, run:

```
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.

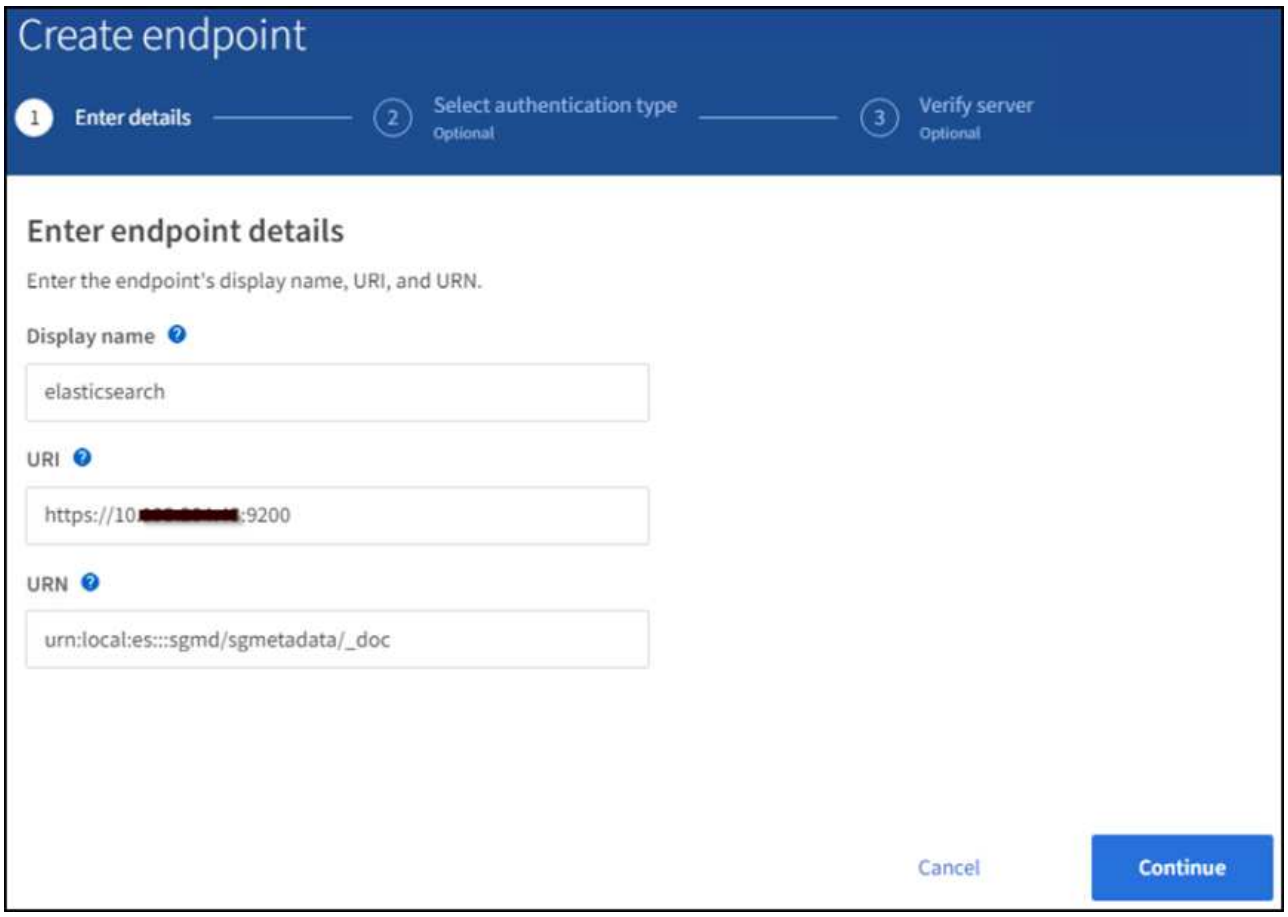
3. Una volta avviato il container Kibana docker, viene visualizzato il link URL `https://0.0.0.0:5601` viene visualizzato nella console. Sostituire 0.0.0.0 con l'indirizzo IP del server nell'URL.
4. Accedere all'interfaccia utente di Kibana utilizzando il nome utente `elastic` E la password generata 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.



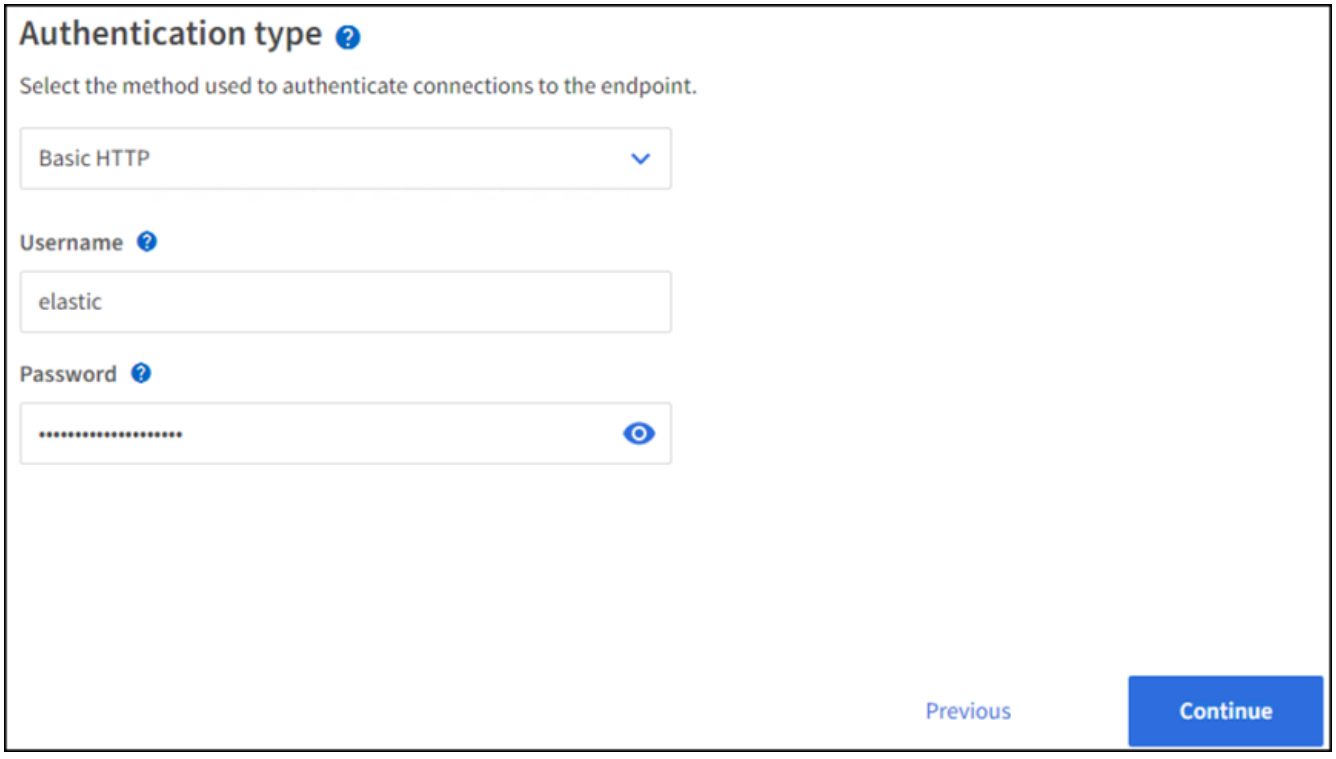
Configurazione degli endpoint dei servizi della piattaforma

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

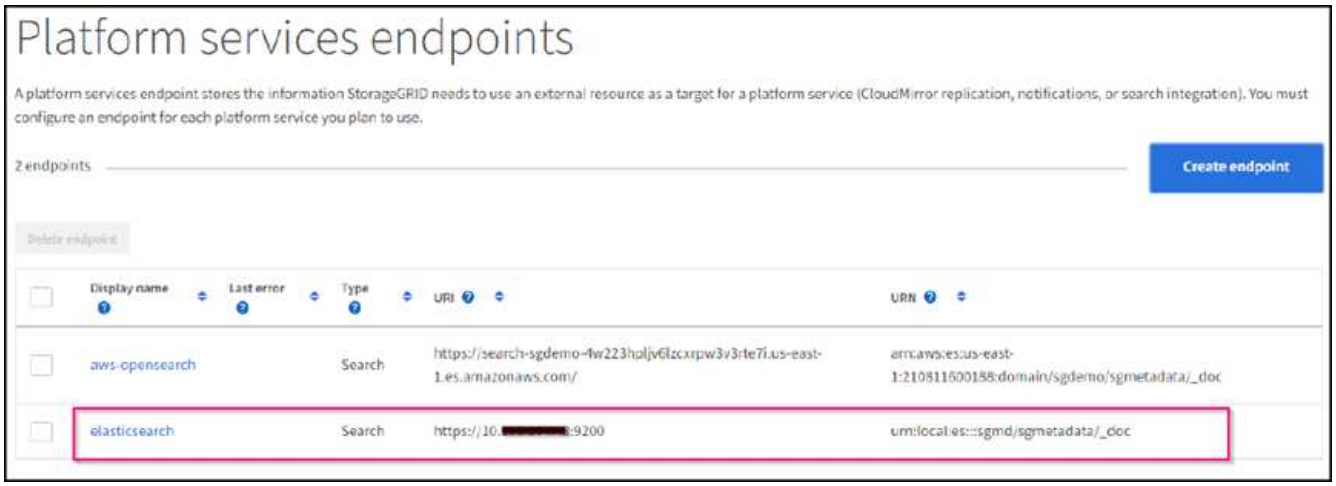
1. In Tenant Manager, andare a STORAGE(S3) > Platform Services Endpoint
2. Fare clic su Create Endpoint (Crea endpoint), immettere quanto segue, quindi fare clic su Continue (continua):
   - Esempio di nome visualizzato: `elasticsearch`
   - URI: `https://<elasticsearch-server-ip or hostname>:9200`
   - 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:

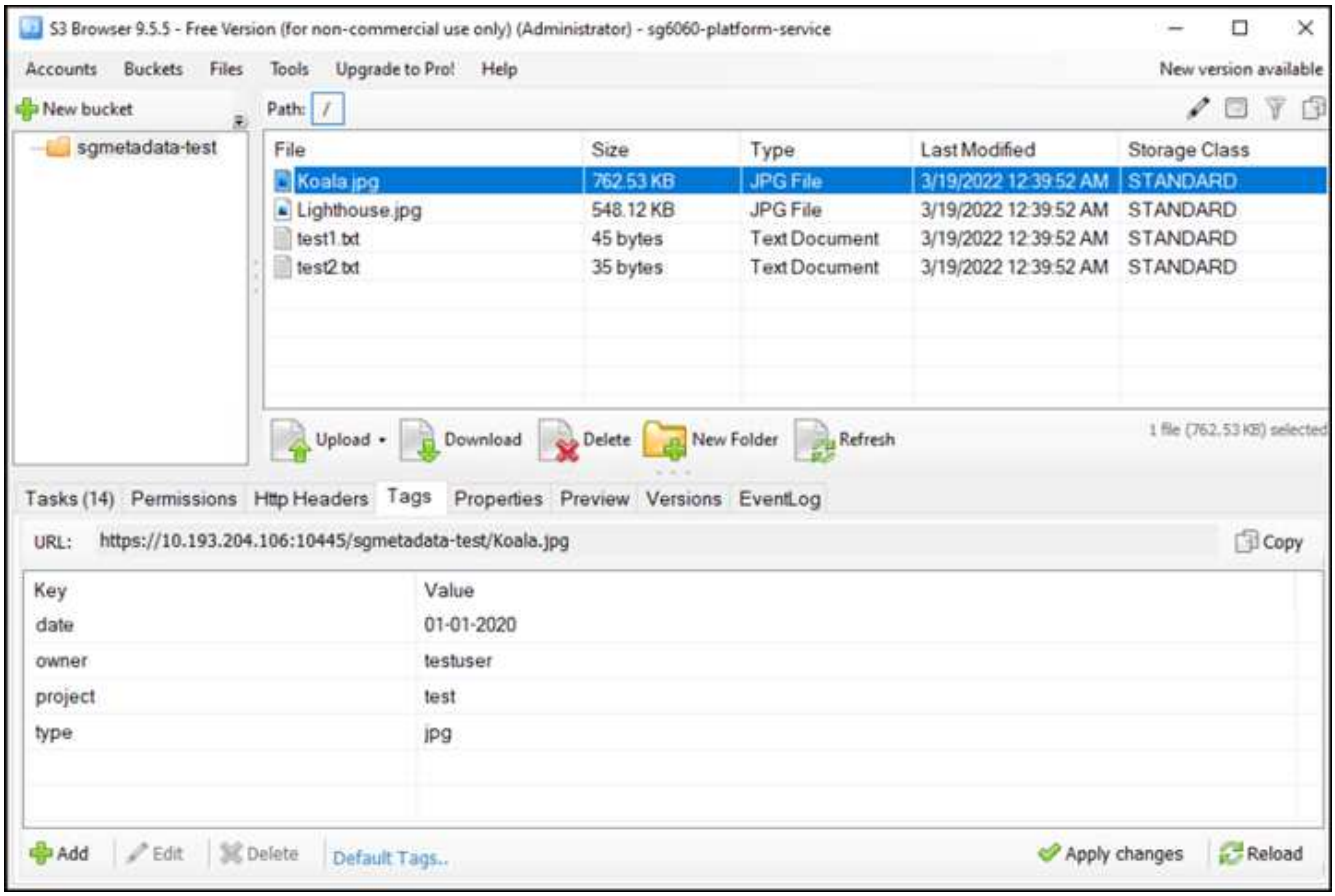
1. In Tenant Manager, andare a STORAGE(S3) > Bucket
2. Fare clic su Create bucket (Crea bucket), inserire il nome del bucket (ad esempio, `sgmetadata-test`) e accettare l'impostazione predefinita `us-east-1` regione.
3. Fare clic su continua > Crea bucket.
4. Per visualizzare la pagina Panoramica del 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.



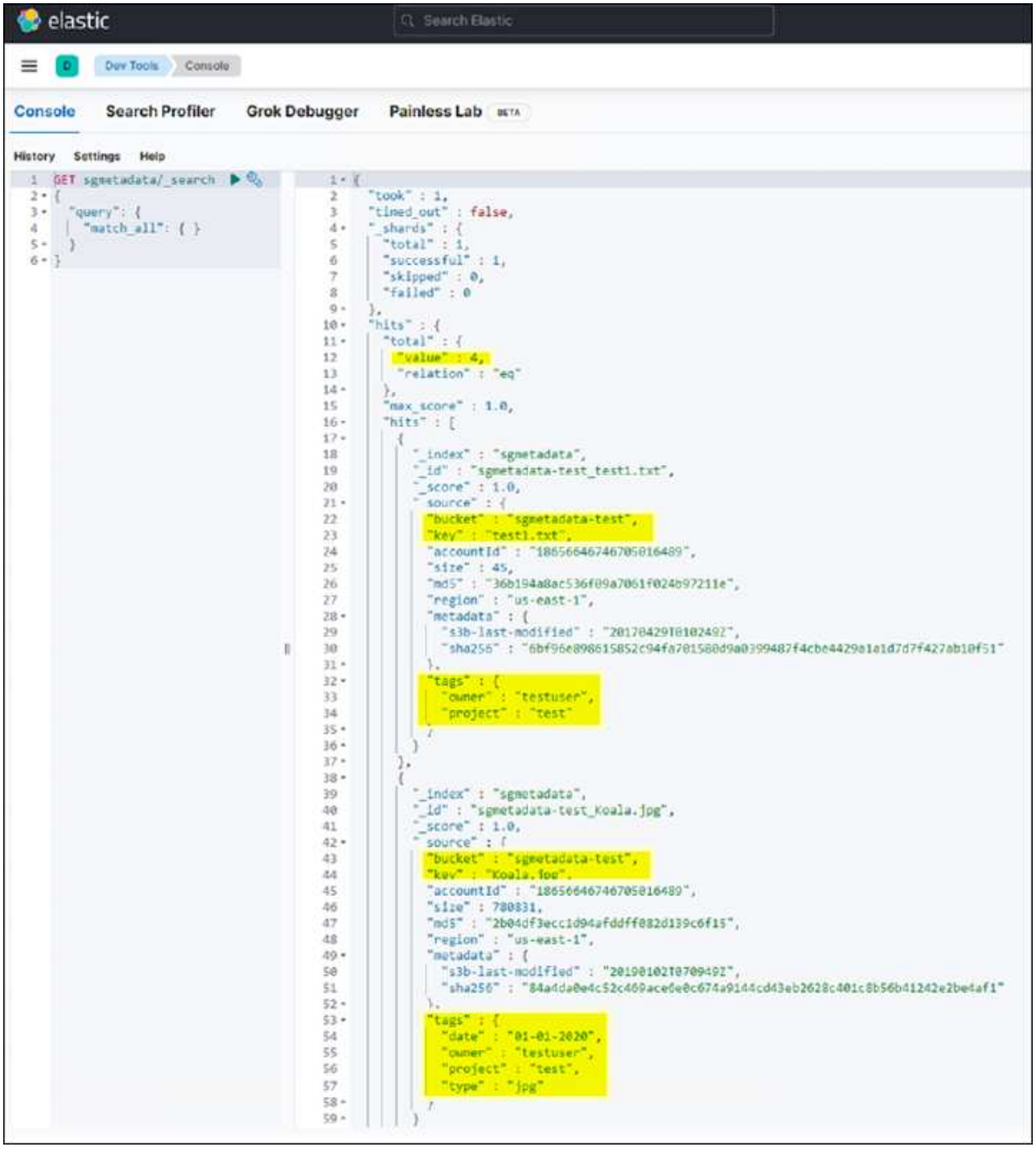
7. Utilizzare l'interfaccia utente di Kibana per verificare che i metadati dell'oggetto siano stati caricati nell'indice di sgmetadata.

   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.

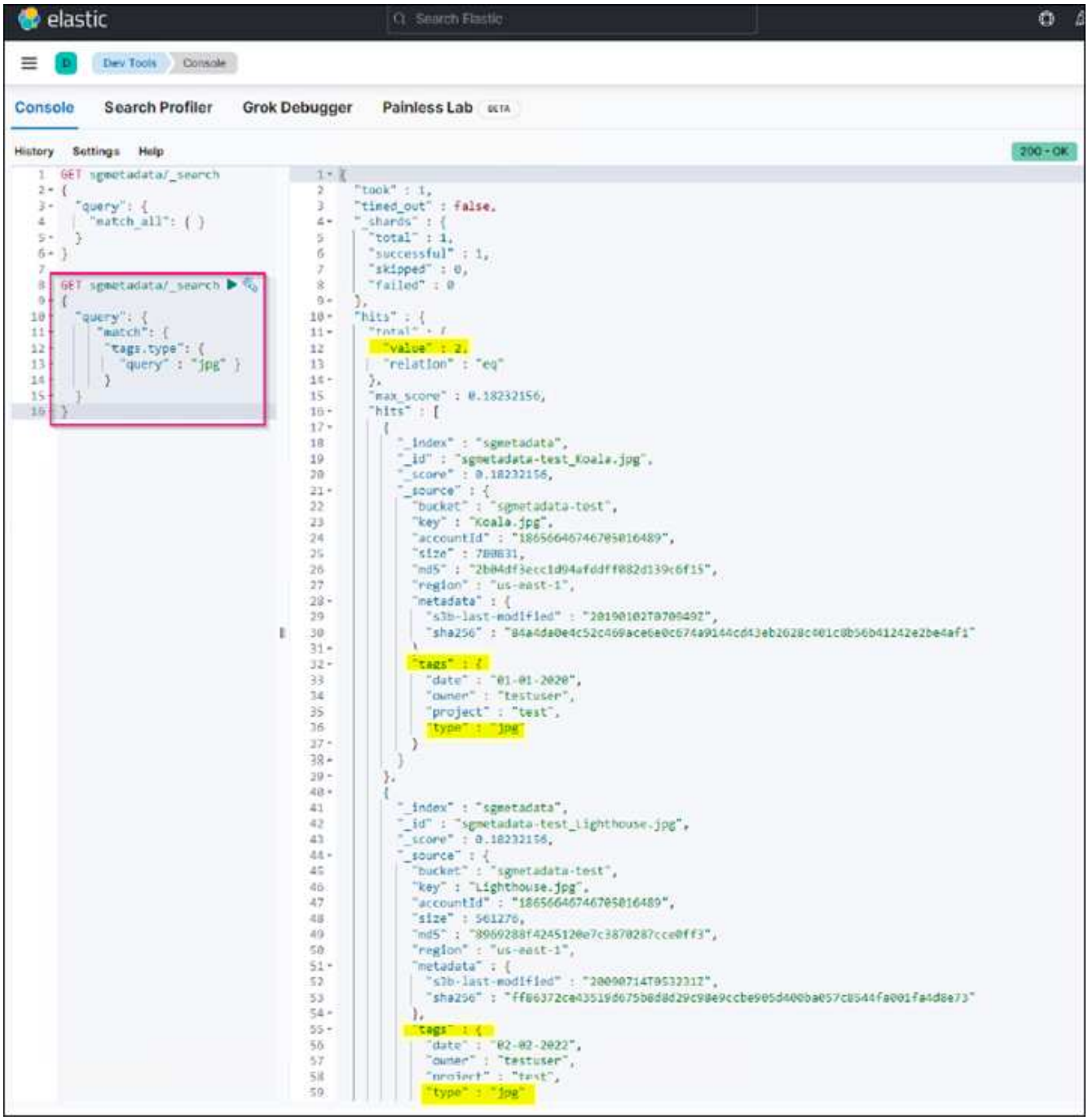
```
GET sgmetadata/_search
{
    "query": {
        "match_all": { }
}
}
```



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.

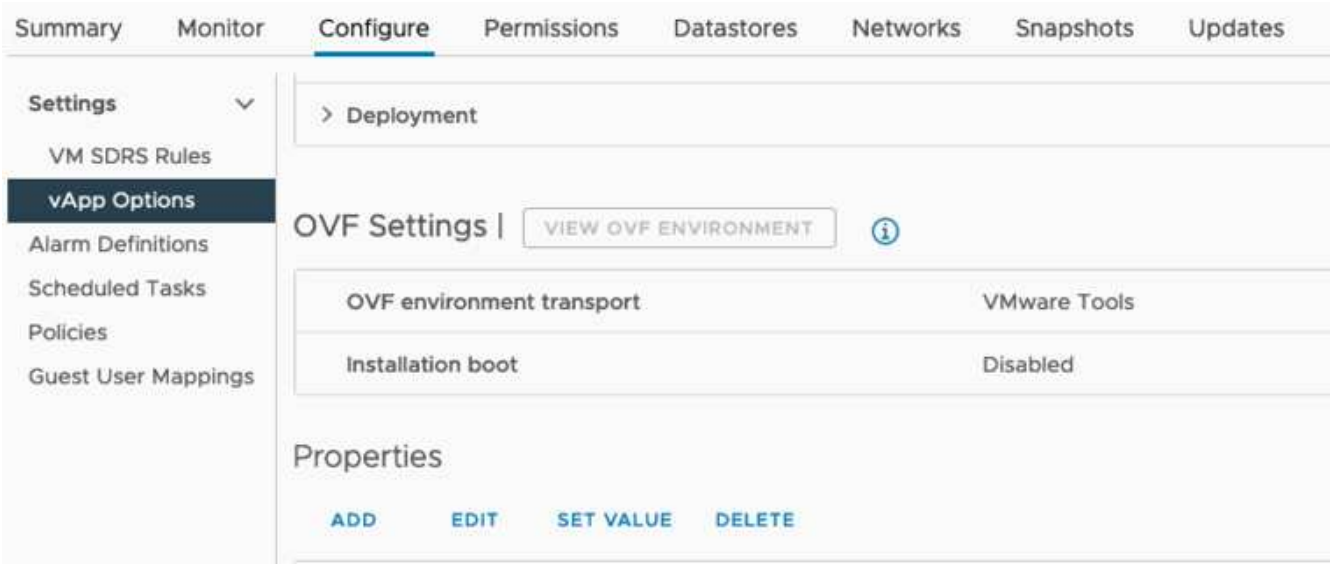
Implementare il nodo gateway sostitutivo

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.



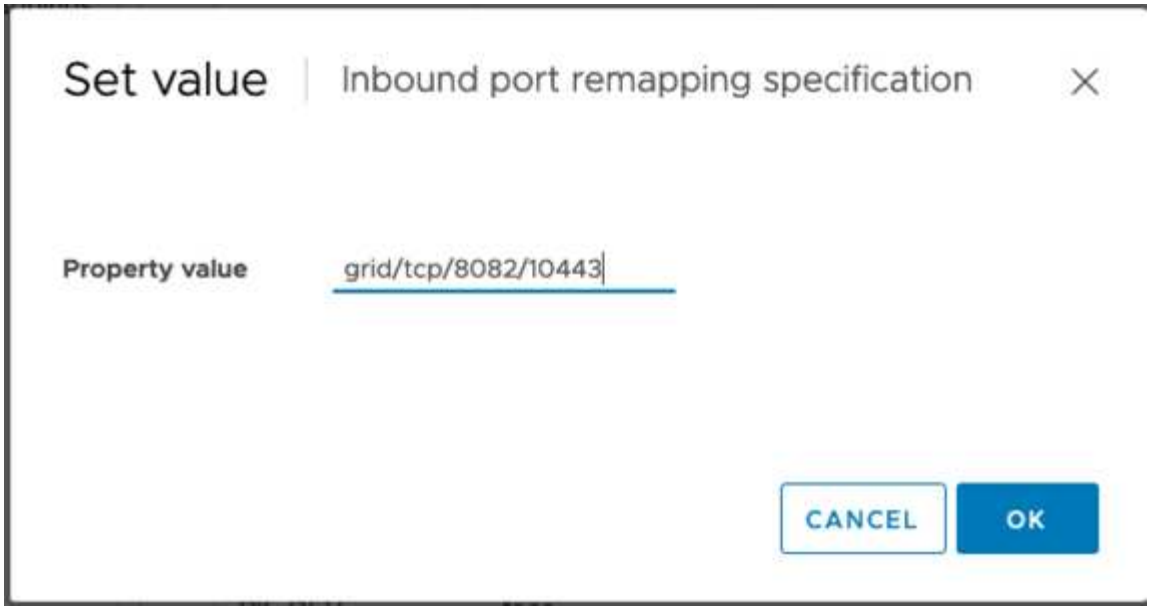
3. Scorrere fino alla sezione Proprietà e selezionare LA proprietà PORT_REMAP_INBOUND

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.

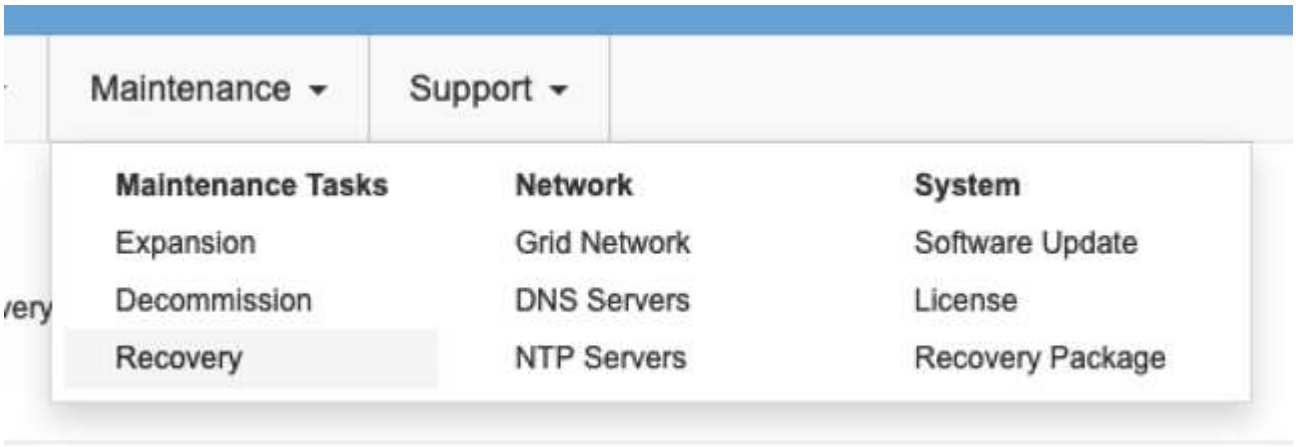


8. Se si utilizzano più reti, utilizzare una virgola (,) per separare le stringhe di rete, ad esempio Grid/tcp/8082/10443,admin/tcp/8082/10443,client/tcp/8082/10443

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`

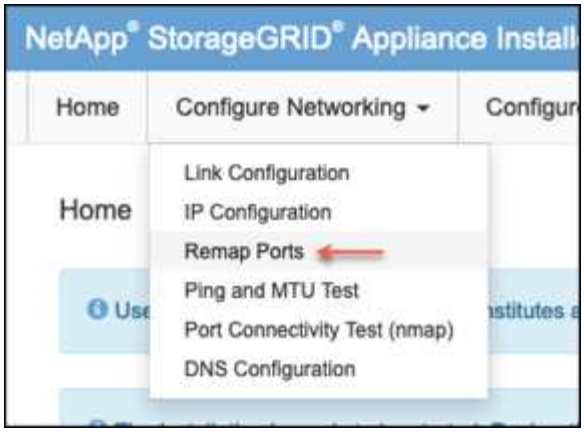
Ricostruire il nodo Admin

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`

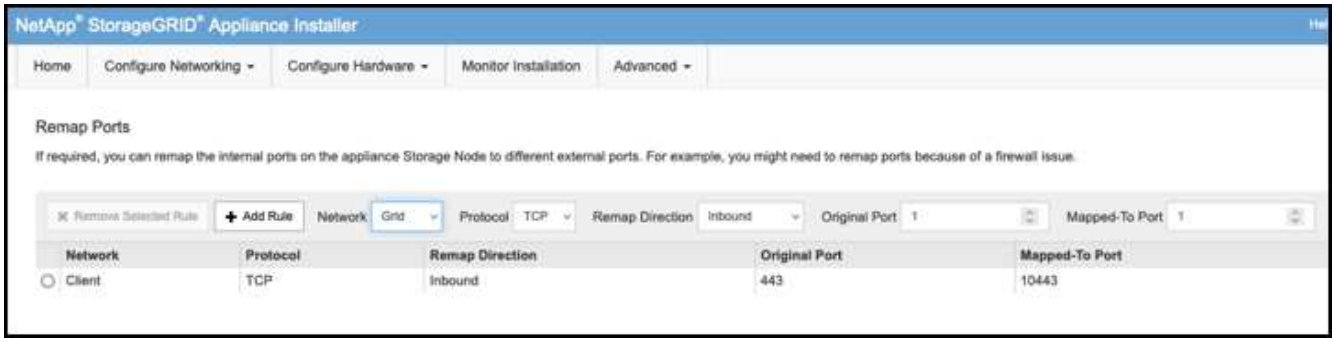
```
root@sg100-01:~ # sgareinstall
WARNING: All StorageGRID Webscale services on this node will be shut
down.
WARNING: Data stored on this node may be lost.
WARNING: You will have to reinstall StorageGRID Webscale to this
node.

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.

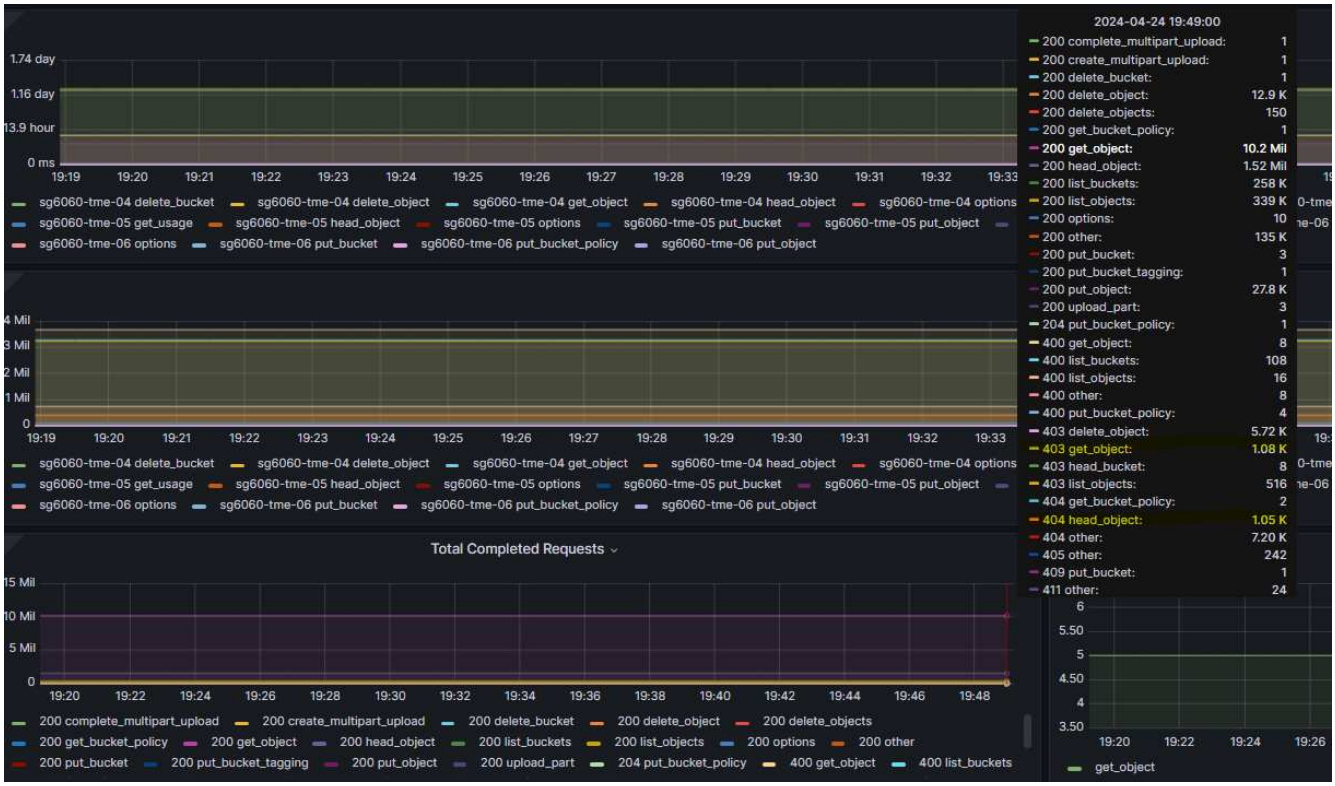
Se è necessario modificare la rete Grid di tutta la griglia, vedere "Modificare gli indirizzi IP per tutti i nodi nella griglia".

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
```

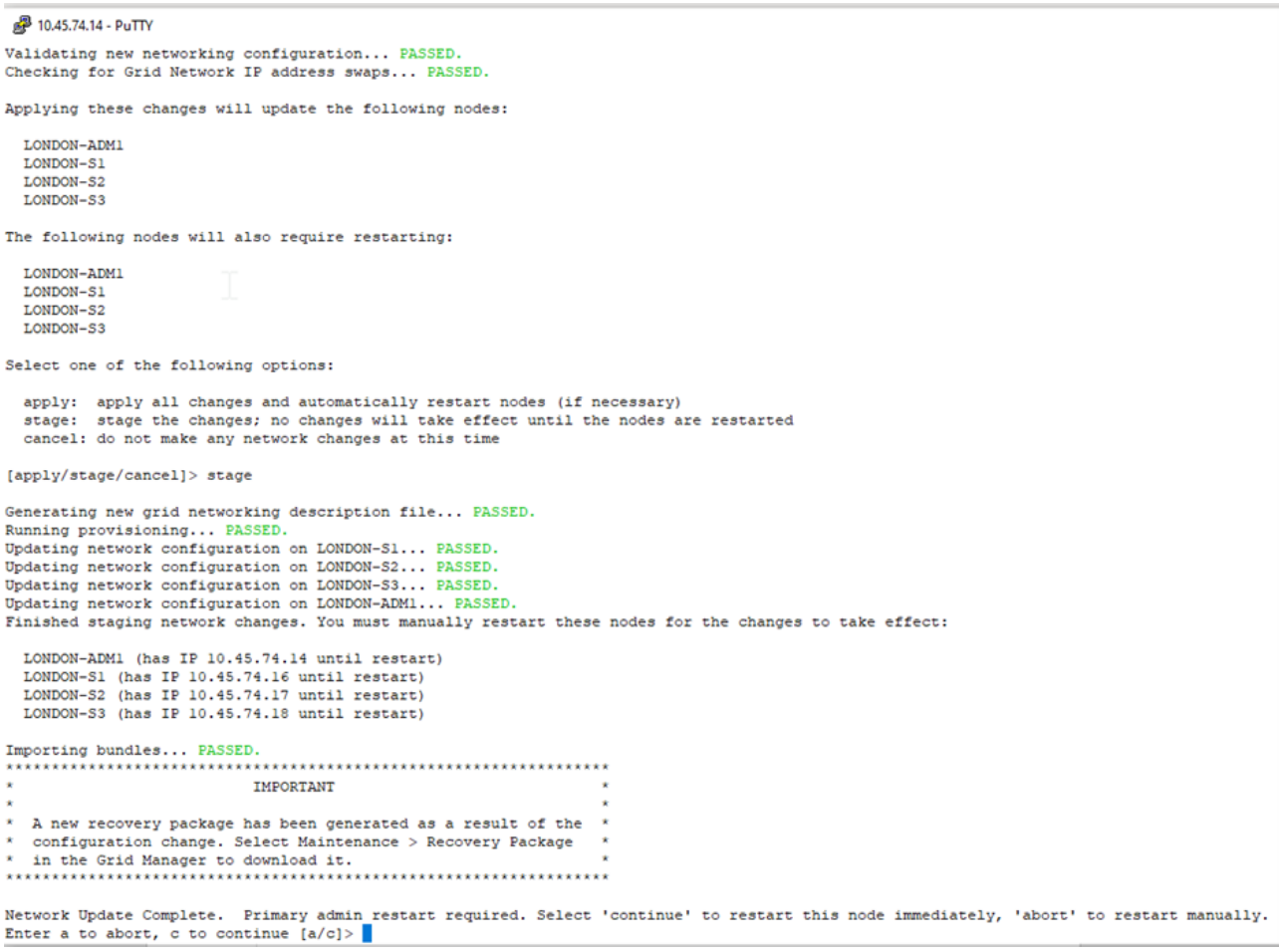
c. selezionare 10 per convalidare e applicare la modifica.

```
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
```

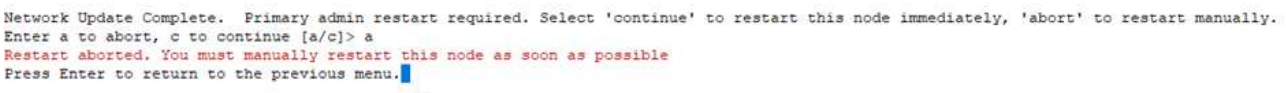
d. In questa fase è necessario selezionare **fase**.

```
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**



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



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.

Guide agli strumenti e alle applicazioni

USA il connettore S3A di Cloudera Hadoop con StorageGRID

Hadoop è da tempo la preferita dai data scientist. Hadoop consente l'elaborazione distribuita di grandi set di dati tra cluster di computer utilizzando semplici framework di programmazione. Hadoop è stato progettato per scalare da singoli server a migliaia di macchine, con ogni macchina in possesso di calcolo e storage locali.

Perché utilizzare S3A per i flussi di lavoro Hadoop?

Con la crescita del volume di dati nel tempo, l'approccio all'aggiunta di nuove macchine con il proprio calcolo e storage è diventato inefficiente. La scalabilità lineare crea delle sfide per l'utilizzo efficiente delle risorse e la gestione dell'infrastruttura.

Per affrontare queste sfide, il client Hadoop S3A offre i/o dalle performance elevate rispetto allo storage a oggetti S3. L'implementazione di un workflow Hadoop con S3A consente di sfruttare lo storage a oggetti come repository di dati e consente di separare calcolo e storage, il che consente di scalare calcolo e storage in modo indipendente. Il disaccoppiamento di calcolo e storage consente inoltre di dedicare la giusta quantità di risorse per i processi di calcolo e di fornire capacità in base alle dimensioni del set di dati. Pertanto, è possibile ridurre il TCO complessivo per i flussi di lavoro Hadoop.

Configurare S3A Connector per l'utilizzo di StorageGRID

Prerequisiti

- Un URL endpoint StorageGRID S3, una chiave di accesso s3 tenant e una chiave segreta per il test di connessione Hadoop S3A.
- Un cluster Cloudera e un'autorizzazione root o sudo a ciascun host del cluster per installare il pacchetto Java.

Ad aprile 2022, Java 11.0.14 con Cloudera 7.1.7 è stato testato rispetto a StorageGRID 11.5 e 11.6. Tuttavia, il numero di versione di Java potrebbe essere diverso al momento di una nuova installazione.

Installare il pacchetto Java

1. Controllare "Matrice di supporto di Cloudera" Per la versione JDK supportata.
2. Scaricare il "Pacchetto Java 11.x." Che corrisponde al sistema operativo del cluster Cloudera. Copiare questo pacchetto su ciascun host del cluster. In questo esempio, il pacchetto rpm viene utilizzato per CentOS.
3. Accedere a ciascun host come root o utilizzando un account con autorizzazione sudo. Eseguire le seguenti operazioni su ciascun host:
   a. Installare il pacchetto:

```
$ sudo rpm -Uvh jdk-11.0.14_linux-x64_bin.rpm
```

b. Controllare dove è installato Java. Se sono installate più versioni, impostare la nuova versione installata come predefinita:

```
alternatives --config java

There are 2 programs which provide 'java'.

  Selection    Command
-----------------------------------------------
 +1           /usr/java/jre1.8.0_291-amd64/bin/java
  2           /usr/java/jdk-11.0.14/bin/java

Enter to keep the current selection[+], or type selection number: 2
```

c. Aggiungere questa riga alla fine di `/etc/profile`. Il percorso deve corrispondere al percorso della selezione precedente:

```
export JAVA_HOME=/usr/java/jdk-11.0.14
```

d. Eseguire il seguente comando per rendere effettivo il profilo:

```
source /etc/profile
```

Configurazione di Cloudera HDFS S3A

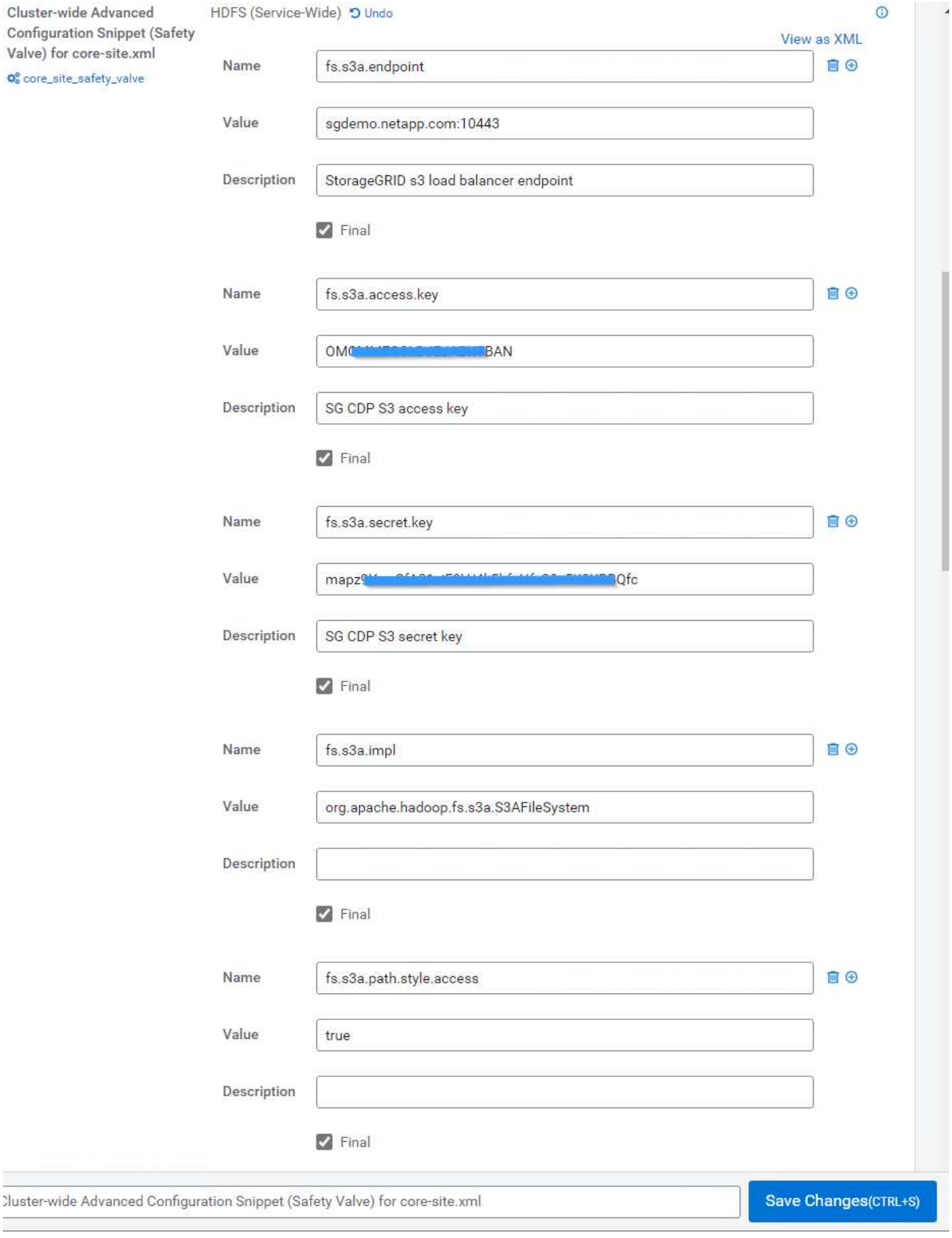
Fasi

1. Dalla GUI di Cloudera Manager, selezionare Clusters > HDFS e selezionare Configuration (Configurazione).
2. In CATEGORY (CATEGORIA), selezionare Advanced (Avanzate) e scorrere verso il basso per individuare `Cluster-wide Advanced Configuration Snippet (Safety Valve) for core-site.xml`.
3. Fare clic sul segno (+) e aggiungere le seguenti coppie di valori.

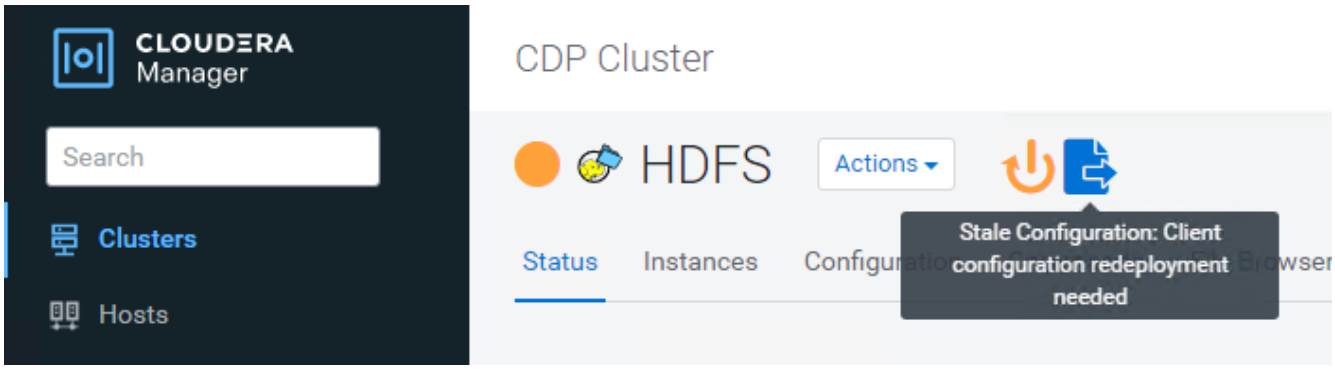
Nome	Valore
fs.s3a.access.key	*<chiave di accesso s3 tenant da StorageGRID>*
fs.s3a.secret.key	*<chiave segreta s3 tenant da StorageGRID>*
fs.s3a.connection.ssl.enabled	[true o false] (l'impostazione predefinita è https se questa voce non è presente)
fs.s3a.endpoint	*<StorageGRID S3 endpoint:porta>*

Nome	Valore
fs.s3a.impl	Org.apache.hadoop.fs.s3a.S3AFileSystem
fs.s3a.path.style.access	[true o false] (l'impostazione predefinita è lo stile dell'host virtuale se questa voce non è presente)

Esempio di screenshot



4. Fare clic sul pulsante Save Changes (Salva modifiche). Selezionare l'icona di configurazione obsoleta dalla barra dei menu di HDFS, selezionare Restart stale Services (Riavvia servizi obsoleti) nella pagina successiva e selezionare Restart Now (Riavvia ora).



Verificare la connessione S3A a StorageGRID

Eseguire un test di connessione di base

Accedere a uno degli host nel cluster Cloudera e immettere `hadoop fs -ls s3a://<bucket-name>/`.

Nell'esempio seguente viene utilizzato il path syle con un bucket hdfs-test preesistente e un oggetto test.

```
[root@ce-n1 ~]# hadoop fs -ls s3a://hdfs-test/
22/02/15 18:24:37 WARN impl.MetricsConfig: Cannot locate configuration:
tried hadoop-metrics2-s3a-file-system.properties,hadoop-
metrics2.properties
22/02/15 18:24:37 INFO impl.MetricsSystemImpl: Scheduled Metric snapshot
period at 10 second(s).
22/02/15 18:24:37 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system started
22/02/15 18:24:37 INFO Configuration.deprecation: No unit for
fs.s3a.connection.request.timeout(0) assuming SECONDS
Found 1 items
-rw-rw-rw-   1 root root       1679 2022-02-14 16:03 s3a://hdfs-test/test
22/02/15 18:24:38 INFO impl.MetricsSystemImpl: Stopping s3a-file-system
metrics system...
22/02/15 18:24:38 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system stopped.
22/02/15 18:24:38 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system shutdown complete.
```

Risoluzione dei problemi

Scenario 1

Utilizzare una connessione HTTPS a StorageGRID e ottenere un `handshake_failure` errore dopo un timeout di 15 minuti.

Motivo: versione precedente di JRE/JDK che utilizza una suite di crittografia TLS obsoleta o non supportata per la connessione a StorageGRID.

Esempio di messaggio di errore

```
[root@ce-n1 ~]# hadoop fs -ls s3a://hdfs-test/
22/02/15 18:52:34 WARN impl.MetricsConfig: Cannot locate configuration:
tried hadoop-metrics2-s3a-file-system.properties,hadoop-
metrics2.properties
22/02/15 18:52:34 INFO impl.MetricsSystemImpl: Scheduled Metric snapshot
period at 10 second(s).
22/02/15 18:52:34 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system started
22/02/15 18:52:35 INFO Configuration.deprecation: No unit for
fs.s3a.connection.request.timeout(0) assuming SECONDS
22/02/15 19:04:51 INFO impl.MetricsSystemImpl: Stopping s3a-file-system
metrics system...
22/02/15 19:04:51 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system stopped.
22/02/15 19:04:51 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system shutdown complete.
22/02/15 19:04:51 WARN fs.FileSystem: Failed to initialize fileystem
s3a://hdfs-test/: org.apache.hadoop.fs.s3a.AWSClientIOException:
doesBucketExistV2 on hdfs: com.amazonaws.SdkClientException: Unable to
execute HTTP request: Received fatal alert: handshake_failure: Unable to
execute HTTP request: Received fatal alert: handshake_failure
ls: doesBucketExistV2 on hdfs: com.amazonaws.SdkClientException: Unable to
execute HTTP request: Received fatal alert: handshake_failure: Unable to
execute HTTP request: Received fatal alert: handshake_failure
```

Risoluzione: assicurarsi che JDK 11.x o versione successiva sia installato e impostare la libreria Java predefinita. Fare riferimento a. Installare il pacchetto Java per ulteriori informazioni.

Scenario 2:

Impossibile connettersi a StorageGRID con messaggio di errore `Unable to find valid certification path to requested target`.

Motivo: il certificato del server endpoint StorageGRID S3 non è attendibile dal programma Java.

Esempio di messaggio di errore:

```
[root@hdp6 ~]# hadoop fs -ls s3a://hdfs-test/
22/03/11 20:58:12 WARN impl.MetricsConfig: Cannot locate configuration:
tried hadoop-metrics2-s3a-file-system.properties,hadoop-
metrics2.properties
22/03/11 20:58:13 INFO impl.MetricsSystemImpl: Scheduled Metric snapshot
period at 10 second(s).
22/03/11 20:58:13 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system started
22/03/11 20:58:13 INFO Configuration.deprecation: No unit for
fs.s3a.connection.request.timeout(0) assuming SECONDS
22/03/11 21:12:25 INFO impl.MetricsSystemImpl: Stopping s3a-file-system
metrics system...
22/03/11 21:12:25 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system stopped.
22/03/11 21:12:25 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system shutdown complete.
22/03/11 21:12:25 WARN fs.FileSystem: Failed to initialize fileystem
s3a://hdfs-test/: org.apache.hadoop.fs.s3a.AWSClientIOException:
doesBucketExistV2 on hdfs: com.amazonaws.SdkClientException: Unable to
execute HTTP request: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find
valid certification path to requested target: Unable to execute HTTP
request: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find
valid certification path to requested target
```

Risoluzione: NetApp consiglia di utilizzare un certificato server emesso da un'autorità pubblica nota per la firma del certificato per garantire che l'autenticazione sia sicura. In alternativa, aggiungere un certificato CA o server personalizzato all'archivio di trust Java.

Completare i seguenti passaggi per aggiungere un certificato CA o server personalizzato StorageGRID all'archivio di trust Java.

1. Eseguire il backup del file caacerts Java predefinito esistente.

```
cp -ap $JAVA_HOME/lib/security/cacerts
$JAVA_HOME/lib/security/cacerts.orig
```

2. Importare il certificato dell'endpoint StorageGRID S3 nell'archivio di trust Java.

```
keytool -import -trustcacerts -keystore $JAVA_HOME/lib/security/cacerts
-storepass changeit -noprompt -alias sg-lb -file <StorageGRID CA or
server cert in pem format>
```

Suggerimenti per la risoluzione dei problemi

1. Aumentare il livello di log di hadoop per ESEGUIRE IL DEBUG.

   ```
   export HADOOP_ROOT_LOGGER=hadoop.root.logger=DEBUG,console
   ```

2. Eseguire il comando e indirizzare i messaggi di log a error.log.

   ```
   hadoop fs -ls s3a://<bucket-name>/ &>error.log
   ```

Di Angela Cheng

Utilizzare S3cmd per testare e dimostrare l'accesso S3 su StorageGRID

S3cmd è un tool e client a riga di comando gratuito per le operazioni S3. È possibile utilizzare s3cmd per testare e dimostrare l'accesso s3 su StorageGRID.

Installare e configurare S3cmd

Per installare S3cmd su una workstation o su un server, scaricarlo da "Client S3 della riga di comando". S3cmd è preinstallato su ciascun nodo StorageGRID come strumento per facilitare la risoluzione dei problemi.

Fasi iniziali della configurazione

1. s3cmd --configure
2. Fornire solo access_key e secret_key, per il resto mantenere le impostazioni predefinite.
3. Verificare l'accesso con le credenziali fornite? [Y/n]: n (ignora il test perché non riesce)
4. Salvare le impostazioni? [s/N] e
   a. Configurazione salvata in '/root/.s3cfg'
5. In .s3cfg svuotare i campi host_base e host_bucket dopo il segno "=" :
   a. host_base =
   b. bucket_host =

> Se si specifica host_base e host_bucket nel passaggio 4, non è necessario specificare un endpoint con --host nella CLI. Esempio:

```
host_base = 192.168.1.91:8082
host_bucket = bucketX.192.168.1.91:8082
s3cmd ls s3://bucketX --no-check-certificate
```

Esempi di comandi di base

- **Creare un bucket:**

```
s3cmd mb s3://s3cmdbucket --host=<endpoint>:<port> --no-check-certificate
```

- **Elenca tutti i bucket:**

```
s3cmd ls --host=<endpoint>:<port> --no-check-certificate
```

- **Elenca tutti i bucket e il loro contenuto:**

```
s3cmd la --host=<endpoint>:<port> --no-check-certificate
```

- **Elenca oggetti in un bucket specifico:**

```
s3cmd ls s3://<bucket> --host=<endpoint>:<port> --no-check-certificate
```

- **Eliminare un bucket:**

```
s3cmd rb s3://s3cmdbucket --host=<endpoint>:<port> --no-check-certificate
```

- **Mettere un oggetto:**

```
s3cmd put <file> s3://<bucket> --host=<endpoint>:<port> --no-check-certificate
```

- **Ottenere un oggetto:**

```
s3cmd get s3://<bucket>/<object> <file> --host=<endpoint>:<port> --no-check
-certificate
```

- **Elimina un oggetto:**

```
s3cmd del s3://<bucket>/<object> --host=<endpoint>:<port> --no-check
-certificate
```

Di Aron Klein

Database in modalità Vertica Eon che utilizza NetApp StorageGRID come storage comune

Questa guida descrive la procedura per creare un database Vertica Eon Mode con storage comune su NetApp StorageGRID.

Introduzione

Vertica è un software per la gestione di database analitici. Si tratta di una piattaforma di storage colonnare progettata per gestire grandi volumi di dati, che consente performance di query molto veloci in uno scenario tradizionalmente intensivo. Un database Vertica viene eseguito in una delle due modalità: EON o Enterprise. Puoi implementare entrambe le modalità on-premise o nel cloud.

Le modalità EON ed Enterprise si differenziano principalmente per la posizione in cui memorizzano i dati:

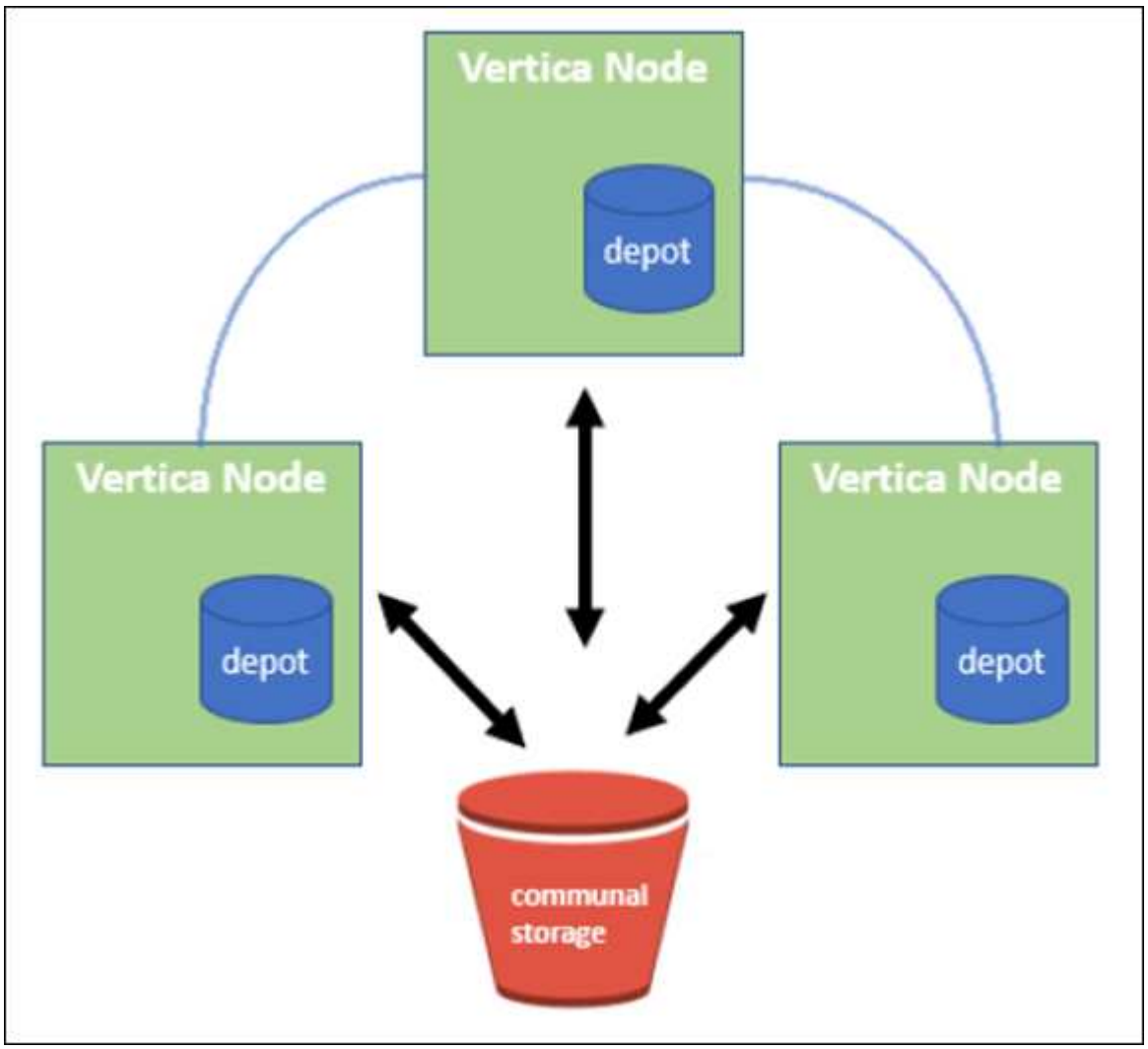
- I database EON Mode utilizzano lo storage comune per i propri dati. Questo è consigliato da Vertica.
- I database in modalità Enterprise memorizzano i dati localmente nel file system dei nodi che compongono

il database.

Architettura EON Mode

La modalità EON separa le risorse di calcolo dal livello di storage comune del database, consentendo la scalabilità separata di calcolo e storage. Vertica in Eon Mode è ottimizzato per gestire carichi di lavoro variabili e isolarli l'uno dall'altro utilizzando risorse di calcolo e storage separate.

La modalità EON memorizza i dati in un archivio di oggetti condiviso chiamato storage comune, un bucket S3, ospitato on-premise o su Amazon S3.



Storage in comune

Invece di memorizzare i dati in locale, Eon Mode utilizza una singola posizione di storage comune per tutti i dati e il catalogo (metadati). Lo storage comune è la posizione di storage centralizzata del database, condivisa tra i nodi del database.

Lo storage comune ha le seguenti proprietà:

- Lo storage comune nel cloud o in sede è più resiliente e meno suscettibile alla perdita di dati dovuta a guasti dello storage rispetto allo storage su disco su singoli computer.
- Tutti i dati possono essere letti da qualsiasi nodo utilizzando lo stesso percorso.

- La capacità non è limitata dallo spazio su disco sui nodi.
- Poiché i dati vengono memorizzati in maniera comune, è possibile scalare in modo elastico il cluster per soddisfare le esigenze in continua evoluzione. Se i dati fossero memorizzati localmente sui nodi, l'aggiunta o la rimozione di nodi richiederebbe lo spostamento di quantità significative di dati tra i nodi per spostarli dai nodi che vengono rimossi o nei nodi appena creati.

Il deposito

Uno svantaggio dello storage comune è la sua velocità. L'accesso ai dati da una posizione cloud condivisa è più lento rispetto alla lettura dal disco locale. Inoltre, la connessione allo storage comune può diventare un collo di bottiglia se molti nodi stanno leggendo i dati da esso contemporaneamente. Per migliorare la velocità di accesso ai dati, i nodi in un database Eon Mode mantengono una cache locale su disco di dati chiamata depot. Durante l'esecuzione di una query, i nodi verificano innanzitutto se i dati necessari si trovano nel deposito. In tal caso, la query viene completata utilizzando la copia locale dei dati. Se i dati non si trovano nel deposito, il nodo recupera i dati dallo storage comune e ne salva una copia nel deposito.

Consigli di NetApp StorageGRID

Vertica archivia i dati del database nello storage a oggetti sotto forma di migliaia (o milioni) di oggetti compressi (le dimensioni osservate sono da 200 a 500 MB per oggetto. Quando un utente esegue query di database, Vertica recupera l'intervallo di dati selezionato da questi oggetti compressi in parallelo utilizzando la chiamata get dell'intervallo di byte. Ogni byte-range GET è di circa 8 KB.

Durante il test delle query utente di depot del database da 10 TB, sono state inviate alla griglia da 4,000 a 10,000 richieste GET (byte-range GET) al secondo. Quando si esegue questo test utilizzando appliance SG6060, sebbene la percentuale di utilizzo della CPU per nodo appliance sia bassa (dal 20% al 30% circa), 2/3 CPU sono in attesa di i/O. Una percentuale molto piccola (da 0% a 0.5%) di attesa i/o viene osservata su SGF6024.

A causa dell'elevata richiesta di IOPS di piccole dimensioni con requisiti di latenza molto bassi (la media dovrebbe essere inferiore a 0.01 secondi), NetApp consiglia di utilizzare SFG6024 per i servizi di storage a oggetti. Se SG6060 è necessario per database di dimensioni molto grandi, il cliente deve collaborare con il team account Vertica per il dimensionamento dei depositi al fine di supportare il set di dati attivamente interrogato.

Per il nodo di amministrazione e il nodo di gateway API, il cliente può utilizzare SG100 o SG1000. La scelta dipende dal numero di richieste di query degli utenti in parallelo e dalle dimensioni del database. Se il cliente preferisce utilizzare un bilanciatore di carico di terze parti, NetApp consiglia un bilanciatore di carico dedicato per carichi di lavoro con domanda di performance elevate. Per il dimensionamento di StorageGRID, consulta l'account team di NetApp.

Altri consigli per la configurazione di StorageGRID includono:

- **Topologia della griglia**. Non mischiare SGF6024 con altri modelli di appliance di storage sullo stesso sito di grid. Se si preferisce utilizzare SG6060 per la protezione dell'archivio a lungo termine, mantenere SGF6024 con un sistema di bilanciamento del carico di rete dedicato nel proprio sito di rete (sito fisico o logico) per un database attivo al fine di migliorare le performance. La combinazione di diversi modelli di appliance sullo stesso sito riduce le performance complessive del sito.
- **Protezione dei dati**. Utilizzare copie replicate per la protezione. Non utilizzare la codifica di cancellazione per un database attivo. Il cliente può utilizzare l'erasure coding per una protezione a lungo termine dei database inattivi.
- **Non attivare la compressione della griglia**. Vertica comprime gli oggetti prima di memorizzarli nello storage a oggetti. L'abilitazione della compressione grid non consente di risparmiare ulteriormente l'utilizzo

dello storage e riduce significativamente le performance di BYTE-range GET.

- **HTTP rispetto alla connessione endpoint HTTPS S3**. Durante il test di benchmark, abbiamo osservato un miglioramento delle performance pari a circa il 5% quando si utilizza una connessione HTTP S3 dal cluster Vertica all'endpoint del bilanciamento del carico di StorageGRID. Questa scelta deve essere basata sui requisiti di sicurezza del cliente.

I consigli per una configurazione Vertica includono:

- **Le impostazioni predefinite del depot del database Vertica sono attivate (valore = 1) per le operazioni di lettura e scrittura**. NetApp consiglia vivamente di mantenere abilitate queste impostazioni di deposito per migliorare le performance.
- **Disattiva le limitazioni dello streaming**. Per informazioni dettagliate sulla configurazione, consultare la sezione Disattivazione delle limitazioni dello streaming.

Installazione della modalità Eon on on on-premise con storage comune su StorageGRID

Nelle sezioni seguenti viene descritta la procedura per installare la modalità Eon on on on-premise con lo storage comune su StorageGRID. La procedura per configurare lo storage a oggetti compatibile con S3 (Simple Storage Service) on-premise è simile alla procedura della guida Vertica, "Installare un database in modalità Eon on on on-premise".

Per il test funzionale è stata utilizzata la seguente configurazione:

- StorageGRID 11.4.0.4
- Verticale 10.1.0
- Tre macchine virtuali (VM) con sistema operativo CentOS 7.x per i nodi Vertica per formare un cluster. Questa configurazione è solo per il test funzionale, non per il cluster di database di produzione Vertica.

Questi tre nodi sono configurati con una chiave Secure Shell (SSH) per consentire SSH senza una password tra i nodi all'interno del cluster.

Informazioni richieste da NetApp StorageGRID

Per installare la modalità Eon on on on-premise con lo storage comune su StorageGRID, è necessario disporre delle seguenti informazioni sui prerequisiti.

- Indirizzo IP o FQDN (Fully Qualified Domain Name) e numero di porta dell'endpoint StorageGRID S3. Se si utilizza HTTPS, utilizzare un'autorità di certificazione personalizzata (CA) o un certificato SSL autofirmato implementato sull'endpoint StorageGRID S3.
- Nome bucket. Deve essere pre-esistente e vuoto.
- Access key ID (ID chiave di accesso) e secret access key (chiave di accesso segreta) con accesso in lettura e scrittura al bucket.

Creazione di un file di autorizzazione per accedere all'endpoint S3

I seguenti prerequisiti si applicano quando si crea un file di autorizzazione per accedere all'endpoint S3:

- Vertica è installato.
- Un cluster viene configurato, configurato e pronto per la creazione del database.

Per creare un file di autorizzazione per accedere all'endpoint S3, attenersi alla seguente procedura:

1. Accedere al nodo Vertica in cui si desidera eseguire `admintools` Per creare il database Eon Mode.

   L'utente predefinito è `dbadmin`, Creato durante l'installazione del cluster Vertica.

2. Utilizzare un editor di testo per creare un file in `/home/dbadmin` directory. Il nome del file può essere qualsiasi cosa si desideri, ad esempio `sg_auth.conf`.
3. Se l'endpoint S3 utilizza una porta HTTP standard 80 o una porta HTTPS 443, ignorare il numero della porta. Per utilizzare HTTPS, impostare i seguenti valori:

   ◦ `awsenablehttps = 1`, altrimenti impostare il valore su `0`.

   ◦ `awsauth = <s3 access key ID>:<secret access key>`

   ◦ `awsendpoint = <StorageGRID s3 endpoint>:<port>`

   Per utilizzare una CA personalizzata o un certificato SSL autofirmato per la connessione HTTPS dell'endpoint StorageGRID S3, specificare il percorso completo del file e il nome del file del certificato. Questo file deve trovarsi nella stessa posizione su ciascun nodo Vertica e disporre dell'autorizzazione di lettura per tutti gli utenti. Saltare questo passaggio se il certificato SSL StorageGRID S3 Endpoint è firmato da una CA pubblicamente conosciuta.

   - `awscafile = <filepath/filename>`

   Ad esempio, vedere il seguente file di esempio:

```
awsauth = MNVU4OYFAY2xyz123:03vuO4M4KmdfwffT8nqnBmnMVTr78Gu9wANabcxyz
awsendpoint = s3.england.connectlab.io:10443
awsenablehttps = 1
awscafile = /etc/custom-cert/grid.pem
```

+

> In un ambiente di produzione, il cliente deve implementare un certificato server firmato da una CA pubblicamente conosciuta su un endpoint di bilanciamento del carico StorageGRID S3.

Scelta di un percorso di deposito su tutti i nodi Vertica

Scegliere o creare una directory su ciascun nodo per il percorso di storage del deposito. La directory fornita per il parametro del percorso di storage del deposito deve essere la seguente:

- Lo stesso percorso su tutti i nodi del cluster (ad esempio, `/home/dbadmin/depot`)
- Essere leggibile e scrivibile dall'utente dbadmin
- Storage sufficiente

  Per impostazione predefinita, Vertica utilizza il 60% dello spazio del file system contenente la directory per lo storage del depot. È possibile limitare le dimensioni del deposito utilizzando `--depot-size` argomento in `create_db` comando. Vedere "Dimensionamento del cluster Vertica per un database in modalità Eon"

articolo per le linee guida generali sul dimensionamento di Vertica o consulta il tuo account manager Vertica.

Il `admintools create_db` lo strumento tenta di creare il percorso del deposito se non ne esiste uno.

Creazione del database Eon on on on-premise

Per creare il database Eon on on on-premise, attenersi alla seguente procedura:

1. Per creare il database, utilizzare `admintools create_db` tool.

   L'elenco seguente fornisce una breve spiegazione degli argomenti utilizzati in questo esempio. Consultare il documento Vertica per una spiegazione dettagliata di tutti gli argomenti richiesti e facoltativi.

   - -x <path/filename of authorization file created in "Creazione di un file di autorizzazione per accedere all'endpoint S3" >.

     I dettagli dell'autorizzazione vengono memorizzati all'interno del database dopo la creazione. È possibile rimuovere questo file per evitare di esporre la chiave segreta S3.

   - --communal-storage-location <s3://storagegrid bucketname>
   - -S <comma-separated list of Vertica nodes to be used for this database>
   - -d <name of database to be created>
   - -p <password to be set for this new database>. Ad esempio, vedere il seguente comando di esempio:

     ```
     admintools -t create_db -x sg_auth.conf --communal-storage
     -location=s3://vertica --depot-path=/home/dbadmin/depot --shard
     -count=6 -s vertica-vm1,vertica-vm2,vertica-vm3 -d vmart -p
     '<password>'
     ```

     La creazione di un nuovo database richiede diversi minuti a seconda del numero di nodi del database. Quando si crea un database per la prima volta, viene richiesto di accettare il Contratto di licenza.

Ad esempio, vedere il seguente file di autorizzazione di esempio e. `create db` comando:

```
[dbadmin@vertica-vm1 ~]$ cat sg_auth.conf
awsauth = MNVU4OYFAY2CPKVXVxxxx:03vuO4M4KmdfwffT8nqnBmnMVTr78Gu9wAN+xxxx
awsendpoint = s3.england.connectlab.io:10445
awsenablehttps = 1

[dbadmin@vertica-vm1 ~]$ admintools -t create_db -x sg_auth.conf
--communal-storage-location=s3://vertica --depot-path=/home/dbadmin/depot
--shard-count=6 -s vertica-vm1,vertica-vm2,vertica-vm3 -d vmart -p
'xxxxxxxx'
Default depot size in use
Distributing changes to cluster.
    Creating database vmart
```

```
    Starting bootstrap node v_vmart_node0007 (10.45.74.19)
    Starting nodes:
        v_vmart_node0007 (10.45.74.19)
    Starting Vertica on all nodes. Please wait, databases with a large
catalog may take a while to initialize.
    Node Status: v_vmart_node0007: (DOWN)
    Node Status: v_vmart_node0007: (DOWN)
    Node Status: v_vmart_node0007: (DOWN)
    Node Status: v_vmart_node0007: (UP)
    Creating database nodes
    Creating node v_vmart_node0008 (host 10.45.74.29)
    Creating node v_vmart_node0009 (host 10.45.74.39)
    Generating new configuration information
    Stopping single node db before adding additional nodes.
    Database shutdown complete
    Starting all nodes
Start hosts = ['10.45.74.19', '10.45.74.29', '10.45.74.39']
    Starting nodes:
        v_vmart_node0007 (10.45.74.19)
        v_vmart_node0008 (10.45.74.29)
        v_vmart_node0009 (10.45.74.39)
    Starting Vertica on all nodes. Please wait, databases with a large
catalog may take a while to initialize.
    Node Status: v_vmart_node0007: (DOWN) v_vmart_node0008: (DOWN)
v_vmart_node0009: (DOWN)
    Node Status: v_vmart_node0007: (DOWN) v_vmart_node0008: (DOWN)
v_vmart_node0009: (DOWN)
    Node Status: v_vmart_node0007: (DOWN) v_vmart_node0008: (DOWN)
v_vmart_node0009: (DOWN)
    Node Status: v_vmart_node0007: (DOWN) v_vmart_node0008: (DOWN)
v_vmart_node0009: (DOWN)
    Node Status: v_vmart_node0007: (UP) v_vmart_node0008: (UP)
v_vmart_node0009: (UP)
Creating depot locations for 3 nodes
Communal storage detected: rebalancing shards

Waiting for rebalance shards. We will wait for at most 36000 seconds.
Installing AWS package
    Success: package AWS installed
Installing ComplexTypes package
    Success: package ComplexTypes installed
Installing MachineLearning package
    Success: package MachineLearning installed
Installing ParquetExport package
    Success: package ParquetExport installed
Installing VFunctions package
```

```
    Success: package VFunctions installed
Installing approximate package
    Success: package approximate installed
Installing flextable package
    Success: package flextable installed
Installing kafka package
    Success: package kafka installed
Installing logsearch package
    Success: package logsearch installed
Installing place package
    Success: package place installed
Installing txtindex package
    Success: package txtindex installed
Installing voltagesecure package
    Success: package voltagesecure installed
Syncing catalog on vmart with 2000 attempts.
Database creation SQL tasks completed successfully. Database vmart created
successfully.
```

Dimensione oggetto (byte)	Percorso completo della chiave bucket/oggetto
61	s3://vertica/051/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a07/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a07_0_0.dfs
145	s3://vertica/2c4/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a3d/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a3d_0_0.dfs
146	s3://vertica/33c/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a1d/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a1d_0_0.dfs
40	s3://vertica/382/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a31/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a31_0_0.dfs
145	s3://vertica/42f/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a21/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a21_0_0.dfs

Dimensione oggetto (byte)	Percorso completo della chiave bucket/oggetto
34	s3://vertica/472/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a25/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a25_0_0.dfs
41	s3://vertica/476/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a2d/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a2d_0_0.dfs
61	s3://vertica/52a/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a5d/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a5d_0_0.dfs
131	s3://vertica/5d2/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a19/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a19_0_0.dfs
91	s3://vertica/5f7/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a11/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a11_0_0.dfs
118	s3://vertica/82d/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a15/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a15_0_0.dfs
115	s3://vertica/9a2/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a61/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a61_0_0.dfs
33	s3://vertica/acd/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a29/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a29_0_0.dfs
133	s3://vertica/b98/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a4d/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a4d_0_0.dfs

Dimensione oggetto (byte)	Percorso completo della chiave bucket/oggetto
38	s3://vertica/db3/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a49/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a49_0_0.dfs
38	s3://vertica/eba/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a59/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a59_0_0.dfs
21521920	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000215e2/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000215e2.tar
6865408	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021602/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021602.tar
204217344	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021610/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021610.tar
16109056	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000217e0/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000217e0.tar
12853248	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021800/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021800.tar
8937984	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a000000002187a/026d63ae9d4a33237bf0e2c2cf2a794a00a000000002187a.tar
56260608	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000218b2/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000218b2.tar

Dimensione oggetto (byte)	Percorso completo della chiave bucket/oggetto
53947904	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000219ba/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000219ba.tar
44932608	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000219de/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000219de.tar
256306688	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a6e/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a6e.tar
8062464	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021e34/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021e34.tar
20024832	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021e70/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021e70.tar
10444	s3://vertica/metadata/VMart/cluster_config.json
823266	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c13_13/chkpt_1.cat.gz
254	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c13_13/completed
2958	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c2_2/chkpt_1.cat.gz

Dimensione oggetto (byte)	Percorso completo della chiave bucket/oggetto
231	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c2_2/completed
822521	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c4_4/chkpt_1.cat.gz
231	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c4_4/completed
746513	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_14_g14.cat
2596	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_3_g3.cat.gz
821065	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_4_g4.cat.gz
6440	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_5_g5.cat
8518	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_8_g8.cat
0	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/tiered_catalog.cat
822922	s3://vertica/metadata/VMart/nodes/v_vmart_node0017/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c14_7/chkpt_1.cat.gz
232	s3://vertica/metadata/VMart/nodes/v_vmart_node0017/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c14_7/completed

Dimensione oggetto (byte)	Percorso completo della chiave bucket/oggetto
822930	s3://vertica/metadata/VMart/nodes/v_vmart_node0017/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_14_g7.cat.gz
755033	s3://vertica/metadata/VMart/nodes/v_vmart_node0017/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_15_g8.cat
0	s3://vertica/metadata/VMart/nodes/v_vmart_node0017/Catalog/859703b06a3456d95d0be28575a673/tiered_catalog.cat
822922	s3://vertica/metadata/VMart/nodes/v_vmart_node0018/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c14_7/chkpt_1.cat.gz
232	s3://vertica/metadata/VMart/nodes/v_vmart_node0018/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c14_7/completed
822930	s3://vertica/metadata/VMart/nodes/v_vmart_node0018/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_14_g7.cat.gz
755033	s3://vertica/metadata/VMart/nodes/v_vmart_node0018/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_15_g8.cat
0	s3://vertica/metadata/VMart/nodes/v_vmart_node0018/Catalog/859703b06a3456d95d0be28575a673/tiered_catalog.cat

Disattivazione delle limitazioni dello streaming

Questa procedura si basa sulla guida Vertica per altri storage a oggetti on-premise e deve essere applicabile a StorageGRID.

1. Dopo aver creato il database, disattivare `AWSStreamingConnectionPercentage` parametro di configurazione impostandolo su `0`. Questa impostazione non è necessaria per un'installazione on Mode on-premise con storage comune. Questo parametro di configurazione controlla il numero di connessioni all'archivio di oggetti utilizzate da Vertica per le letture in streaming. In un ambiente cloud, questa impostazione consente di evitare che i dati in streaming dall'archivio di oggetti utilizzino tutti gli handle di file disponibili. In questo modo, alcuni handle di file sono disponibili per altre operazioni di archiviazione di oggetti. A causa della bassa latenza degli archivi di oggetti on-premise, questa opzione non è necessaria.
2. Utilizzare un `vsql` per aggiornare il valore del parametro. La password è la password del database

impostata in "creazione del database Eon on on on-premise". Ad esempio, vedere il seguente esempio di output:

```
[dbadmin@vertica-vm1 ~]$ vsql
Password:
Welcome to vsql, the Vertica Analytic Database interactive terminal.
Type:   \h or \? for help with vsql commands
        \g or terminate with semicolon to execute query
        \q to quit
dbadmin=> ALTER DATABASE DEFAULT SET PARAMETER
AWSStreamingConnectionPercentage = 0; ALTER DATABASE
dbadmin=> \q
```

Verifica delle impostazioni del deposito in corso

Le impostazioni predefinite del depot del database Vertica sono attivate (valore = 1) per le operazioni di lettura e scrittura. NetApp consiglia vivamente di mantenere abilitate queste impostazioni di deposito per migliorare le performance.

```
vsql -c 'show current all;' | grep -i UseDepot
DATABASE | UseDepotForReads | 1
DATABASE | UseDepotForWrites | 1
```

Caricamento dei dati di esempio (opzionale)

Se questo database è destinato al test e verrà rimosso, è possibile caricare i dati campione in questo database per il test. Vertica viene fornito con un set di dati di esempio, VMart, disponibile in `/opt/vertica/examples/VMart_Schema/` Su ogni nodo Vertica. Sono disponibili ulteriori informazioni su questo set di dati di esempio "qui".

Per caricare i dati di esempio, procedere come segue:

1. Accedere come dbadmin a uno dei nodi Vertica: cd /opt/vertica/exemes/VMart_Schema/
2. Caricare i dati di esempio nel database e inserire la password del database quando richiesto nelle fasi c e d:
   a. `cd /opt/vertica/examples/VMart_Schema`
   b. `./vmart_gen`
   c. `vsql < vmart_define_schema.sql`
   d. `vsql < vmart_load_data.sql`
3. Esistono più query SQL predefinite, alcune delle quali possono essere eseguite per confermare che i dati di test sono stati caricati correttamente nel database. Ad esempio: `vsql < vmart_queries1.sql`

Dove trovare ulteriori informazioni

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

siti Web:

- "Documentazione del prodotto NetApp StorageGRID 11,7"
- "Scheda tecnica di StorageGRID"
- "Documentazione del prodotto Vertica 10.1"

Cronologia delle versioni

Versione	Data	Cronologia delle versioni del documento
Versione 1.0	Settembre 2021	Release iniziale.

Di Angela Cheng

Analisi dei log StorageGRID con stack ELK

Con la funzione di inoltro syslog di StorageGRID 11.6, è possibile configurare un server syslog esterno per la raccolta e l'analisi dei messaggi di registro di StorageGRID. ELK (Elasticsearch, Logstash, Kibana) è diventata una delle soluzioni di analisi dei log più diffuse. Guarda il "Analisi del log StorageGRID con video ELK" Per visualizzare una configurazione ELK di esempio e come può essere utilizzata per identificare e risolvere i problemi delle richieste S3 non riuscite. Questo articolo fornisce file di esempio di configurazione di Logstash, query Kibana, grafici e dashboard per fornire un rapido avvio per la gestione dei log e l'analisi di StorageGRID.

Requisiti

- StorageGRID 11.6.0.2 o superiore
- ELK (Elasticsearch, Logstash e Kibana) 7.1x o superiore installato e in funzione

File di esempio

- "Scarica il pacchetto di file di esempio Logstash 7.x." + **checksum md5** 148c23d0021d9a4bb4a6c0287464deab + **checksum sha256** f51ec9e2e3f842d5a7861566b167a561beb4373038b4e7bb3c8be3d522adf2d6
- "Scarica il pacchetto di file di esempio Logstash 8.x." + **checksum md5** e11bae3a662f87c310ef363d0fe06835 + **checksum sha256** 5c670755742cfdfd5aa723a596ba087e0153a65bcaef3934afdb682f61cd278d

Assunzione

I lettori conoscono la terminologia e le operazioni di StorageGRID ed ELK.

Istruzioni

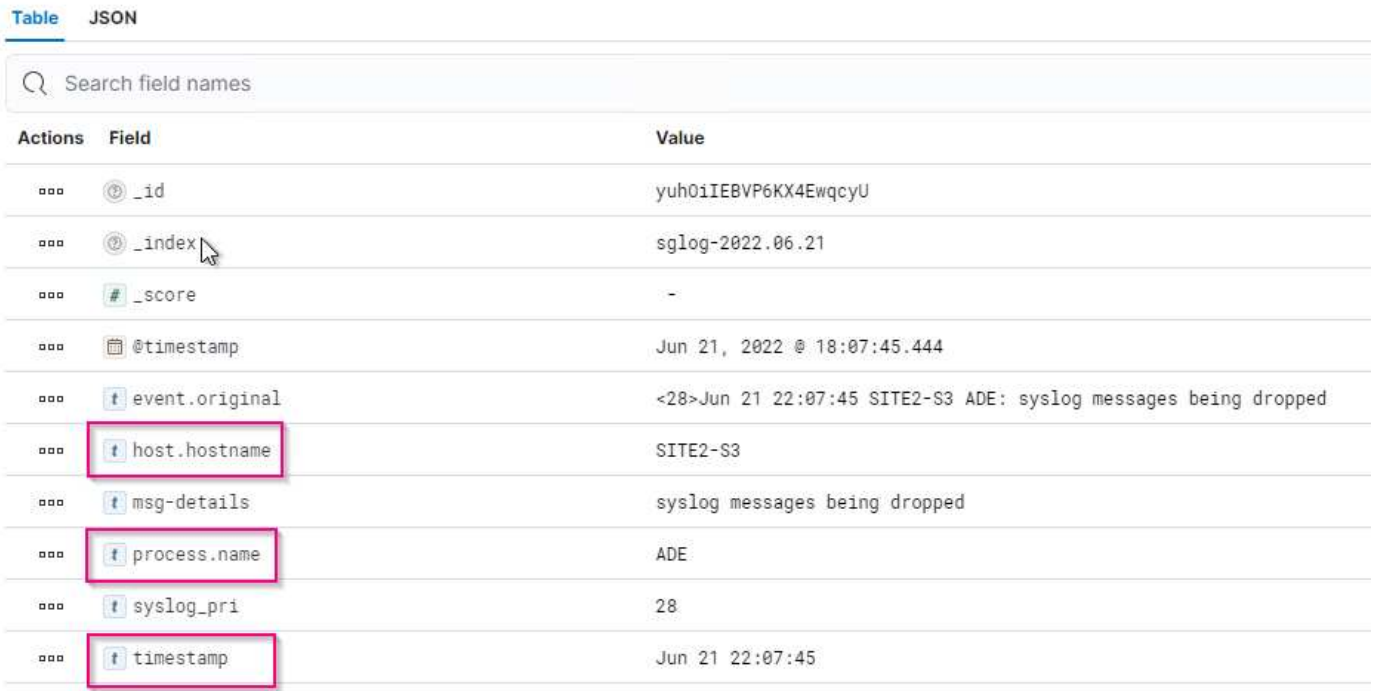
Due versioni di esempio sono fornite a causa delle differenze nei nomi definiti dai modelli grok. Ad esempio, il modello SYSLOGBASE grok nel file di configurazione di Logstash definisce i nomi dei campi in modo diverso a seconda della versione di Logstash installata.

```
match => {"message" => '<%{POSINT:syslog_pri}>%{SYSLOGBASE}
%{GREEDYDATA:msg-details}'}
```

Esempio di Logstash 7.17

Field	Value
t _id	7C1MaYEBRH8UbfKnIls8
t _index	sgrid2-2022.06.15
# _score	-
t _type	_doc
@timestamp	Jun 15, 2022 @ 17:36:46.038
t host	grid2-site2-s1
t logsource	SITE2-S1
t msg-details	Reloading syslog service
t pid	628
t program	update-sysl
t syslog_pri	37
t timestamp	Jun 15 21:36:46

Esempio di Logstash 8.23



Fasi

1. Decomprimere l'esempio fornito in base alla versione ELK installata. La cartella di esempio include due esempi di configurazione di Logstash: + **sglog-2-file.conf:** questo file di configurazione genera messaggi di log StorageGRID in un file su Logstash senza trasformazione dei dati. È possibile utilizzare questa opzione per confermare che Logstash riceve messaggi StorageGRID o per comprendere meglio i modelli di log di StorageGRID. + **sglog-2-es.conf:** questo file di configurazione trasforma i messaggi di log di StorageGRID utilizzando vari modelli e filtri. Include istruzioni drop di esempio, che consentono di eliminare i messaggi in base a modelli o filtri. L'output viene inviato a Elasticsearch per l'indicizzazione. + personalizzare il file di configurazione selezionato in base alle istruzioni contenute nel file.
2. Verificare il file di configurazione personalizzato:

```
/usr/share/logstash/bin/logstash --config.test_and_exit -f <config-file-path/file>
```

   Se l'ultima riga restituita è simile alla riga seguente, il file di configurazione non presenta errori di sintassi:

```
[LogStash::Runner] runner - Using config.test_and_exit mode. Config Validation Result: OK. Exiting Logstash
```

3. Copiare il file di configurazione personalizzato nella configurazione del server Logstash: /Etc/logstash/conf.d + se non si è abilitato config.reload.automatic in /etc/logstash/logstash.yml, riavviare il servizio Logstash. In caso contrario, attendere lo scadere dell'intervallo di ricarica della configurazione.

```
 grep reload /etc/logstash/logstash.yml
# Periodically check if the configuration has changed and reload the
pipeline
config.reload.automatic: true
config.reload.interval: 5s
```

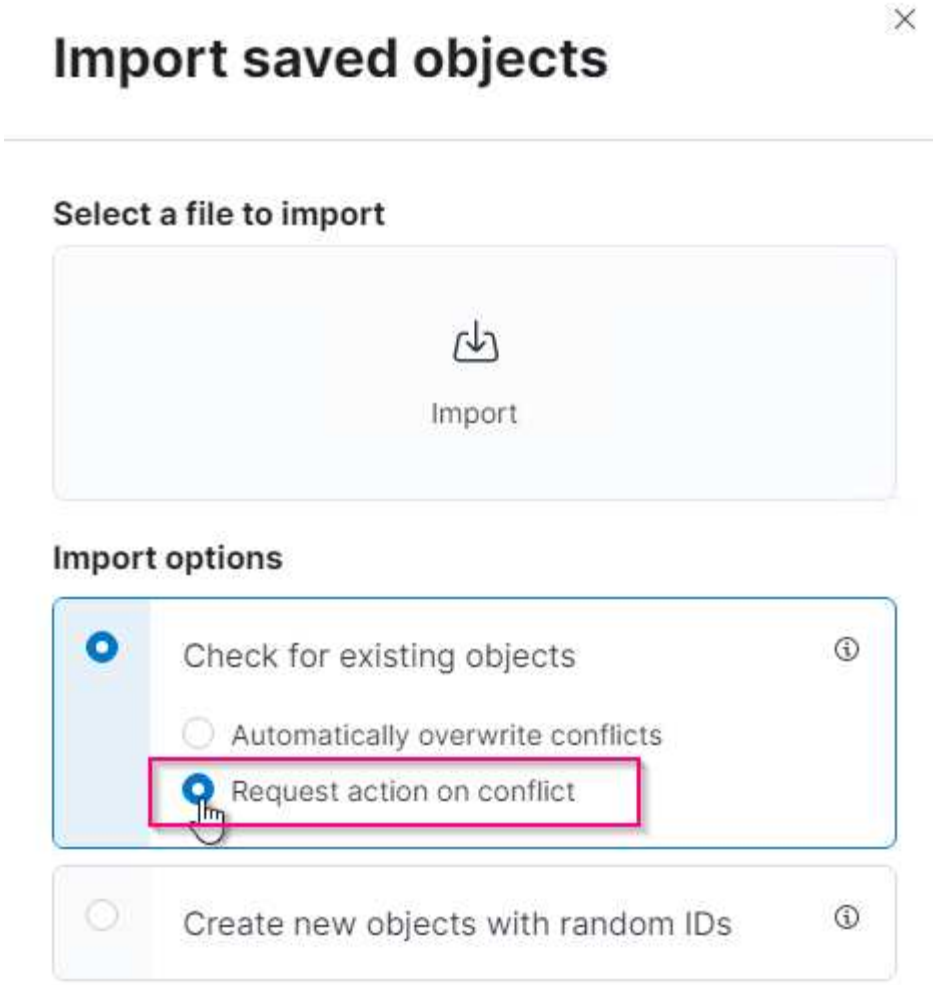
4. Controllare /var/log/logstash/logstash-plain.log e verificare che non ci siano errori durante l'avvio di Logstash con il nuovo file di configurazione.
5. Verificare che la porta TCP sia stata avviata e in attesa. + in questo esempio, viene utilizzata la porta TCP 5000.

```
netstat -ntpa | grep 5000
tcp6       0      0 :::5000                 :::*
LISTEN      25744/java
```

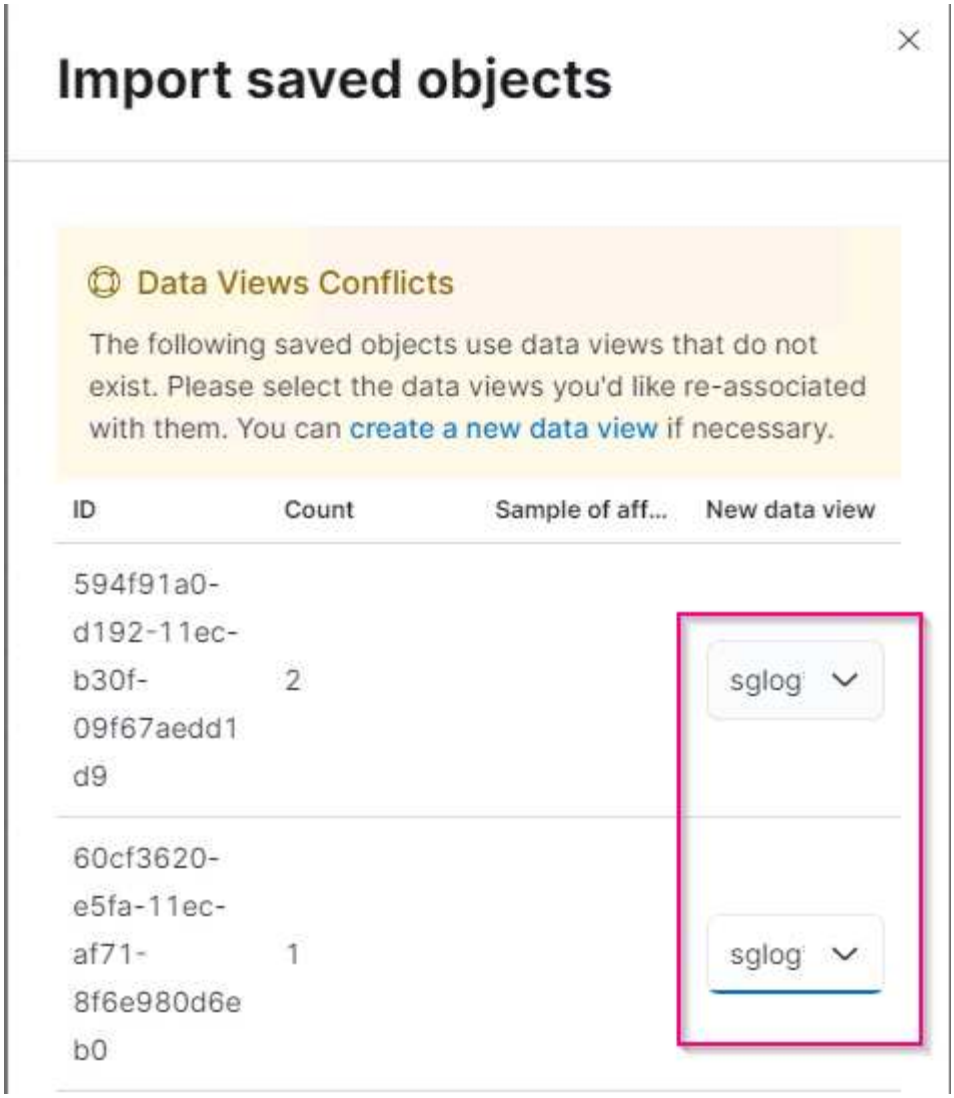
6. Dalla GUI di StorageGRID Manager, configurare il server syslog esterno per l'invio dei messaggi di log a Logstash. Fare riferimento a. "video dimostrativo" per ulteriori informazioni.
7. È necessario configurare o disattivare il firewall sul server Logstash per consentire la connessione dei nodi StorageGRID alla porta TCP definita.
8. Dalla GUI di Kibana, selezionare Management (Gestione) → Dev Tools (Strumenti di sviluppo). Nella pagina Console, eseguire questo comando GET per confermare la creazione di nuovi indici in Elasticsearch.

```
GET /_cat/indices/*?v=true&s=index
```

9. Dalla GUI di Kibana, creare un modello di indice (ELK 7.x) o una vista dati (ELK 8.x).
10. Dalla GUI di Kibana, inserire "oggetti memorizzati" nella casella di ricerca situata in alto al centro. + nella pagina Saved Objects (oggetti salvati), selezionare Import (Importa). In Opzioni di importazione, selezionare "Richiedi azione in caso di conflitto"



Importa elk <version>-query-chart-sample.ndjson. + quando viene richiesto di risolvere il conflitto, selezionare il modello di indice o la vista dati creata al punto 8.



Vengono importati i seguenti oggetti Kibana: + **Query** + * audit-msg-s3rq-orlm + * bycast log s3 messaggi correlati + * loglevel warning o superiore + * failed Security event + **Chart** + * s3 requests count based on bycast.log + * HTTP status code + * audit msg breakdown by type + * Average s3 Response Time + **Dashboard** + * S3 dashboard di richiesta utilizzando i grafici sopra riportati.

A questo punto, è possibile eseguire l'analisi del registro StorageGRID utilizzando Kibana.

Risorse aggiuntive

- "syslog101"
- "Cos'è lo stack ELK"
- "Elenco dei modelli di grok"
- "Guida per principianti a Logstash: Grok"
- "Una guida pratica a Logstash: Approfondimento di Syslog"
- "Guida di Kibana – Esplora il documento"
- "Riferimento ai messaggi del registro di controllo di StorageGRID"

Di Angela Cheng

Utilizza Prometheus e Grafana per estendere la conservazione delle metriche

Questo report tecnico fornisce istruzioni dettagliate per la configurazione di NetApp StorageGRID 11.6 con servizi esterni Prometheus e Grafana.

Introduzione

StorageGRID memorizza le metriche utilizzando Prometheus e fornisce visualizzazioni di queste metriche attraverso dashboard Grafana integrate. È possibile accedere in modo sicuro alle metriche Prometheus da StorageGRID configurando i certificati di accesso client e abilitando l'accesso prometheus per il client specificato. Oggi, la conservazione di questi dati metrici è limitata dalla capacità di storage del nodo di amministrazione. Per ottenere una durata maggiore e la possibilità di creare visualizzazioni personalizzate di queste metriche, implementeremo un nuovo server Prometheus e Grafana, configureremo il nostro nuovo server per scartare le metriche dall'istanza StorageGRID e costruiremo una dashboard con le metriche che sono importanti per noi. È possibile ottenere ulteriori informazioni sulle metriche Prometheus raccolte in "Documentazione StorageGRID".

Federare Prometheus

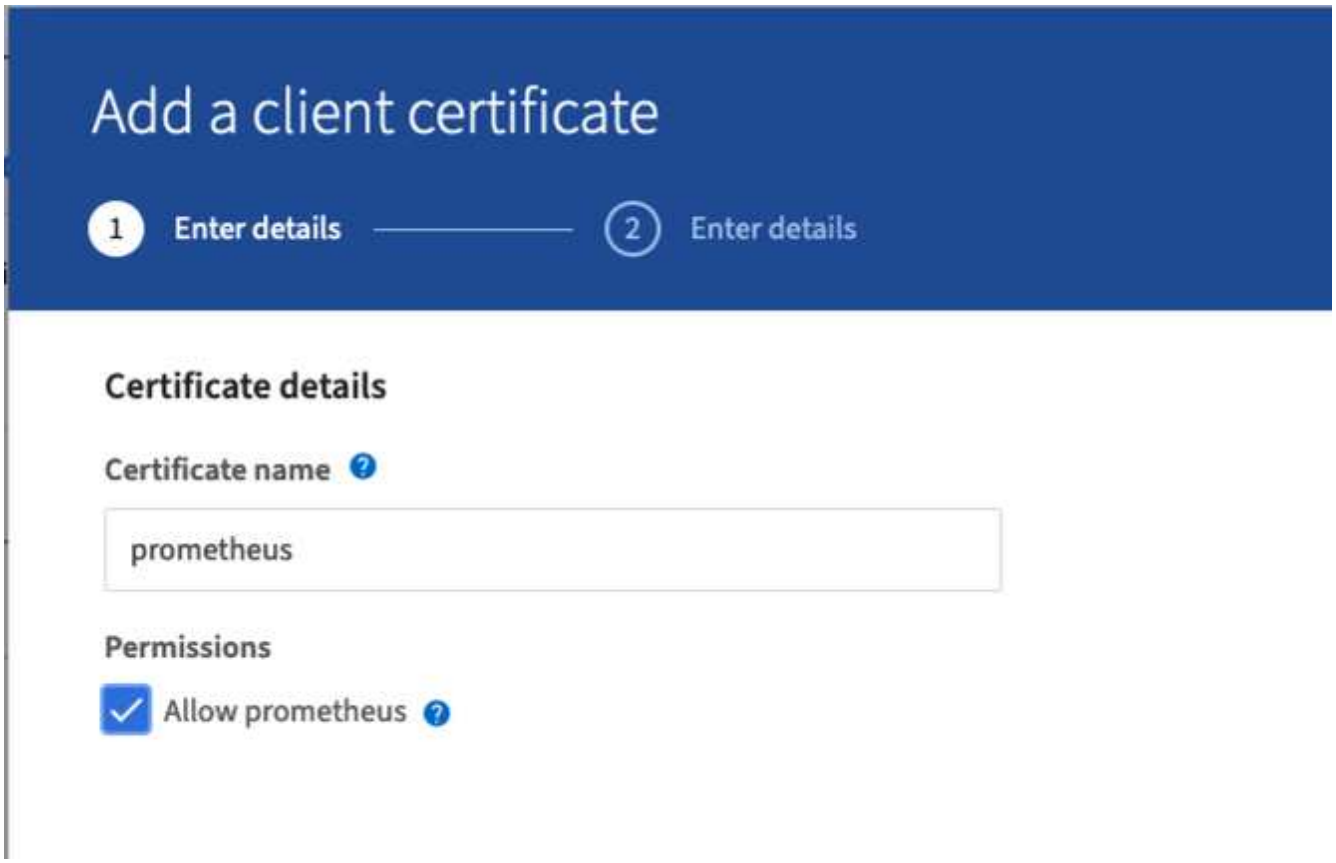
Dettagli del laboratorio

Ai fini di questo esempio, userò tutte le macchine virtuali per i nodi StorageGRID 11.6 e un server Debian 11. L'interfaccia di gestione di StorageGRID è configurata con un certificato CA pubblicamente attendibile. Questo esempio non riguarda l'installazione e la configurazione del sistema StorageGRID o dell'installazione di Debian linux. Puoi utilizzare qualsiasi versione di Linux supportata da Prometheus e Grafana. Prometheus e Grafana possono essere installati come container docker, build from source o binari pre-compilati. In questo esempio installerò entrambi i binari Prometheus e Grafana direttamente sullo stesso server Debian. Scaricare e seguire le istruzioni di installazione di base da https://prometheus.io e. https://grafana.com/grafana/ rispettivamente.

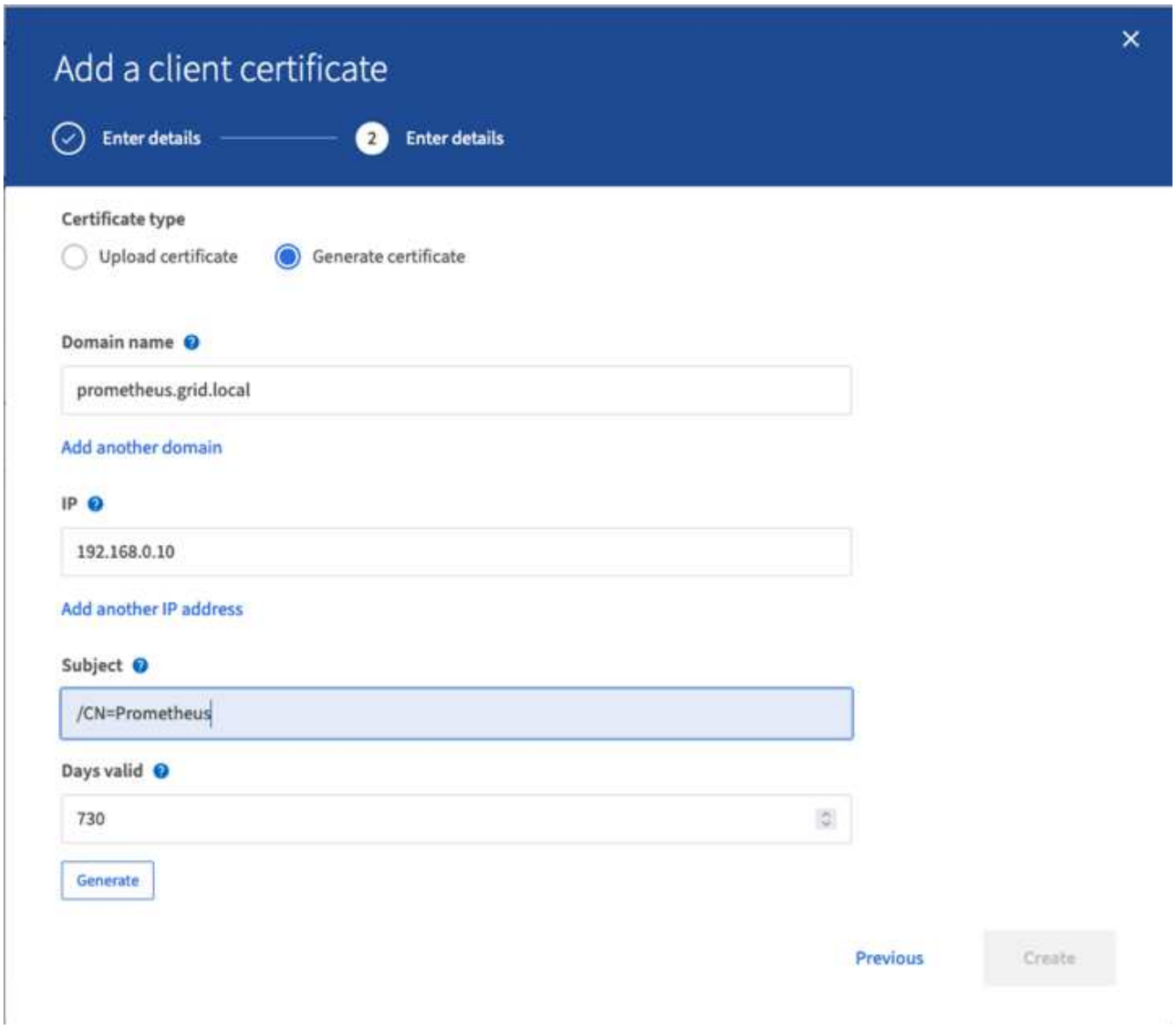
Configurare StorageGRID per l'accesso al client Prometheus

Per ottenere l'accesso alle metriche StorageGRID Stored prometheus, è necessario generare o caricare un certificato client con chiave privata e abilitare l'autorizzazione per il client. L'interfaccia di gestione StorageGRID deve disporre di un certificato SSL. Il certificato deve essere attendibile dal server prometheus da una CA attendibile o manualmente se autofirmato. Per ulteriori informazioni, visitare il "Documentazione StorageGRID".

1. Nell'interfaccia di gestione di StorageGRID, selezionare "CONFIGURATION" (CONFIGURAZIONE) in basso a sinistra e nella seconda colonna sotto "Security" (sicurezza) fare clic su Certificates (certificati).
2. Nella pagina certificati, selezionare la scheda "Client" e fare clic sul pulsante "Aggiungi".
3. Specificare un nome per il client a cui verrà concesso l'accesso e utilizzare questo certificato. Fare clic sulla casella sotto "permessi", davanti a "Consenti Prometheus" e fare clic sul pulsante continua.

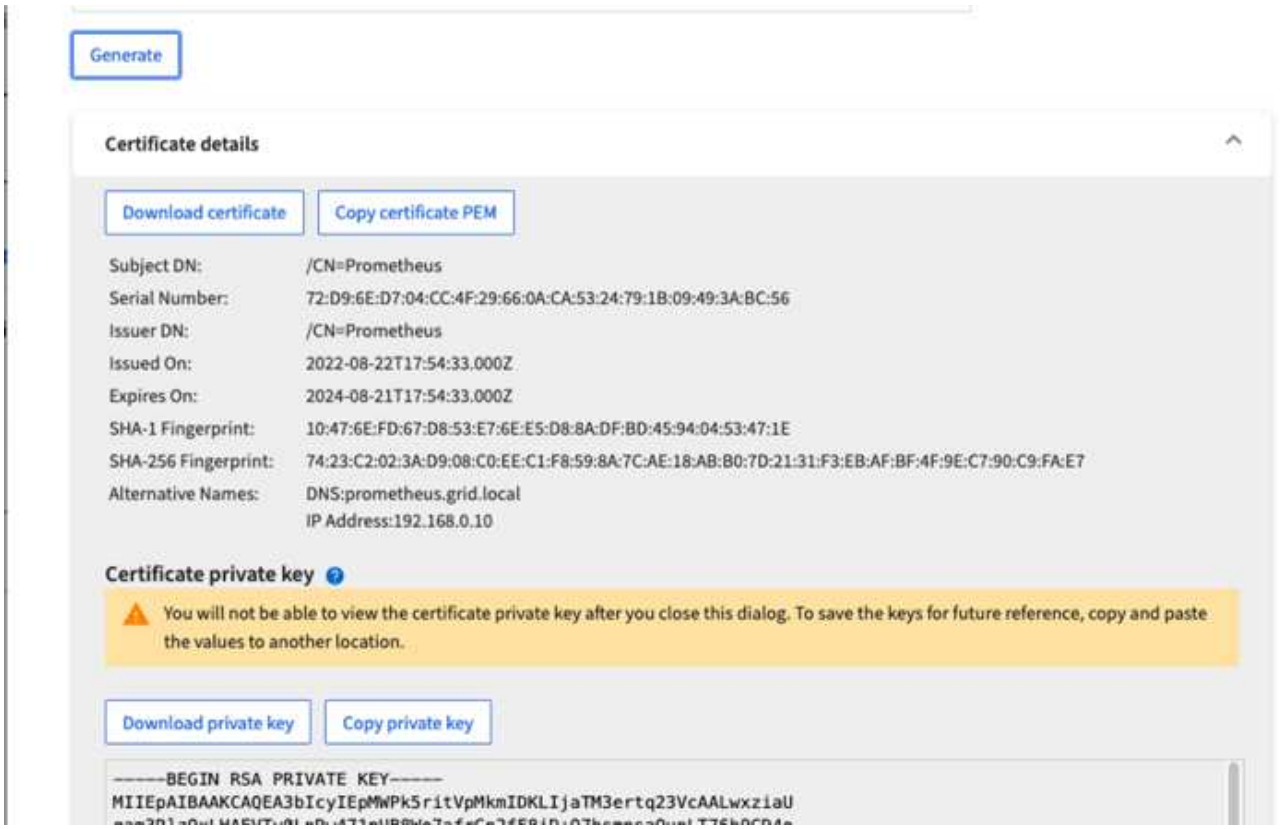


4. Se si dispone di un certificato firmato dalla CA, è possibile selezionare il pulsante di opzione "carica certificato", ma in questo caso StorageGRID genererà il certificato client selezionando il pulsante di opzione "genera certificato". Vengono visualizzati i campi obbligatori da compilare. Inserire l'FQDN per il server client, l'IP del server, l'oggetto e i giorni validi. Quindi fare clic sul pulsante "generate" (genera).



> Be mindful of the certificate days valid entry as you will need to renew this certificate in both StorageGRID and the Prometheus server before it expires to maintain uninterrupted collection.

1. Scaricare il file pem del certificato e il file pem della chiave privata.



This is the only time you can download the private key, so make sure you do not skip this step.

Preparare il server Linux per l'installazione di Prometheus

Prima di installare Prometheus, desidero preparare il mio ambiente con un utente Prometheus, la struttura di directory e configurare la capacità per la posizione di storage delle metriche.

1. Creare l'utente Prometheus.

```
sudo useradd -M -r -s /bin/false Prometheus
```

2. Creare le directory per Prometheus, certificato client e dati di metriche.

```
sudo mkdir /etc/Prometheus /etc/Prometheus/cert /var/lib/Prometheus
```

3. Ho formattato il disco che sto usando per la conservazione delle metriche con un filesystem ext4.

```
mkfs -t ext4 /dev/sdb
```

4. Ho quindi montato il file system nella directory Prometheus metrics.

```
sudo mount -t auto /dev/sdb /var/lib/prometheus/
```

5. Ottenere l'uuid del disco utilizzato per i dati delle metriche.

```
sudo ls -al /dev/disk/by-uuid/
   lrwxrwxrwx 1 root root   9 Aug 18 17:02 9af2c5a3-bfc2-4ec1-85d9-
ebab850bb4a1 -> ../../sdb
```

6. Aggiungere una voce in /etc/fstab/ rendere il mount persistente durante i riavvii usando l'uuid di /dev/sdb.

```
/etc/fstab
UUID=9af2c5a3-bfc2-4ec1-85d9-ebab850bb4a1 /var/lib/prometheus   ext4
defaults    0   0
```

Installare e configurare Prometheus

Ora che il server è pronto, posso iniziare l'installazione di Prometheus e configurare il servizio.

1. Estrarre il pacchetto di installazione di Prometheus

```
tar xzf prometheus-2.38.0.linux-amd64.tar.gz
```

2. Copiare i file binari in /usr/local/bin e modificare la proprietà dell'utente prometheus creato in precedenza

```
sudo cp prometheus-2.38.0.linux-amd64/{prometheus,promtool}
/usr/local/bin
sudo chown prometheus:prometheus /usr/local/bin/{prometheus,promtool}
```

3. Copiare le console e le librerie in /etc/prometheus

```
sudo cp -r prometheus-2.38.0.linux-amd64/{consoles,console_libraries}
/etc/prometheus/
```

4. Copiare i file PEM del certificato client e della chiave privata scaricati in precedenza da StorageGRID in /etc/prometheus/certs
5. Creare il file yaml di configurazione prometheus

```
sudo nano /etc/prometheus/prometheus.yml
```

6. Inserire la seguente configurazione. Il nome del lavoro può essere qualsiasi cosa si desideri. Modificare "-

targets: [""] in FQDN del nodo admin e, se i nomi dei file dei certificati e delle chiavi private sono modificati, aggiornare la sezione tls_config in modo che corrisponda. quindi salvare il file. Se l'interfaccia di gestione della griglia utilizza un certificato autofirmato, scaricare il certificato e posizionarlo con il certificato client con un nome univoco, quindi nella sezione tls_config aggiungere ca_file: /Etc/prometheus/cert/UIcert.pem

a. In questo esempio, vengono raccolte tutte le metriche che iniziano con alertmanager, cassandra, Node e StorageGRID. Per ulteriori informazioni sulle metriche Prometheus, consultare la "Documentazione StorageGRID".

```
# my global config
global:
  scrape_interval: 60s # Set the scrape interval to every 15 seconds.
Default is every 1 minute.

scrape_configs:
  - job_name: 'StorageGRID'
    honor_labels: true
    scheme: https
    metrics_path: /federate
    scrape_interval: 60s
    scrape_timeout: 30s
    tls_config:
      cert_file: /etc/prometheus/cert/certificate.pem
      key_file: /etc/prometheus/cert/private_key.pem
    params:
      match[]:
        -
'{__name__=~"alertmanager_.*|cassandra_.*|node_.*|storagegrid_.*"}'
    static_configs:
    - targets: ['sgdemo-rtp.netapp.com:9091']
```

Se l'interfaccia di gestione della griglia utilizza un certificato autofirmato, scaricare il certificato e posizionarlo con il certificato client con un nome univoco. Nella sezione tls_config aggiungere il certificato sopra le righe del certificato client e della chiave privata

```
        ca_file: /etc/prometheus/cert/UIcert.pem
```

1. Modificare la proprietà di tutti i file e le directory in /etc/prometheus e /var/lib/prometheus nell'utente prometheus

```
sudo chown -R prometheus:prometheus /etc/prometheus/
sudo chown -R prometheus:prometheus /var/lib/prometheus/
```

2. Creare un file di servizio prometheus in /etc/systemd/system

```
sudo nano /etc/systemd/system/prometheus.service
```

3. Inserire le seguenti righe, annotare il n.--storage.tsdb.retention.time=1y n. che imposta la conservazione dei dati metrici su 1 anno. In alternativa, è possibile utilizzare n.--storage.tsdb.retention.size=n. 300GiB per basare la conservazione sui limiti di storage. Questa è l'unica posizione in cui impostare la conservazione delle metriche.

```
[Unit]
Description=Prometheus Time Series Collection and Processing Server
Wants=network-online.target
After=network-online.target

[Service]
User=prometheus
Group=prometheus
Type=simple
ExecStart=/usr/local/bin/prometheus \
        --config.file /etc/prometheus/prometheus.yml \
        --storage.tsdb.path /var/lib/prometheus/ \
        --storage.tsdb.retention.time=1y \
        --web.console.templates=/etc/prometheus/consoles \
        --web.console.libraries=/etc/prometheus/console_libraries

[Install]
WantedBy=multi-user.target
```

4. Ricaricare il servizio systemd per registrare il nuovo servizio prometheus. quindi avviare e attivare il servizio prometheus.

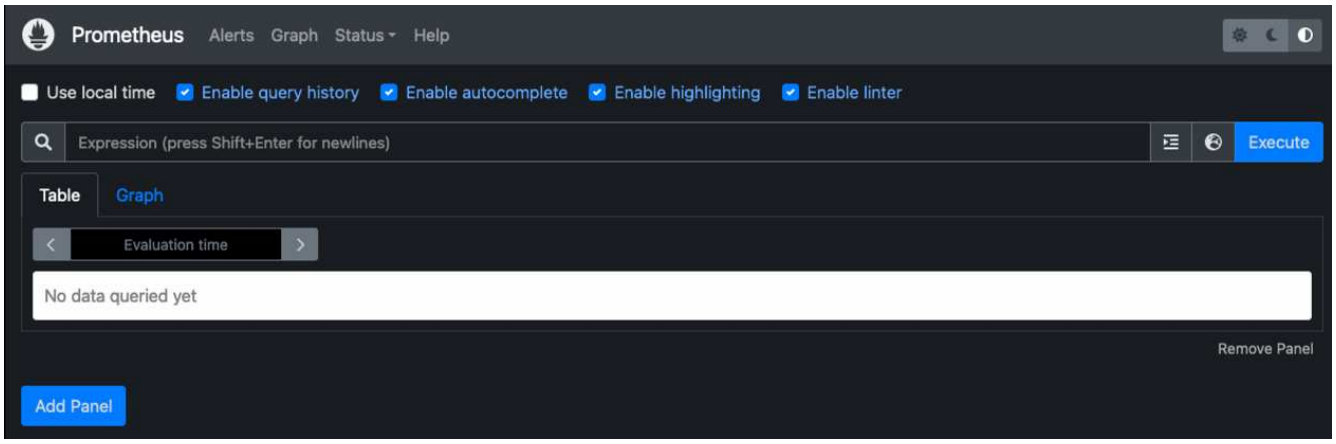
```
sudo systemctl daemon-reload
sudo systemctl start prometheus
sudo systemctl enable prometheus
```

5. Verificare che il servizio sia in funzione correttamente

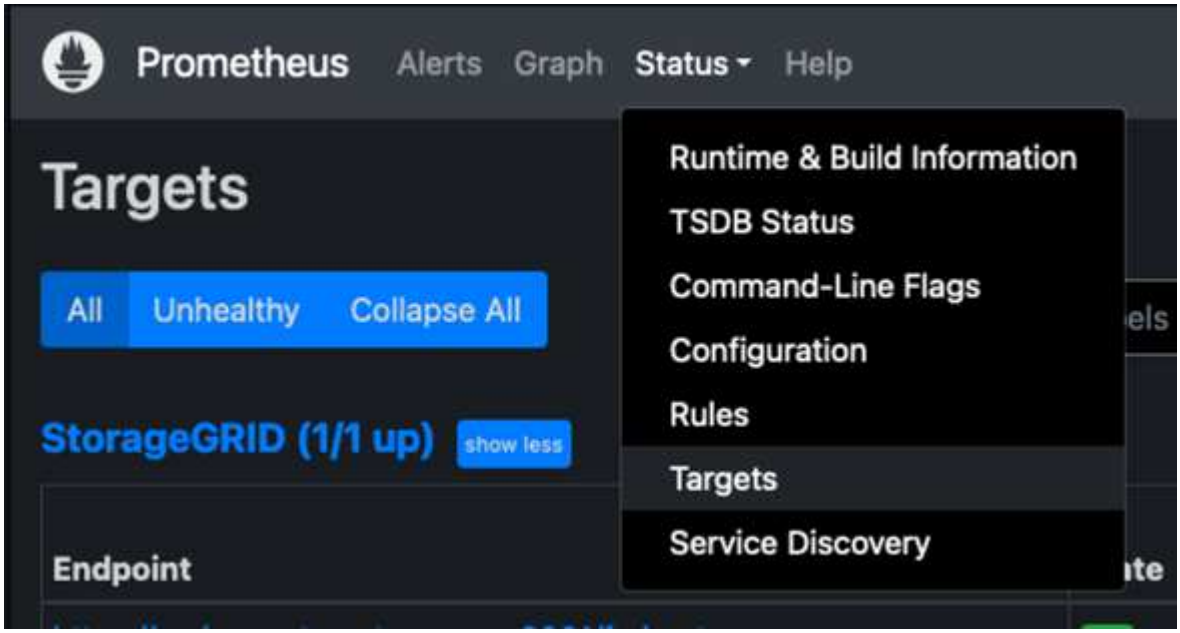
```
sudo systemctl status prometheus
```

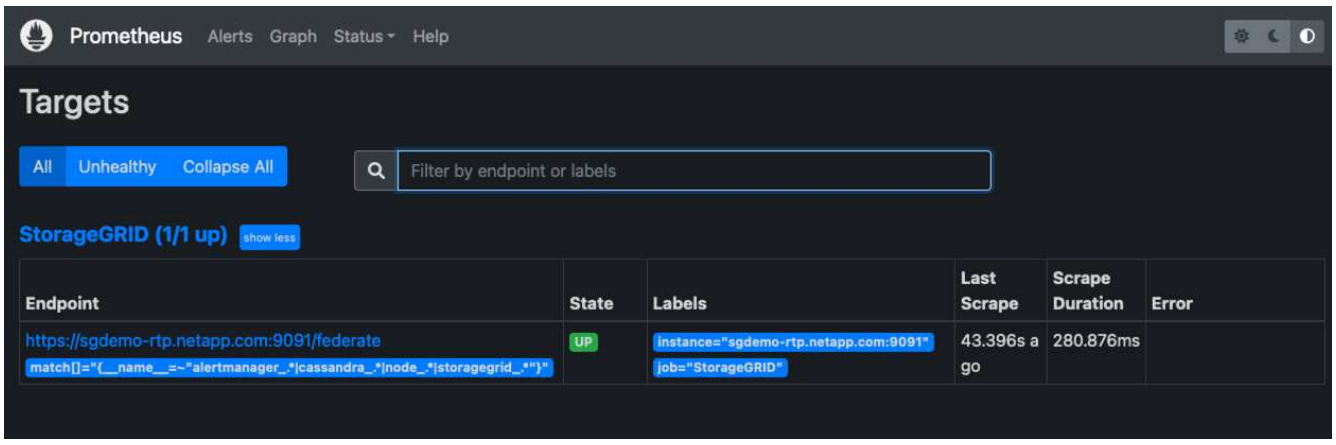
```
● prometheus.service - Prometheus Time Series Collection and Processing
Server
     Loaded: loaded (/etc/systemd/system/prometheus.service; enabled;
vendor preset: enabled)
     Active: active (running) since Mon 2022-08-22 15:14:24 EDT; 2s ago
   Main PID: 6498 (prometheus)
      Tasks: 13 (limit: 28818)
     Memory: 107.7M
        CPU: 1.143s
     CGroup: /system.slice/prometheus.service
             └─6498 /usr/local/bin/prometheus --config.file
/etc/prometheus/prometheus.yml --storage.tsdb.path /var/lib/prometheus/
--web.console.templates=/etc/prometheus/consoles --web.con>

Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.510Z caller=head.go:544 level=info component=tsdb
msg="Replaying WAL, this may take a while"
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.816Z caller=head.go:615 level=info component=tsdb msg="WAL
segment loaded" segment=0 maxSegment=1
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.816Z caller=head.go:615 level=info component=tsdb msg="WAL
segment loaded" segment=1 maxSegment=1
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.816Z caller=head.go:621 level=info component=tsdb msg="WAL
replay completed" checkpoint_replay_duration=55.57µs wal_rep>
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.831Z caller=main.go:997 level=info fs_type=EXT4_SUPER_MAGIC
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.831Z caller=main.go:1000 level=info msg="TSDB started"
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.831Z caller=main.go:1181 level=info msg="Loading
configuration file" filename=/etc/prometheus/prometheus.yml
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.832Z caller=main.go:1218 level=info msg="Completed loading
of configuration file" filename=/etc/prometheus/prometheus.y>
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.832Z caller=main.go:961 level=info msg="Server is ready to
receive web requests."
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.832Z caller=manager.go:941 level=info component="rule
manager" msg="Starting rule manager..."
```

6. A questo punto, dovresti essere in grado di accedere all'interfaccia utente del tuo server prometheus http://Prometheus-server:9090 E consultare l'interfaccia utente

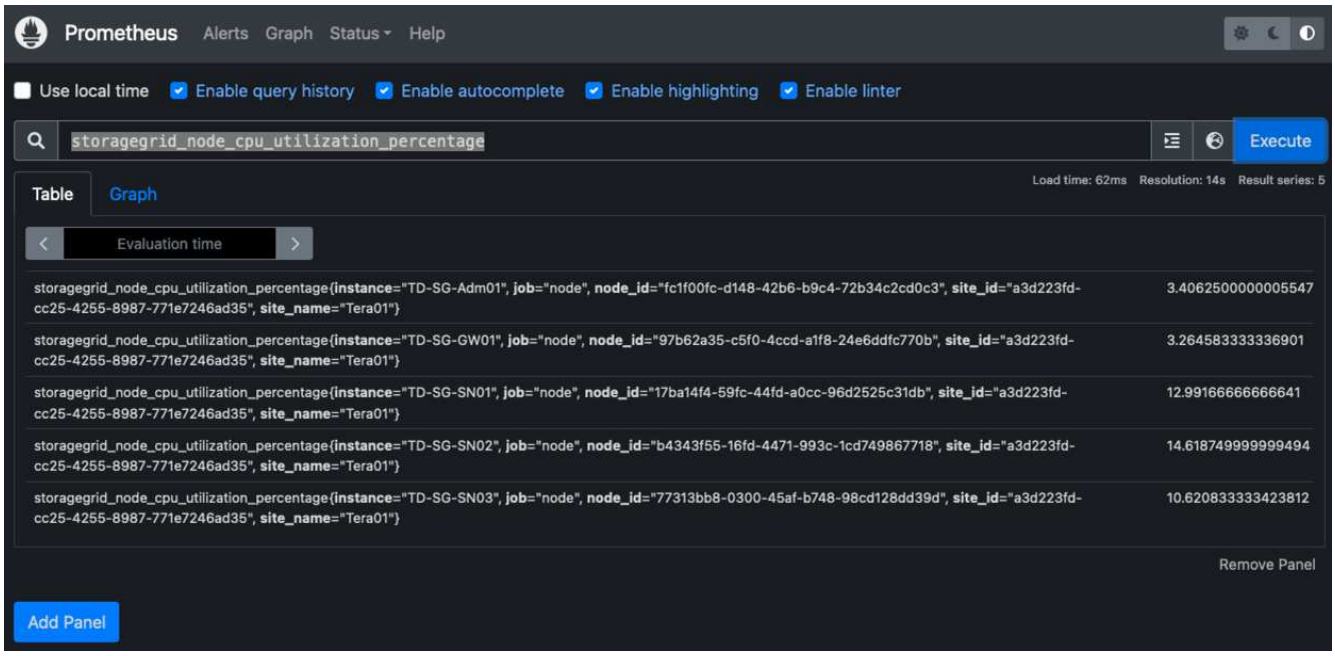


7. Sotto "Stato", è possibile visualizzare lo stato dell'endpoint StorageGRID configurato in prometheus.yml





8. Nella pagina Graph (grafico), è possibile eseguire una query di test e verificare che i dati siano stati scartati correttamente. Ad esempio, immettere "storagegrid_node_cpu_Utilization_percent" nella barra delle query e fare clic sul pulsante Execute.



Installare e configurare Grafana

Ora che prometheus è installato e funzionante, possiamo passare all'installazione di Grafana e alla configurazione di una dashboard

Installazione di Grafana

1. Installare l'ultima edizione Enterprise di Grafana

```
sudo apt-get install -y apt-transport-https
sudo apt-get install -y software-properties-common wget
sudo wget -q -O /usr/share/keyrings/grafana.key
https://packages.grafana.com/gpg.key
```

2. Aggiungi questo repository per le release stabili:

```
echo "deb [signed-by=/usr/share/keyrings/grafana.key]
https://packages.grafana.com/enterprise/deb stable main" | sudo tee -a
/etc/apt/sources.list.d/grafana.list
```

3. Dopo aver aggiunto il repository.

```
sudo apt-get update
sudo apt-get install grafana-enterprise
```

4. Ricaricare il servizio systemd per registrare il nuovo servizio Grafana. Quindi avviare e attivare il servizio Grafana.

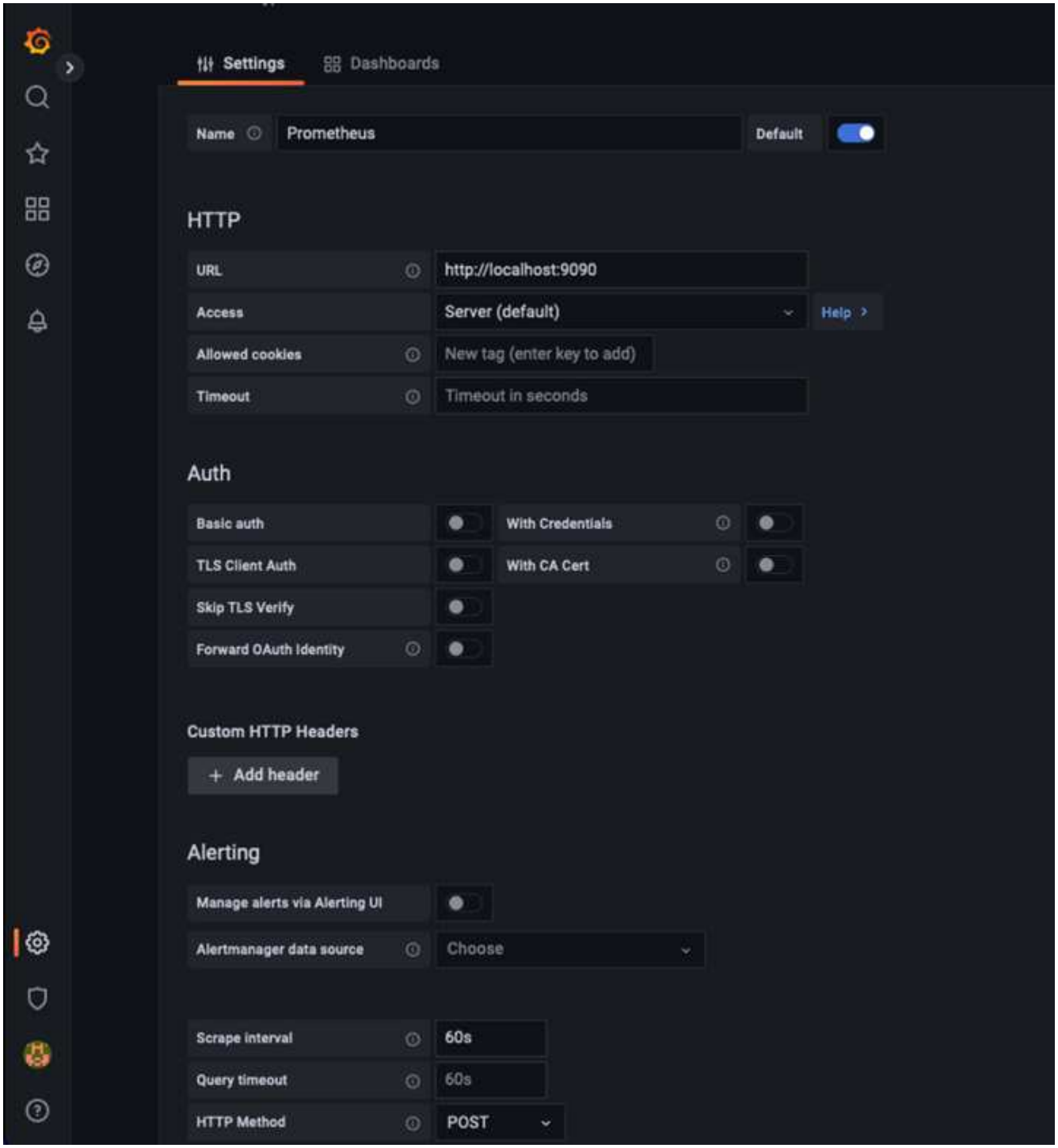
```
sudo systemctl daemon-reload
sudo systemctl start grafana-server
sudo systemctl enable grafana-server.service
```

5. Grafana è ora installato e in esecuzione. Quando si apre un browser per HTTP://Prometheus-server:3000 viene visualizzata la pagina di accesso Grafana.
6. Le credenziali di accesso predefinite sono admin/admin ed è necessario impostare una nuova password come richiesto.

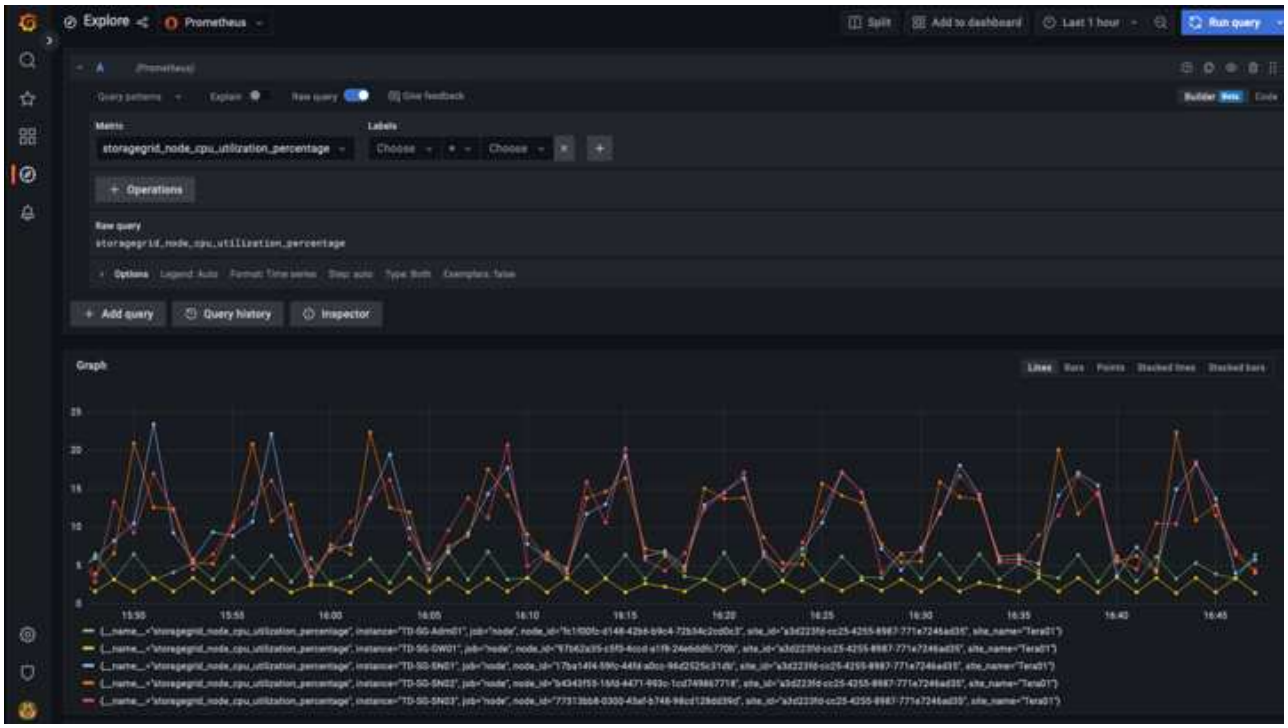
Creare una dashboard Grafana per StorageGRID

Con Grafana e Prometheus installati e in esecuzione, ora è il momento di collegare i due elementi creando un'origine dati e creando una dashboard

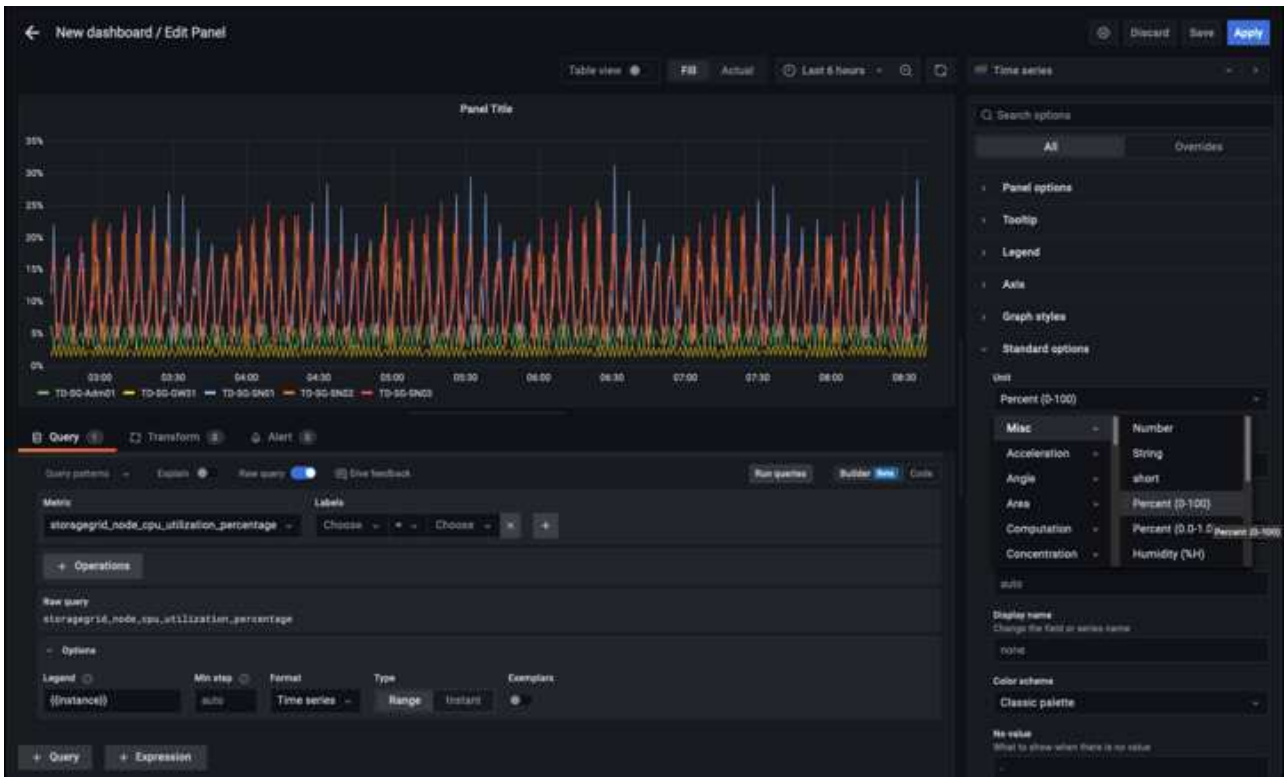
1. Nel riquadro di sinistra, espandere "Configuration" (Configurazione) e selezionare "Data Sources" (origini dati), quindi fare clic sul pulsante "Add Data Source" (Aggiungi origine dati)
2. Prometheus sarà una delle principali fonti di dati tra cui scegliere. In caso contrario, utilizzare la barra di ricerca per individuare "Prometheus"
3. Configurare l'origine Prometheus immettendo l'URL dell'istanza prometheus e l'intervallo di scrape in modo che corrisponda all'intervallo Prometheus. Ho anche disattivato la sezione degli avvisi perché non ho configurato il gestore degli avvisi su prometheus.



4. Una volta inserite le impostazioni desiderate, scorrere verso il basso e fare clic su "Save & test" (Salva e verifica).
5. Una volta completato il test di configurazione, fare clic sul pulsante Esplora.
    a. Nella finestra Esplora puoi utilizzare la stessa metrica che abbiamo testato Prometheus con "storagegrid_node_cpu_Utilization_percent" e fare clic sul pulsante "Esegui query"



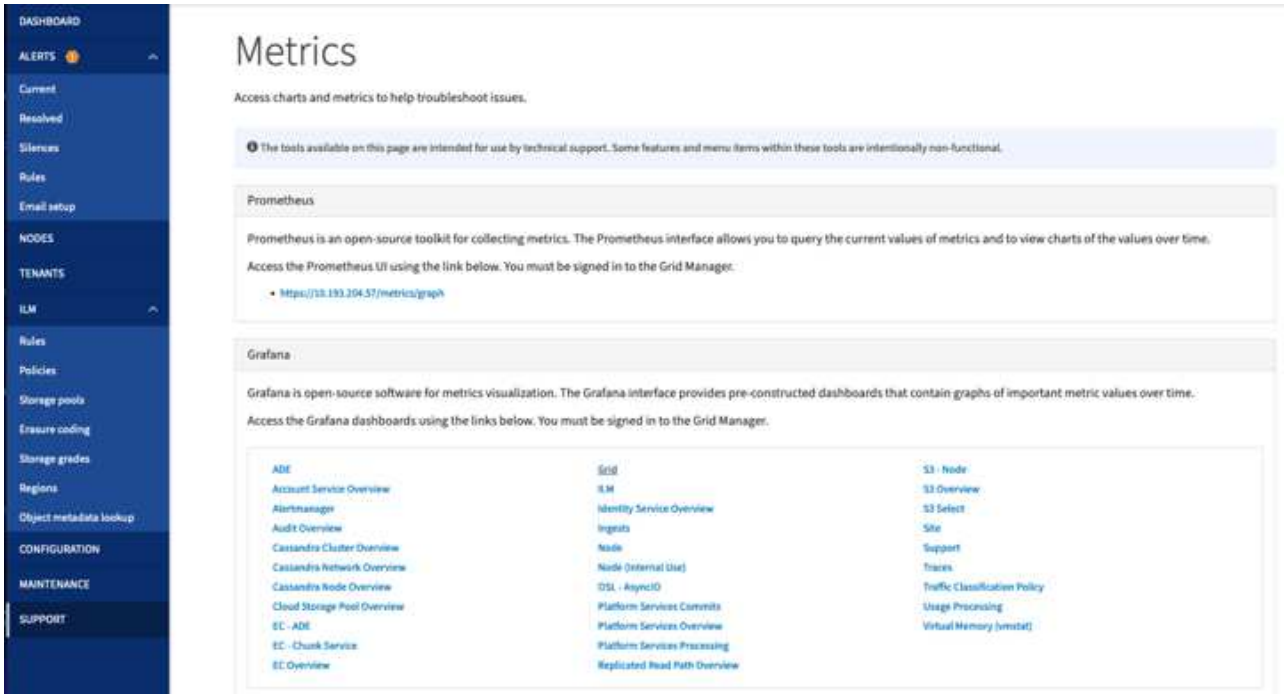
6. Ora che abbiamo configurato l'origine dati, possiamo creare una dashboard.
   a. Nel riquadro di sinistra, espandere "Dashboard" e selezionare "+ new Dashboard"
   b. Seleziona "Aggiungi un nuovo pannello"
   c. Configurare il nuovo pannello selezionando una metrica, di nuovo userò "storagegrid_node_cpu_Utilization_Percent", inserire un titolo per il pannello, espandere "Opzioni" in basso e per la modifica della legenda su custom e inserire "{{instance}}" per definire i nomi dei nodi", e nel pannello di destra in "Opzioni standard" impostare "unità" su "varie/percentuali(0-100)". Quindi fare clic su "Apply" (Applica) per salvare il pannello nella dashboard.



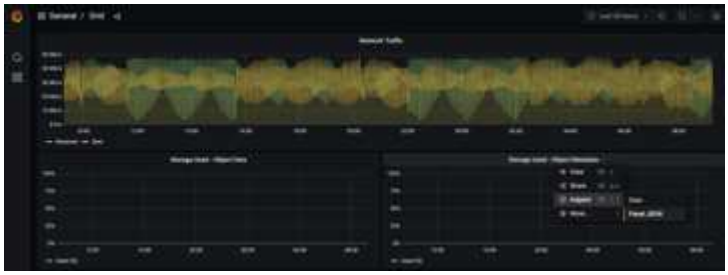
7. Potremmo continuare a costruire la nostra dashboard in questo modo per ogni metrica che vogliamo, ma fortunatamente StorageGRID dispone già di dashboard con pannelli che possiamo copiare nelle nostre dashboard personalizzate.

   a. Dal riquadro sinistro dell'interfaccia di gestione StorageGRID, selezionare "supporto", quindi fare clic su "metriche" nella parte inferiore della colonna "Strumenti".

   b. All'interno delle metriche, selezionerò il link "Grid" nella parte superiore della colonna centrale.

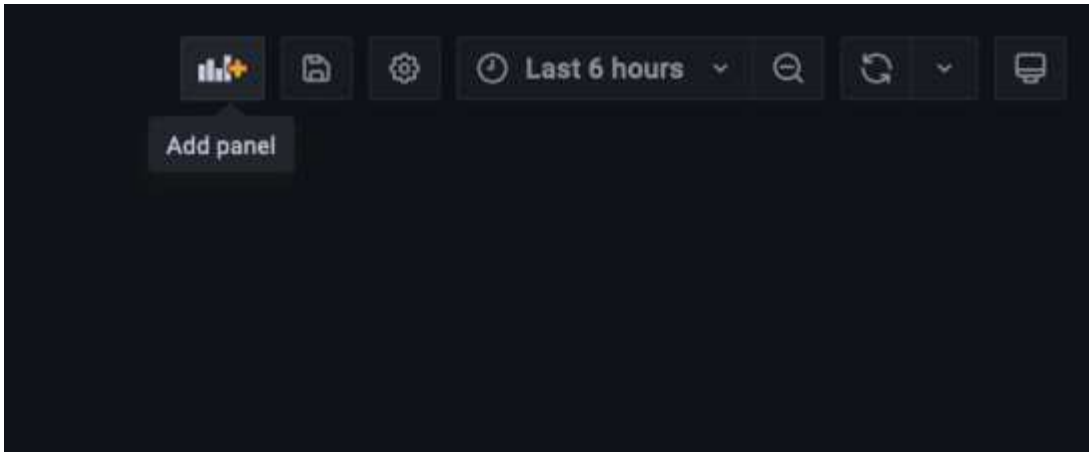


   c. Dalla dashboard della griglia, selezionare il pannello "Storage used - Object Metadata" (Storage utilizzato - metadati oggetto). Fare clic sulla piccola freccia verso il basso e sulla fine del titolo del pannello per visualizzare un menu a discesa. Da questo menu selezionare "Inspect" (ispezione) e "Panel JSON" (pannello JSON).



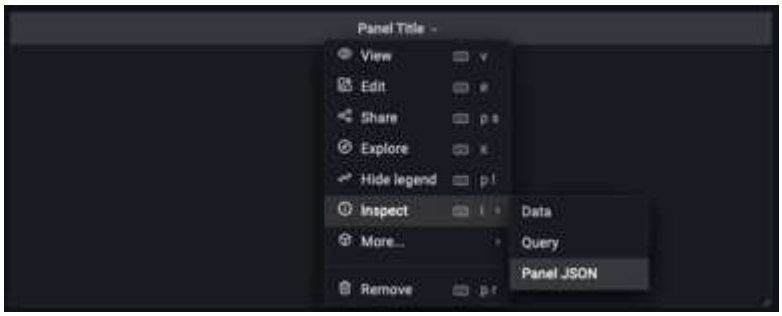
   d. Copiare il codice JSON e chiudere la finestra.

e. Nella nuova dashboard, fare clic sull'icona per aggiungere un nuovo pannello.

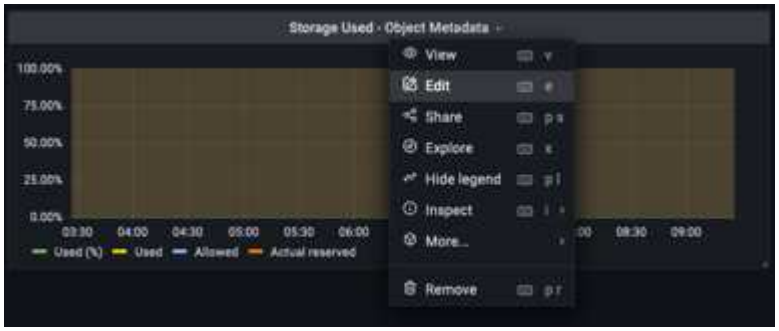


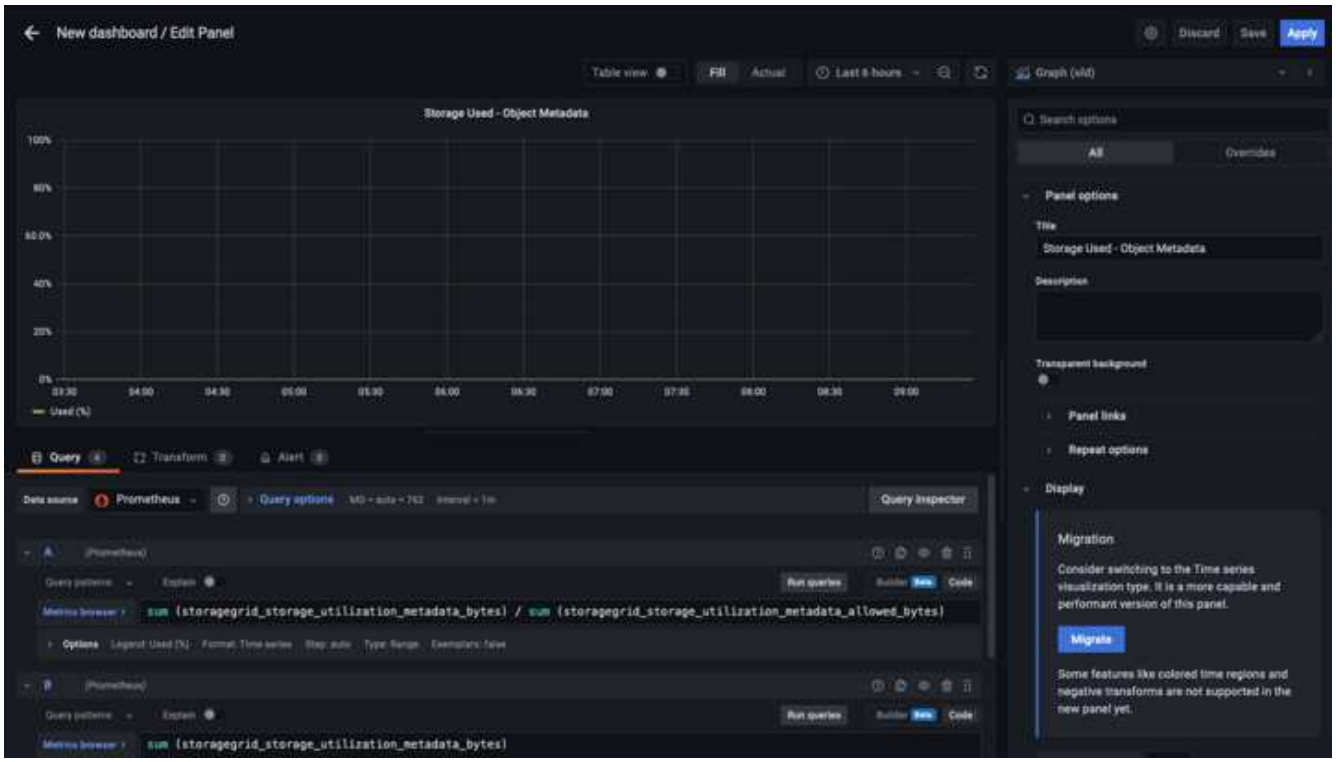
f. Applicare il nuovo pannello senza apportare modifiche

g. Proprio come per il pannello StorageGRID, controllare il JSON. Rimuovere tutto il codice JSON e sostituirlo con il codice copiato dal pannello StorageGRID.



h. Modificare il nuovo pannello e sul lato destro viene visualizzato un messaggio di migrazione con il pulsante "Migrate" (migrazione). Fare clic sul pulsante, quindi sul pulsante "Apply" (Applica).





8. Una volta che tutti i pannelli sono in posizione e configurati come si desidera. Salvare la dashboard facendo clic sull'icona del disco in alto a destra e assegnando un nome alla dashboard.

Conclusione

Ora disponiamo di un server Prometheus con capacità di storage e conservazione dei dati personalizzabili. Con questo possiamo continuare a costruire le nostre dashboard con le metriche più rilevanti per le nostre operazioni. È possibile ottenere ulteriori informazioni sulle metriche Prometheus raccolte in "Documentazione StorageGRID".

Di Aron Klein

Configurazione SNMP Datadog

Configurare Datadog per raccogliere le metriche e i trap snmp di StorageGRID.

Configurare Datadog

Datadog è una soluzione di monitoraggio che fornisce metriche, visualizzazioni e avvisi. La seguente configurazione è stata implementata con l'agente linux versione 7.43.1 su un host Ubuntu 22.04.1 distribuito localmente nel sistema StorageGRID.

Profilo Datadog e file trap generati dal file MIB StorageGRID

Datadog fornisce un metodo per convertire i file MIB del prodotto in file di riferimento datadog necessari per mappare i messaggi SNMP.

Questo file yaml di StorageGRID per la mappatura della risoluzione del trap Datadog generato in base alle istruzioni trovate "qui". + inserire questo file in /etc/datadog-Agent/conf.d/snmp.d/trap_db/ +

- "Scaricare il file yaml trap" +
  - **checksum md5** 42e27e4210719945a46172b98c379517 +
  - **sha256 checksum** d0fe5c8e6ca3c902d054f854b70a85f928cba8b7c76391d356f05d2cf73b6887 +

Questo file yaml del profilo StorageGRID per la mappatura delle metriche Datadog generato in base alle istruzioni trovate "qui". + inserire questo file in /etc/datadog-Agent/conf.d/snmp.d/profiles/ +

- "Scarica il file yaml del profilo" +
  - **checksum md5** 72b7784f4801adda4e0c3ea77df19aa +
  - **sha256 checksum** b6b7fadd33063422a8bb8e39b3ead8ab38349ee02229926eadc8585f0087b8cee +

Configurazione Datadog SNMP per metriche

La configurazione di SNMP per le metriche può essere gestita in due modi. È possibile configurare il rilevamento automatico fornendo un intervallo di indirizzi di rete contenente i sistemi StorageGRID o definendo gli IP dei singoli dispositivi. La posizione della configurazione è diversa in base alla decisione presa. Il rilevamento automatico viene definito nel file yaml dell'agente datadog. Le definizioni esplicite dei dispositivi vengono configurate nel file yaml di configurazione snmp. Di seguito sono riportati alcuni esempi di ciascuno per lo stesso sistema StorageGRID.

Rilevamento automatico

la configurazione si trova in /etc/datadog-agent/datadog.yaml

```
listeners:
  - name: snmp
snmp_listener:
  workers: 100  # number of workers used to discover devices concurrently
  discovery_interval: 3600  # interval between each autodiscovery in
seconds
  loader: core  # use core check implementation of SNMP integration.
recommended
  use_device_id_as_hostname: true  # recommended
  configs:
    - network_address: 10.0.0.0/24  # CIDR subnet
      snmp_version: 2
      port: 161
      community_string: 'st0r@gegrid'  # enclose with single quote
      profile: netapp-storagegrid
```

Singoli dispositivi

/etc/datadog-agent/conf.d/snmp.d/conf.yaml

```
init_config:
  loader: core  # use core check implementation of SNMP integration.
recommended
  use_device_id_as_hostname: true  # recommended
instances:
- ip_address: '10.0.0.1'
  profile: netapp-storagegrid
  community_string: 'st0r@gegrid'  # enclose with single quote
- ip_address: '10.0.0.2'
  profile: netapp-storagegrid
  community_string: 'st0r@gegrid'
- ip_address: '10.0.0.3'
  profile: netapp-storagegrid
 community_string: 'st0r@gegrid'
- ip_address: '10.0.0.4'
  profile: netapp-storagegrid
  community_string: 'st0r@gegrid'
```

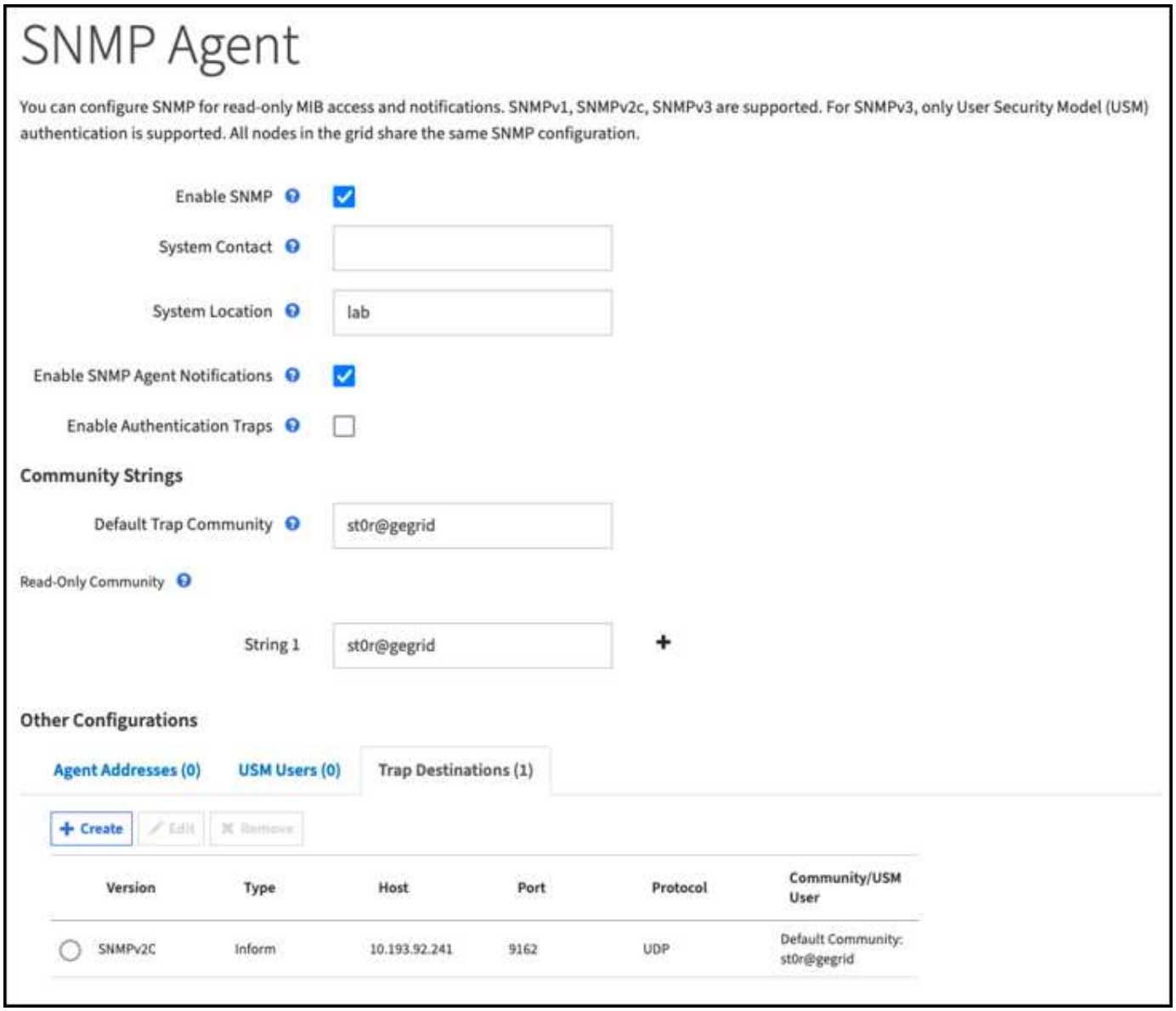
Configurazione SNMP per i trap

La configurazione per i trap SNMP è definita nel file yaml di configurazione del datadog /etc/datadog-Agent/datadog.yaml

```
network_devices:
  namespace:  # optional, defaults to "default".
  snmp_traps:
    enabled: true
    port: 9162 # on which ports to listen for traps
    community_strings: # which community strings to allow for v2 traps
      - st0r@gegrid
```

Esempio di configurazione SNMP StorageGRID

L'agente SNMP nel sistema StorageGRID si trova nella scheda di configurazione, colonna Monitoring (monitoraggio). Attivare SNMP e immettere le informazioni desiderate. Se si desidera configurare i trap, selezionare "Destinations trap" (Destinazioni trap) e creare una destinazione per l'host dell'agente Datadog contenente la configurazione trap.



Di Aron Klein

Utilizzare rclone per migrare, INSERIRE ed ELIMINARE oggetti su StorageGRID

Rclone è un tool e client a riga di comando gratuito per le operazioni S3. È possibile utilizzare rclone per migrare, copiare ed eliminare i dati degli oggetti su StorageGRID. rclone include la possibilità di eliminare i bucket anche quando non sono vuoti con una funzione di "purge", come illustrato nell'esempio riportato di seguito.

Installare e configurare rclone

Per installare rclone su una workstation o su un server, scaricarlo da "rclone.org".

Fasi iniziali della configurazione

1. Creare il file di configurazione rclone eseguendo lo script di configurazione o creando manualmente il file.
2. In questo esempio userò sgdemo come nome dell'endpoint remoto di StorageGRID S3 nella configurazione rclone.
   a. Creare il file di configurazione ~/.config/rclone/rclone.conf

```
[sgdemo]
type = s3
provider = Other
access_key_id = ABCDEFGH123456789JKL
secret_access_key = 123456789ABCDEFGHIJKLMN0123456789PQRST+V
endpoint = sgdemo.netapp.com
```

   b. Eseguire rclone config

config. rclone

```
2023/04/13 14:22:45 NOTICE: Config file
"/root/.config/rclone/rclone.conf" not found - using defaults
No remotes found - make a new one
n) New remote
s) Set configuration password
q) Quit config
n/s/q> n
name> sgdemo
```

```
Option Storage.
Type of storage to configure.
Enter a string value. Press Enter for the default ("").
Choose a number from below, or type in your own value.
 1 / 1Fichier
   \ "fichier"
 2 / Alias for an existing remote
   \ "alias"
 3 / Amazon Drive
   \ "amazon cloud drive"
 4 / Amazon S3 Compliant Storage Providers including AWS,
Alibaba, Ceph, Digital Ocean, Dreamhost, IBM COS, Minio,
SeaweedFS, and Tencent COS
   \ "s3"
 5 / Backblaze B2
   \ "b2"
 6 / Better checksums for other remotes
   \ "hasher"
 7 / Box
   \ "box"
 8 / Cache a remote
   \ "cache"
 9 / Citrix Sharefile
   \ "sharefile"
10 / Compress a remote
   \ "compress"
11 / Dropbox
   \ "dropbox"
12 / Encrypt/Decrypt a remote
   \ "crypt"
13 / Enterprise File Fabric
   \ "filefabric"
14 / FTP Connection
```

```
   \ "ftp"
15 / Google Cloud Storage (this is not Google Drive)
   \ "google cloud storage"
16 / Google Drive
   \ "drive"
17 / Google Photos
   \ "google photos"
18 / Hadoop distributed file system
   \ "hdfs"
19 / Hubic
   \ "hubic"
20 / In memory object storage system.
   \ "memory"
21 / Jottacloud
   \ "jottacloud"
22 / Koofr
   \ "koofr"
23 / Local Disk
   \ "local"
24 / Mail.ru Cloud
   \ "mailru"
25 / Mega
   \ "mega"
26 / Microsoft Azure Blob Storage
   \ "azureblob"
27 / Microsoft OneDrive
   \ "onedrive"
28 / OpenDrive
   \ "opendrive"
29 / OpenStack Swift (Rackspace Cloud Files, Memset Memstore,
OVH)
   \ "swift"
30 / Pcloud
   \ "pcloud"
31 / Put.io
   \ "putio"
32 / QingCloud Object Storage
   \ "qingstor"
33 / SSH/SFTP Connection
   \ "sftp"
34 / Sia Decentralized Cloud
   \ "sia"
35 / Sugarsync
   \ "sugarsync"
36 / Tardigrade Decentralized Cloud Storage
   \ "tardigrade"
```

```
37 / Transparently chunk/split large files
   \ "chunker"
38 / Union merges the contents of several upstream fs
   \ "union"
39 / Uptobox
   \ "uptobox"
40 / Webdav
   \ "webdav"
41 / Yandex Disk
   \ "yandex"
42 / Zoho
   \ "zoho"
43 / http Connection
   \ "http"
44 / premiumize.me
   \ "premiumizeme"
45 / seafile
   \ "seafile"
```

```
Storage> 4
```

```
Option provider.
Choose your S3 provider.
Enter a string value. Press Enter for the default ("").
Choose a number from below, or type in your own value.
 1 / Amazon Web Services (AWS) S3
   \ "AWS"
 2 / Alibaba Cloud Object Storage System (OSS) formerly Aliyun
   \ "Alibaba"
 3 / Ceph Object Storage
   \ "Ceph"
 4 / Digital Ocean Spaces
   \ "DigitalOcean"
 5 / Dreamhost DreamObjects
   \ "Dreamhost"
 6 / IBM COS S3
   \ "IBMCOS"
 7 / Minio Object Storage
   \ "Minio"
 8 / Netease Object Storage (NOS)
   \ "Netease"
 9 / Scaleway Object Storage
   \ "Scaleway"
10 / SeaweedFS S3
   \ "SeaweedFS"
11 / StackPath Object Storage
   \ "StackPath"
12 / Tencent Cloud Object Storage (COS)
   \ "TencentCOS"
13 / Wasabi Object Storage
   \ "Wasabi"
14 / Any other S3 compatible provider
   \ "Other"
provider> 14
```

```
Option env_auth.
Get AWS credentials from runtime (environment variables or
EC2/ECS meta data if no env vars).
Only applies if access_key_id and secret_access_key is blank.
Enter a boolean value (true or false). Press Enter for the
default ("false").
Choose a number from below, or type in your own value.
 1 / Enter AWS credentials in the next step.
   \ "false"
 2 / Get AWS credentials from the environment (env vars or IAM).
   \ "true"
env_auth> 1
```

```
Option access_key_id.
AWS Access Key ID.
Leave blank for anonymous access or runtime credentials.
Enter a string value. Press Enter for the default ("").
access_key_id> ABCDEFGH123456789JKL
```

```
Option secret_access_key.
AWS Secret Access Key (password).
Leave blank for anonymous access or runtime credentials.
Enter a string value. Press Enter for the default ("").
secret_access_key> 123456789ABCDEFGHIJKLMN0123456789PQRST+V
```

```
Option region.
Region to connect to.
Leave blank if you are using an S3 clone and you don't have a
region.
Enter a string value. Press Enter for the default ("").
Choose a number from below, or type in your own value.
   / Use this if unsure.
 1 | Will use v4 signatures and an empty region.
   \ ""
   / Use this only if v4 signatures don't work.
 2 | E.g. pre Jewel/v10 CEPH.
   \ "other-v2-signature"
region> 1
```

```
Option endpoint.
Endpoint for S3 API.
Required when using an S3 clone.
Enter a string value. Press Enter for the default ("").
endpoint> sgdemo.netapp.com
```

```
Option location_constraint.
Location constraint - must be set to match the Region.
Leave blank if not sure. Used when creating buckets only.
Enter a string value. Press Enter for the default ("").
location_constraint>
```

```
Option acl.
Canned ACL used when creating buckets and storing or copying
objects.
This ACL is used for creating objects and if bucket_acl isn't
set, for creating buckets too.
For more info visit
https://docs.aws.amazon.com/AmazonS3/latest/dev/acl-
overview.html#canned-acl
Note that this ACL is applied when server-side copying objects as
S3
doesn't copy the ACL from the source but rather writes a fresh
one.
Enter a string value. Press Enter for the default ("").
Choose a number from below, or type in your own value.
   / Owner gets FULL_CONTROL.
 1 | No one else has access rights (default).
   \ "private"
   / Owner gets FULL_CONTROL.
 2 | The AllUsers group gets READ access.
   \ "public-read"
   / Owner gets FULL_CONTROL.
 3 | The AllUsers group gets READ and WRITE access.
   | Granting this on a bucket is generally not recommended.
   \ "public-read-write"
   / Owner gets FULL_CONTROL.
 4 | The AuthenticatedUsers group gets READ access.
   \ "authenticated-read"
   / Object owner gets FULL_CONTROL.
 5 | Bucket owner gets READ access.
   | If you specify this canned ACL when creating a bucket,
Amazon S3 ignores it.
   \ "bucket-owner-read"
   / Both the object owner and the bucket owner get FULL_CONTROL
over the object.
 6 | If you specify this canned ACL when creating a bucket,
Amazon S3 ignores it.
   \ "bucket-owner-full-control"
acl>
```

```
Edit advanced config?
y) Yes
n) No (default)
y/n> n
```

```
--------------------
[sgdemo]
type = s3
provider = Other
access_key_id = ABCDEFGH123456789JKL
secret_access_key = 123456789ABCDEFGHIJKLMN0123456789PQRST+V
endpoint = sgdemo.netapp.com:443
--------------------
y) Yes this is OK (default)
e) Edit this remote
d) Delete this remote
y/e/d>
```

```
Current remotes:
```

```
Name                 Type
====                 ====
sgdemo               s3
```

```
e) Edit existing remote
n) New remote
d) Delete remote
r) Rename remote
c) Copy remote
s) Set configuration password
q) Quit config
e/n/d/r/c/s/q> q
```

Esempi di comandi di base

- **Creare un bucket:**

  `rclone mkdir remote:bucket`

  ```
  mkdir sgdemo:test01
  ```

  > Utilizzare --no-check-certificate se si desidera ignorare i certificati SSL.

- **Elenca tutti i bucket:**

```
rclone lsd remote:
```

1. rclone lsd sgdemo:

- **Elenca oggetti in un bucket specifico:**

```
rclone ls remote:bucket
```

rclone ls sgdemo:test01

```
    65536 TestObject.0
    65536 TestObject.1
    65536 TestObject.10
    65536 TestObject.12
    65536 TestObject.13
    65536 TestObject.14
    65536 TestObject.15
    65536 TestObject.16
    65536 TestObject.17
    65536 TestObject.18
    65536 TestObject.2
    65536 TestObject.3
    65536 TestObject.5
    65536 TestObject.6
    65536 TestObject.7
    65536 TestObject.8
    65536 TestObject.9
  33554432 bigobj
      102 key.json
       47 locked01.txt
4294967296 sequential-read.0.0
       15 test.txt
      116 version.txt
```

- **Eliminare un bucket:**

```
rclone rmdir remote:bucket
```

rclone rmdir sgdemo:test02

- **Mettere un oggetto:**

```
rclone copy filename remote:bucket
```

~/test/testfile.txt sgdemo:test01

- **Ottenere un oggetto:**

```
rclone copy remote:bucket/objectname filename
```

~/testfile.txt test/testfileS3.txt

- **Elimina un oggetto:**

```
rclone delete remote:bucket/objectname
```

rclone delete sgdemo:test01/testfile.txt

- **Migrare oggetti in un bucket**

```
rclone sync source:bucket destination:bucket --progress

rclone sync source_directory destination:bucket --progress
```

rclone sync sgdemo:test01 sgdemo:clone01 --progress

```
Transferred:        4.032 GiB / 4.032 GiB, 100%, 95.484 KiB/s, ETA
0s
Transferred:           22 / 22, 100%
Elapsed time:       1m4.2s
```

Utilizzare --Progress o -P per visualizzare l'avanzamento dell'attività. In caso contrario, non viene visualizzato alcun output.

- **Elimina un bucket e tutti i contenuti degli oggetti**

```
rclone purge remote:bucket --progress
```

rclone purge sgdemo:test01 --progress

```
Transferred:              0 B / 0 B, -, 0 B/s, ETA -
Checks:                46 / 46, 100%
Deleted:               23 (files), 1 (dirs)
Elapsed time:         10.2s
```

rclone ls sgdemo:test01

```
2023/04/14 09:40:51 Failed to ls: directory not found
```

Di Siegfried Hepp e Aron Klein

Best practice di StorageGRID per l'implementazione con Veeam Backup and Replication

Questa guida si concentra sulla configurazione di NetApp StorageGRID e, in parte, su Veeam Backup and Replication. Questo documento è stato scritto per gli amministratori di storage e rete che hanno familiarità con i sistemi Linux e hanno il compito di mantenere o implementare un sistema NetApp StorageGRID in combinazione con Veeam Backup and Replication.

Panoramica

Gli amministratori dello storage cercano di gestire la crescita dei propri dati con soluzioni che soddisfino la disponibilità, gli obiettivi di recovery rapido, scalino per soddisfare le loro esigenze e automatizzino la policy per la conservazione dei dati a lungo termine. Queste soluzioni devono anche fornire protezione da perdite o attacchi dannosi. Insieme, Veeam e NetApp hanno avviato una partnership per creare una soluzione di data Protection che combina Veeam Backup & Recovery con NetApp StorageGRID per lo storage a oggetti on-premise.

Veeam e NetApp StorageGRID offrono una soluzione facile da utilizzare che lavorano insieme per contribuire a soddisfare le richieste di una rapida crescita dei dati e di maggiori normative in tutto il mondo. Lo storage a oggetti basato sul cloud è celebre per la sua resilienza, la sua capacità di scalare, le efficienze operative e i costi che lo rendono la scelta naturale come destinazione dei backup. Questo documento fornirà linee guida e consigli per la configurazione della soluzione Veeam Backup e del sistema StorageGRID.

Il workload a oggetti di Veeam crea un elevato numero di operazioni simultanee di PUT, DELETE ed LIST di piccoli oggetti. L'attivazione dell'immutabilità aumenta il numero di richieste all'archivio oggetti per l'impostazione della conservazione e dell'elenco delle versioni. Il processo di un processo di backup include la scrittura degli oggetti per la modifica giornaliera, quindi, una volta completate le nuove scritture, il processo eliminerà tutti gli oggetti in base al criterio di conservazione del backup. La pianificazione dei processi di backup si sovrappone quasi sempre. Questa sovrapposizione risulterà in un'ampia parte della finestra di backup che consiste in un carico di lavoro PUT/DELETE di 50/50 KB sull'archivio di oggetti. Rettificare in Veeam il numero di operazioni simultanee con l'impostazione dello slot di attività, aumentando la dimensione dell'oggetto aumentando la dimensione del blocco di lavoro di backup, riducendo il numero di oggetti nelle

richieste di eliminazione multioggetto, inoltre, la scelta della finestra temporale massima per il completamento dei lavori ottimizzerà la soluzione in termini di prestazioni e costi.

Assicurarsi di leggere la documentazione del prodotto per "Backup e replica di Veeam" e. "StorageGRID" prima di iniziare. Veeam offre calcolatori per comprendere il dimensionamento dell'infrastruttura Veeam e i requisiti di capacità da utilizzare prima del dimensionamento della soluzione StorageGRID. Verifica sempre le configurazioni validate di Veeam-NetApp nel sito web del Veeam Ready Program per "Veeam Ready Object, immutabilità degli oggetti e Repository".

Configurazione Veeam

Versione consigliata

Si consiglia sempre di rimanere aggiornati e di applicare gli aggiornamenti rapidi più recenti per il sistema Veeam Backup & Replication 12. Al momento consigliamo almeno di installare la patch Veeam P20230718.

S3 Configurazione del repository

Un repository di backup scale-out (SOBR) è il Tier di capacità dello storage a oggetti S3. Il Tier di capacità è un'estensione del repository primario che offre periodi di conservazione dei dati più lunghi e una soluzione di storage a costi inferiori. Veeam offre la possibilità di fornire immutabilità tramite l'API S3 Object Lock. Veeam 12 può utilizzare bucket multipli in un repository scale-out. StorageGRID non ha un limite per il numero di oggetti o la capacità in un singolo bucket. L'utilizzo di bucket multipli può migliorare le performance durante il backup di set di dati molto grandi, dove i dati di backup possono raggiungere la scalabilità di petabyte in oggetti.

In base al dimensionamento della soluzione e ai requisiti specifici, potrebbe essere necessario limitare le attività simultanee. Le impostazioni predefinite specificano uno slot di attività del repository per ogni core della CPU e per ogni slot di attività un limite di 64 slot di attività simultanei. Ad esempio, se il server dispone di 2 core CPU, per l'archivio oggetti verrà utilizzato un totale di 128 thread simultanei. Questo include PUT, GET e Batch Delete. Si consiglia di selezionare un limite conservativo agli slot di attività da utilizzare per iniziare e regolare questo valore una volta che i backup Veeam hanno raggiunto lo stato stabile dei nuovi backup e dei dati di backup in scadenza. Collabora con l'account team di NetApp per dimensionare il sistema StorageGRID in modo appropriato e soddisfare le finestre temporali e le performance desiderate. Per fornire la soluzione ottimale, potrebbe essere necessario regolare il numero di slot di attività e il limite di attività per slot.

Configurazione del processo di backup

I job di backup Veeam possono essere configurati con diverse opzioni di dimensione del blocco che devono essere prese in considerazione con attenzione. Le dimensioni predefinite del blocco sono di 1MB KB e, grazie all'efficienza dello storage, Veeam offre funzionalità di compressione e deduplica crea dimensioni degli oggetti di circa 500KB KB per il backup completo iniziale e oggetti 100-200kB per i job incrementali. Possiamo aumentare enormemente le performance e ridurre i requisiti per l'archivio di oggetti scegliendo una dimensione maggiore dei blocchi di backup. Sebbene le dimensioni maggiori dei blocchi apportino notevoli miglioramenti nelle performance dell'archivio di oggetti, si presenta al costo di potenzialmente aumentare i requisiti di capacità dello storage primario grazie alle ridotte performance di efficienza dello storage. Si consiglia di configurare i processi di backup con una dimensione blocco di 4MB KB che crea circa 2MB oggetti per i backup completi e dimensioni oggetto di 700kB-1MB KB per i backup incrementali. I clienti possono prendere in considerazione anche la configurazione dei lavori di backup utilizzando blocchi di 8 MB, che possono essere abilitati con l'assistenza del supporto Veeam.

L'implementazione di backup immutabili utilizza S3 Object Lock nell'archivio oggetti. L'opzione immutabilità genera un numero maggiore di richieste all'archivio oggetti per l'elenco e la conservazione degli aggiornamenti sugli oggetti.

Alla scadenza delle trattenute di backup, i lavori di backup elaboreranno l'eliminazione degli oggetti. Veeam invia le richieste di eliminazione all'archivio oggetti nelle richieste di eliminazione di più oggetti di 1000 oggetti per richiesta. Per le soluzioni di piccole dimensioni, potrebbe essere necessario regolarle per ridurre il numero di oggetti per richiesta. La riduzione di questo valore avrà il vantaggio di distribuire in modo più uniforme le richieste di eliminazione tra i nodi nel sistema StorageGRID. Si consiglia di utilizzare i valori nella tabella seguente come punto di partenza per configurare il limite di eliminazione di più oggetti. Moltiplicare il valore nella tabella per il numero di nodi per il tipo di appliance scelto per ottenere il valore per l'impostazione in Veeam. Se questo valore è uguale o superiore a 1000 non è necessario regolare il valore predefinito. Se questo valore deve essere modificato, si prega di collaborare con il supporto di Veeam per apportare la modifica.

Modello di appliance	S3MultiObjectDeleteLimit per nodo
SG5712	34
SG5760	75
SG6060	200

Contatta il tuo account team NetApp per ottenere la configurazione consigliata in base alle tue esigenze specifiche. Le raccomandazioni sulle impostazioni di configurazione di Veeam includono:

- Dimensione blocco processo di backup = 4MB
- Limite slot attività SOBR= 2-16
- Limite eliminazione oggetti multipli = 34-1000

Configurazione StorageGRID

Versione consigliata

NetApp StorageGRID 11,6 o 11,7 con la correzione rapida più recente sono le versioni consigliate per le implementazioni Veeam. Nel StorageGRID 11.6.0.11 e 11.7.0.4 sono state introdotte molte funzionalità di ottimizzazione che saranno vantaggiose per i workload Veeam. Si consiglia di restare sempre aggiornati e di applicare gli aggiornamenti rapidi più recenti per il sistema StorageGRID in uso.

Bilanciamento del carico e configurazione dell'endpoint S3

Veeam richiede che l'endpoint sia connesso solo tramite HTTPS. Una connessione non crittografata non è supportata da Veeam. Il certificato SSL può essere un certificato autofirmato, un'autorità di certificazione privata attendibile o un'autorità di certificazione pubblica attendibile. Per garantire un accesso continuo al repository S3, si consiglia di utilizzare almeno due bilanciatori del carico in una configurazione ha. I bilanciatori del carico possono essere un servizio di bilanciamento del carico integrato fornito da StorageGRID situato in ogni nodo amministrativo e nodo gateway o soluzione di terze parti come F5, Kemp, HAproxy, Loadbalanacer.org, ecc. L'utilizzo di un bilanciatore del carico StorageGRID fornirà la possibilità di impostare classificatori di traffico (regole QoS) che possono dare priorità al workload Veeam, o limitare Veeam a non influire sui carichi di lavoro a priorità più alta sul sistema StorageGRID.

Bucket S3

StorageGRID è un sistema storage multi-tenant sicuro. Si consiglia di creare un tenant dedicato per il workload Veeam. È possibile assegnare facoltativamente una quota di archiviazione. Come Best practice, è possibile utilizzare "utilizzare la propria origine identità". Proteggere l'utente di gestione root del tenant con una

password appropriata. Veeam Backup 12 richiede una forte coerenza per i bucket S3. StorageGRID offre diverse opzioni di coerenza configurate a livello di bucket. Per le implementazioni multi-sito con Veeam che accede ai dati da posizioni multiple, seleziona "strong-Global". Se Veeam effettua backup e ripristini solo su un singolo sito, dovrebbe essere impostato su "strong-site". Per ulteriori informazioni sui livelli di coerenza della benna, consultare la "documentazione". Per utilizzare StorageGRID per i backup di Veeam Immutability, S3 Object Lock deve essere abilitato a livello globale e configurato nel bucket durante la creazione del bucket.

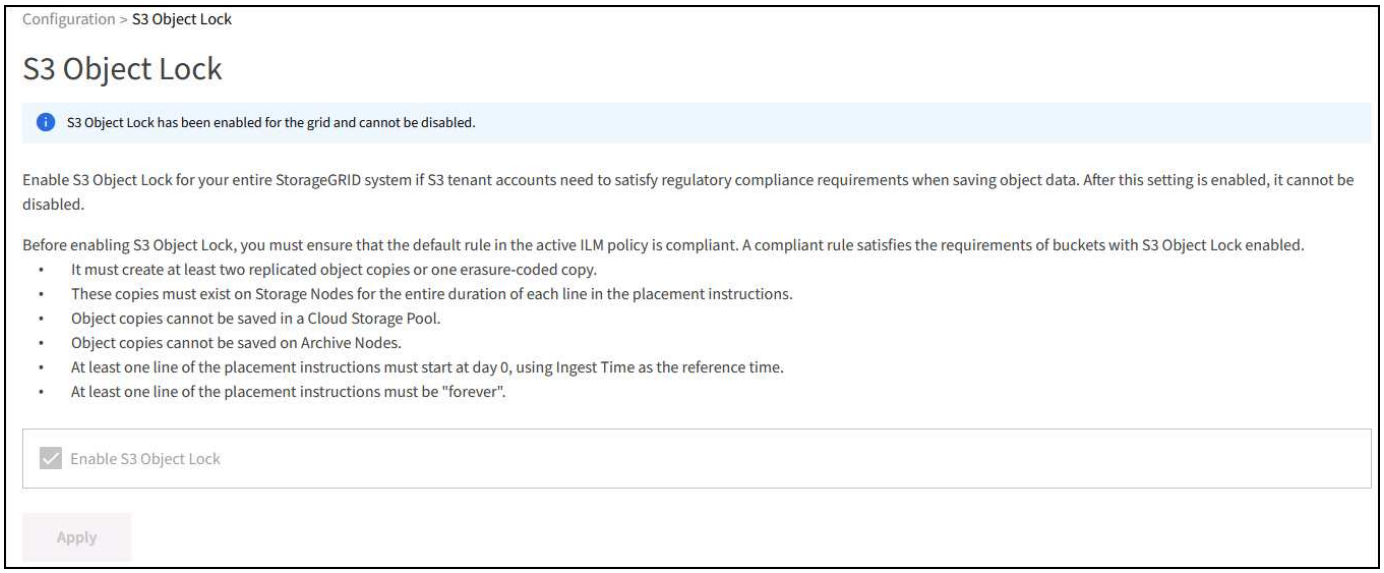
Gestione del ciclo di vita

StorageGRID supporta la replica e l'erasure coding per la protezione a livello di oggetto in siti e nodi StorageGRID. L'erasure coding richiede almeno una dimensione dell'oggetto di 200kB KB. Le dimensioni predefinite dei blocchi per Veeam di 1MB producono dimensioni degli oggetti che possono spesso essere inferiori a questa dimensione minima consigliata di 200kB KB dopo le efficienze di storage di Veeam. Per le performance della soluzione, non è consigliabile utilizzare un profilo di erasure coding su più siti, a meno che la connettività tra i siti non sia sufficiente per non aggiungere latenza o limitare la larghezza di banda del sistema StorageGRID. In un sistema StorageGRID multisito, la regola ILM può essere configurata per memorizzare una singola copia in ciascun sito. Per garantire la massima durata, è possibile configurare una regola per memorizzare una copia con erasure coding in ogni sito. L'utilizzo di due copie locali nei server Veeam Backup è l'implementazione più consigliata per questo workload.

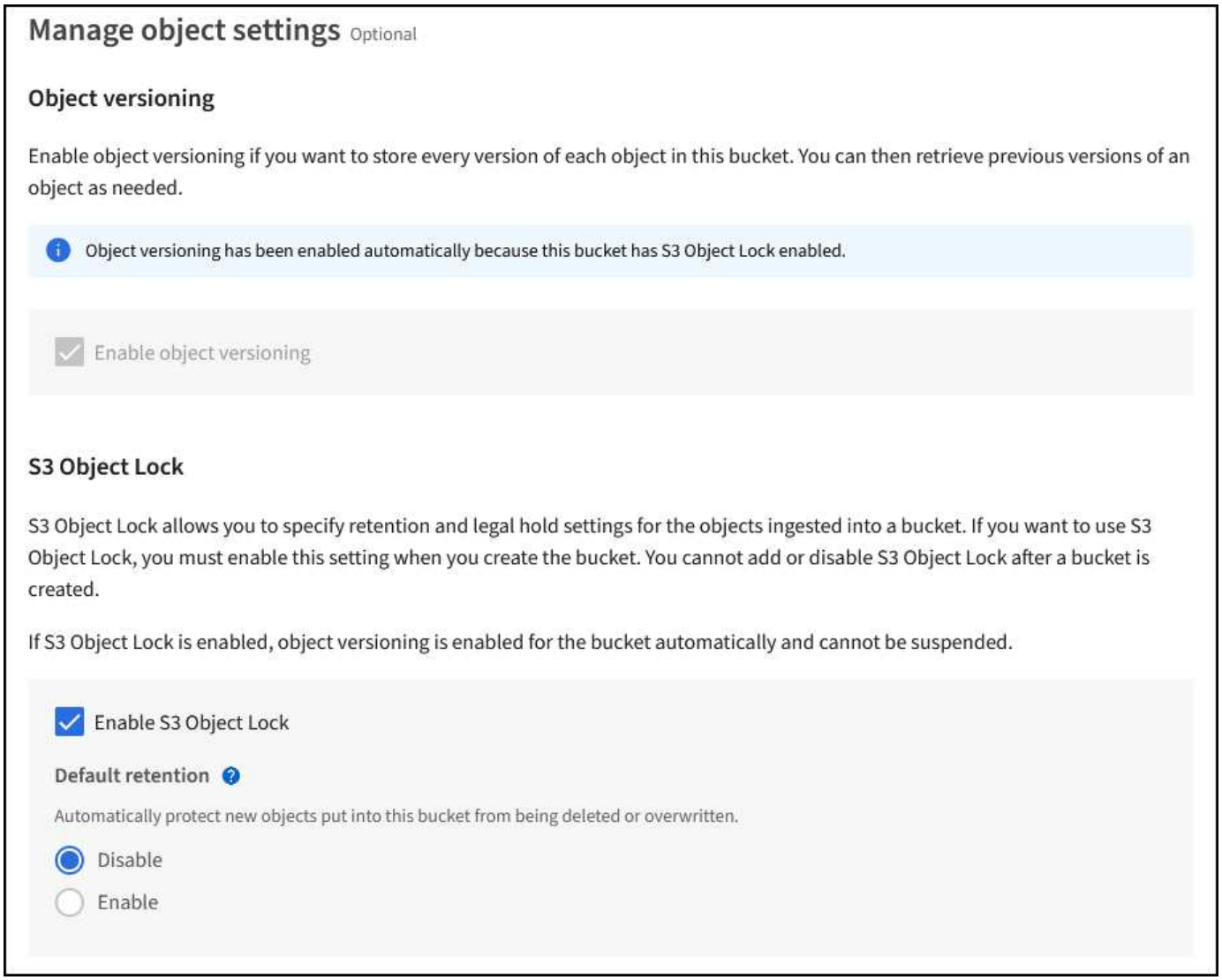
Punti chiave di implementazione

StorageGRID

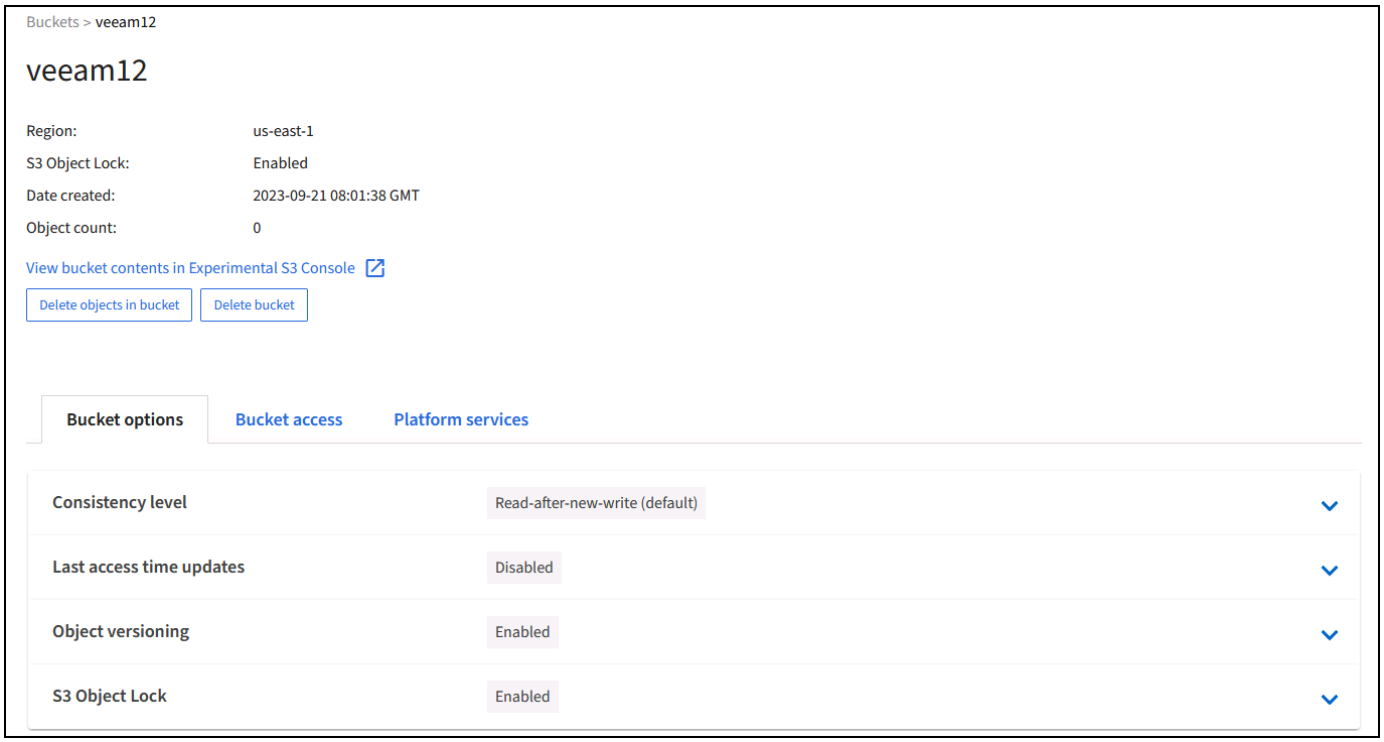
Assicurarsi che blocco oggetti sia attivato sul sistema StorageGRID se è necessaria l'immutabilità. Individuare l'opzione nell'interfaccia utente di gestione in Configurazione/blocco oggetti S3.



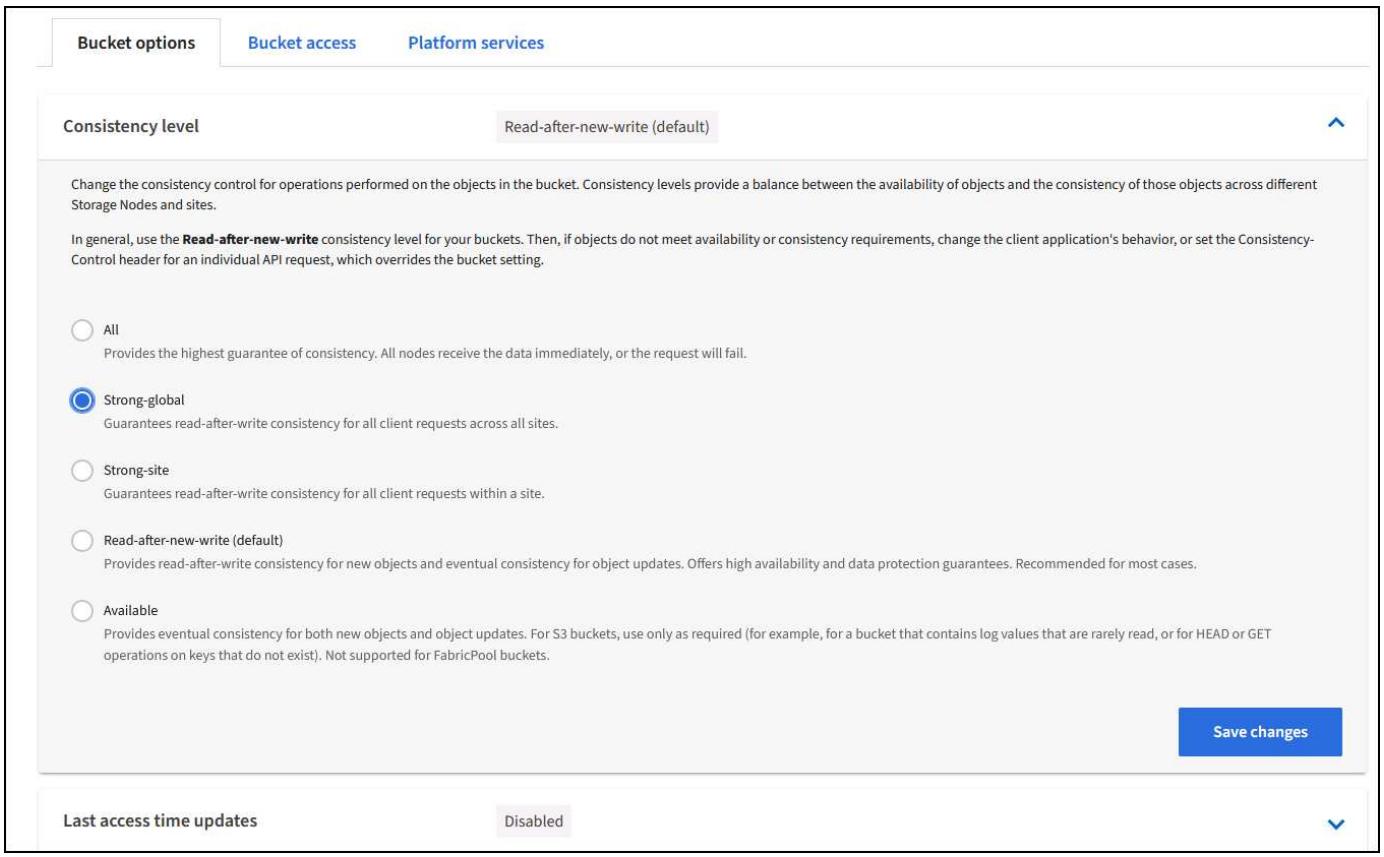
Quando si crea il bucket, selezionare "Enable S3 Object Lock" (attiva blocco oggetti 3D) se questo bucket deve essere utilizzato per i backup di immutabilità. In questo modo si attiva automaticamente la versione bucket. Lasciare disattivata la conservazione predefinita poiché Veeam imposterà esplicitamente la conservazione degli oggetti. Versioning e blocco oggetto S3 non devono essere selezionati se Veeam non sta creando backup immutabili.



Una volta creato il bucket, andare alla pagina dei dettagli del bucket creato. Selezionare il livello di coerenza.



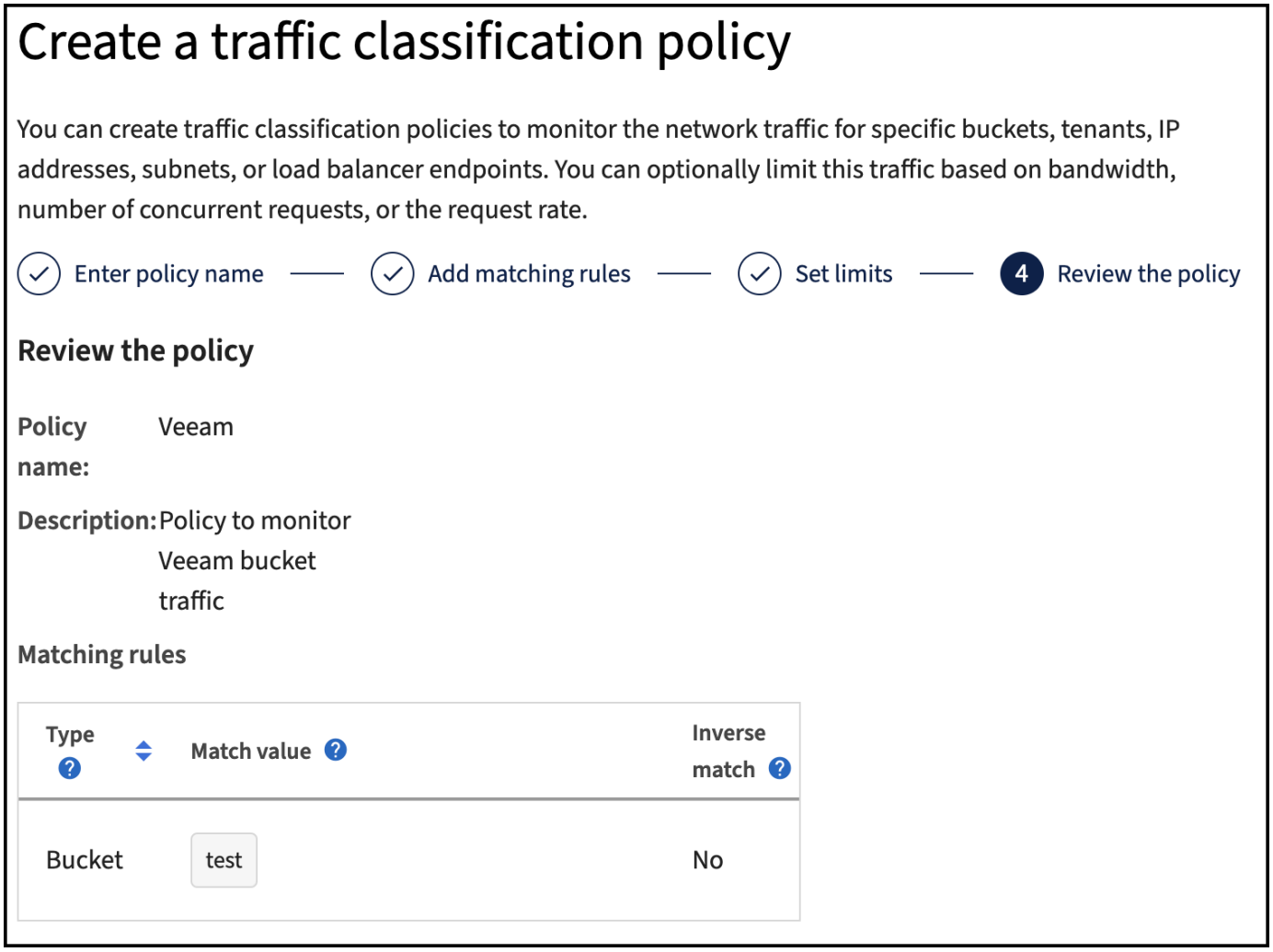
Veeam richiede una forte coerenza per i bucket S3. Quindi, per implementazioni multi-sito con Veeam che accede ai dati da posizioni multiple, seleziona "strong-Global". Se Veeam effettua backup e ripristini solo su un singolo sito, dovrebbe essere impostato su "strong-site". Salvare le modifiche.



StorageGRID fornisce un servizio di bilanciamento del carico integrato in ogni nodo amministrativo e nodo di gateway dedicato. Uno dei numerosi vantaggi dell'utilizzo di questo bilanciamento del carico è la possibilità di

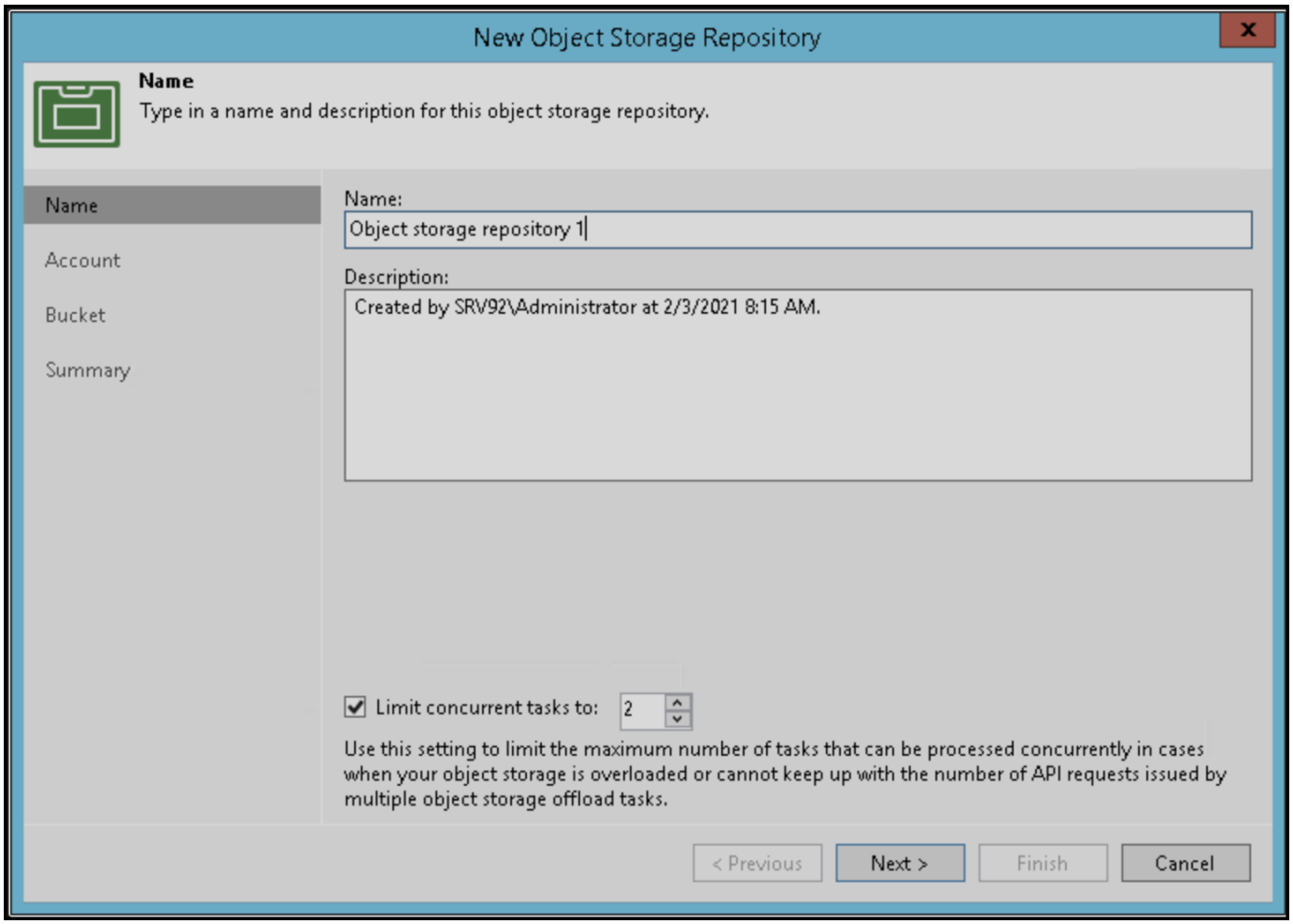
configurare i criteri di classificazione del traffico (QoS). Sebbene vengano utilizzati principalmente per limitare l'impatto di un'applicazione su altri carichi di lavoro dei client o per assegnare priorità a un carico di lavoro rispetto ad altri, forniscono anche un bonus di raccolta di metriche aggiuntive per agevolare il monitoraggio.

Nella scheda di configurazione, selezionare "Traffic Classification" (classificazione traffico) e creare una nuova policy. Assegnare un nome alla regola e selezionare il bucket o il tenant come tipo. Immettere i nomi dei bucket o locatario. Se la QoS è necessaria, impostare un limite, ma per la maggior parte delle implementazioni, è sufficiente aggiungere i vantaggi di monitoraggio che questo fornisce, quindi non impostare un limite.

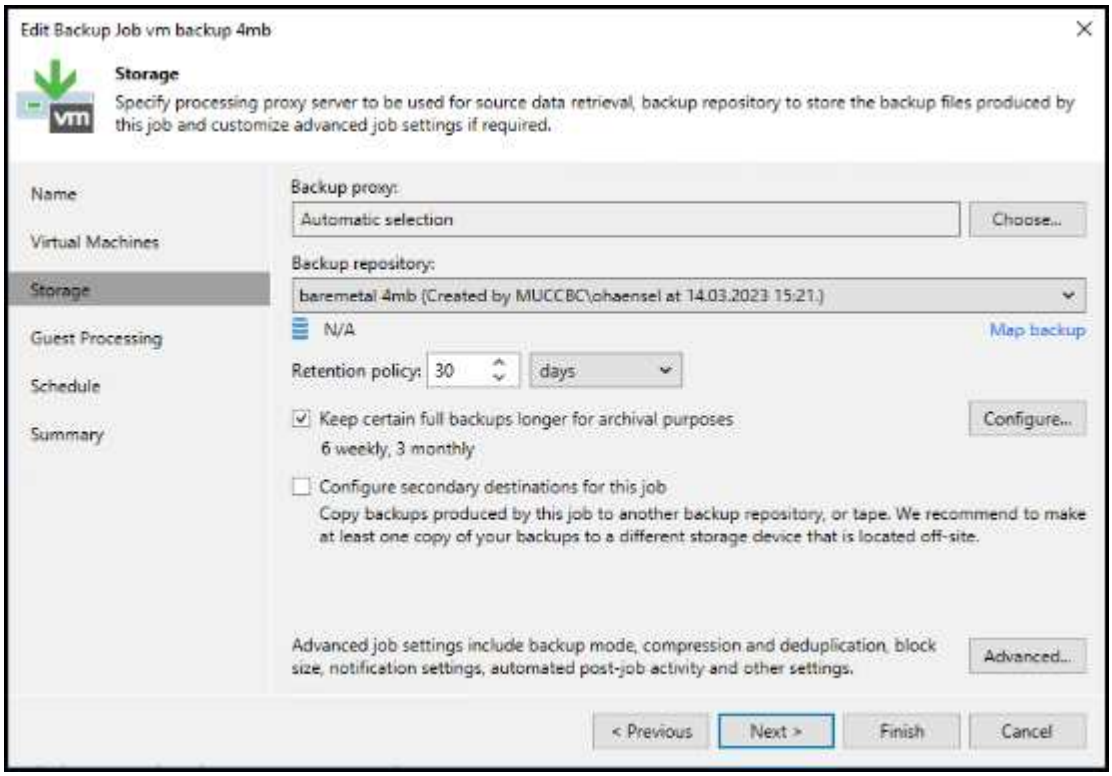


Veeam

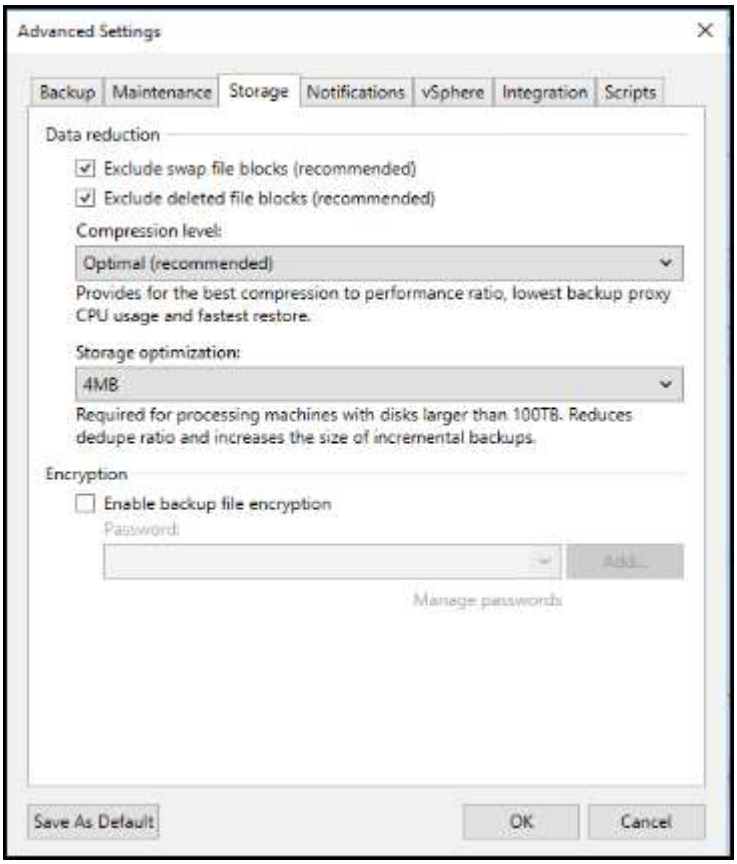
A seconda del modello e della quantità di appliance StorageGRID, potrebbe essere necessario selezionare e configurare un limite al numero di operazioni simultanee nel bucket.



Seguite la documentazione Veeam sulla configurazione del lavoro di backup nella console Veeam per avviare la procedura guidata. Dopo aver aggiunto le VM, selezionare il repository SOBR.



Fare clic su Impostazioni avanzate e modificare le impostazioni di ottimizzazione dell'archiviazione a 4 MB o più. Compressione e deduplica devono essere abilitate. Modificare le impostazioni guest in base ai requisiti e configurare la pianificazione del processo di backup.



Monitoraggio di StorageGRID

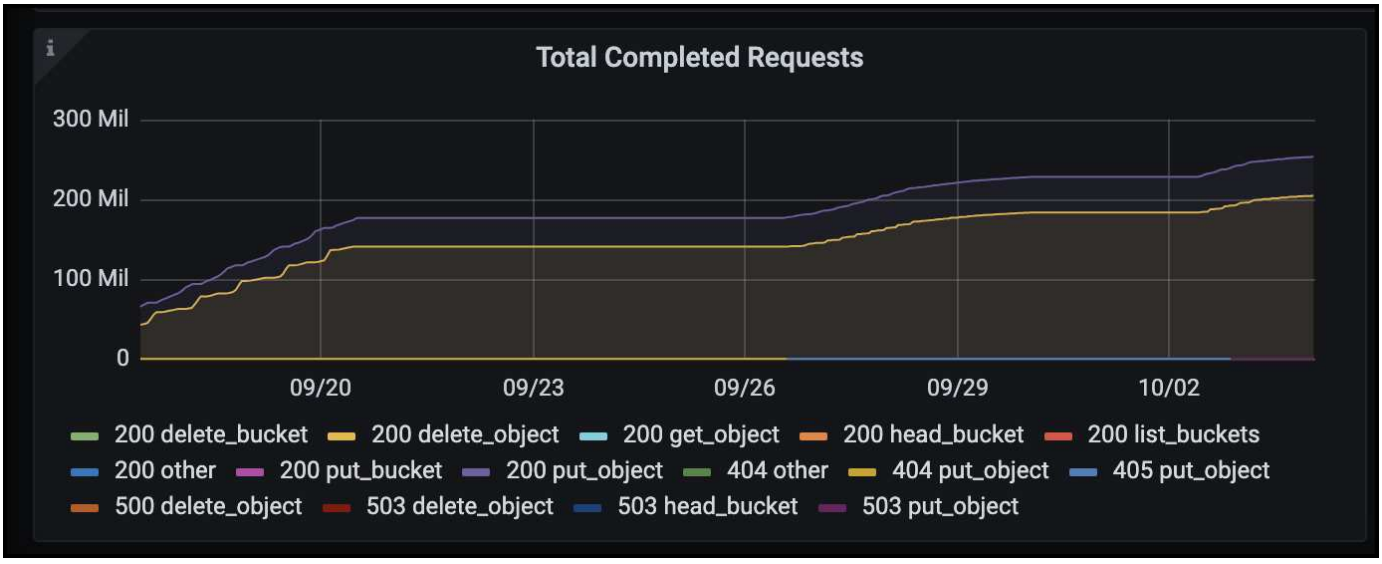
Per avere un quadro completo delle prestazioni congiunte di Veeam e StorageGRID, devi attendere la scadenza del tempo di conservazione dei primi backup. Fino a questo punto il workload Veeam è costituito principalmente da operazioni PUT e non si sono verificati eliminazioni. Una volta che i dati di backup stanno per scadere e le operazioni di pulizia sono in corso, è ora possibile vedere l'utilizzo completo e coerente nell'archivio oggetti e regolare le impostazioni in Veeam, se necessario.

StorageGRID fornisce utili grafici per monitorare il funzionamento del sistema nella pagina metriche della scheda supporto. I dashboard principali da esaminare saranno S3 Overview, ILM e Traffic Classification Policy, se è stato creato un criterio. Nel dashboard Panoramica di S3 sono disponibili informazioni su velocità operative, latenze e risposte delle richieste di S3.

Osservando le velocità S3 e le richieste attive è possibile visualizzare la quantità di carico gestita da ciascun nodo e il numero complessivo di richieste in base al tipo.

Il grafico durata media mostra il tempo medio impiegato da ciascun nodo per ciascun tipo di richiesta. Questa è la latenza media della richiesta e potrebbe essere un buon indicatore che potrebbe essere necessaria una regolazione aggiuntiva o che il sistema StorageGRID può assumere più carico.

Nel grafico Total Completed Requests (Richieste totali completate), è possibile visualizzare le richieste per tipo e codici di risposta. Se si visualizzano risposte diverse da 200 (OK) per le risposte, questo potrebbe indicare un problema come il sistema StorageGRID sta caricando pesantemente inviando 503 risposte (rallentando) e potrebbe essere necessario un ulteriore tuning, o è arrivato il momento di espandere il sistema per il carico aumentato.



Nel dashboard ILM è possibile monitorare le prestazioni di eliminazione del sistema StorageGRID. StorageGRID utilizza una combinazione di eliminazioni sincrone e asincrone su ciascun nodo per provare e

ottimizzare le performance complessive per tutte le richieste.

Con una Traffic Classification Policy, possiamo visualizzare le metriche sul carico bilanciatore richiesta throughput, tassi, durata, così come le dimensioni oggetto che Veeam sta inviando e ricevendo.

Dove trovare ulteriori informazioni

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

- "Documentazione del prodotto NetApp StorageGRID 11,7"
- "Backup e replica di Veeam"

Di Oliver Haensel e Aron Klein

Configurare l'origine dati Dremio con StorageGRID

Dremio supporta una varietà di origini dati, incluso lo storage a oggetti on-premise o basato su cloud. È possibile configurare Dremio in modo che utilizzi StorageGRID come origine dati dello storage a oggetti.

Configurare l'origine dati Dremio

Prerequisiti

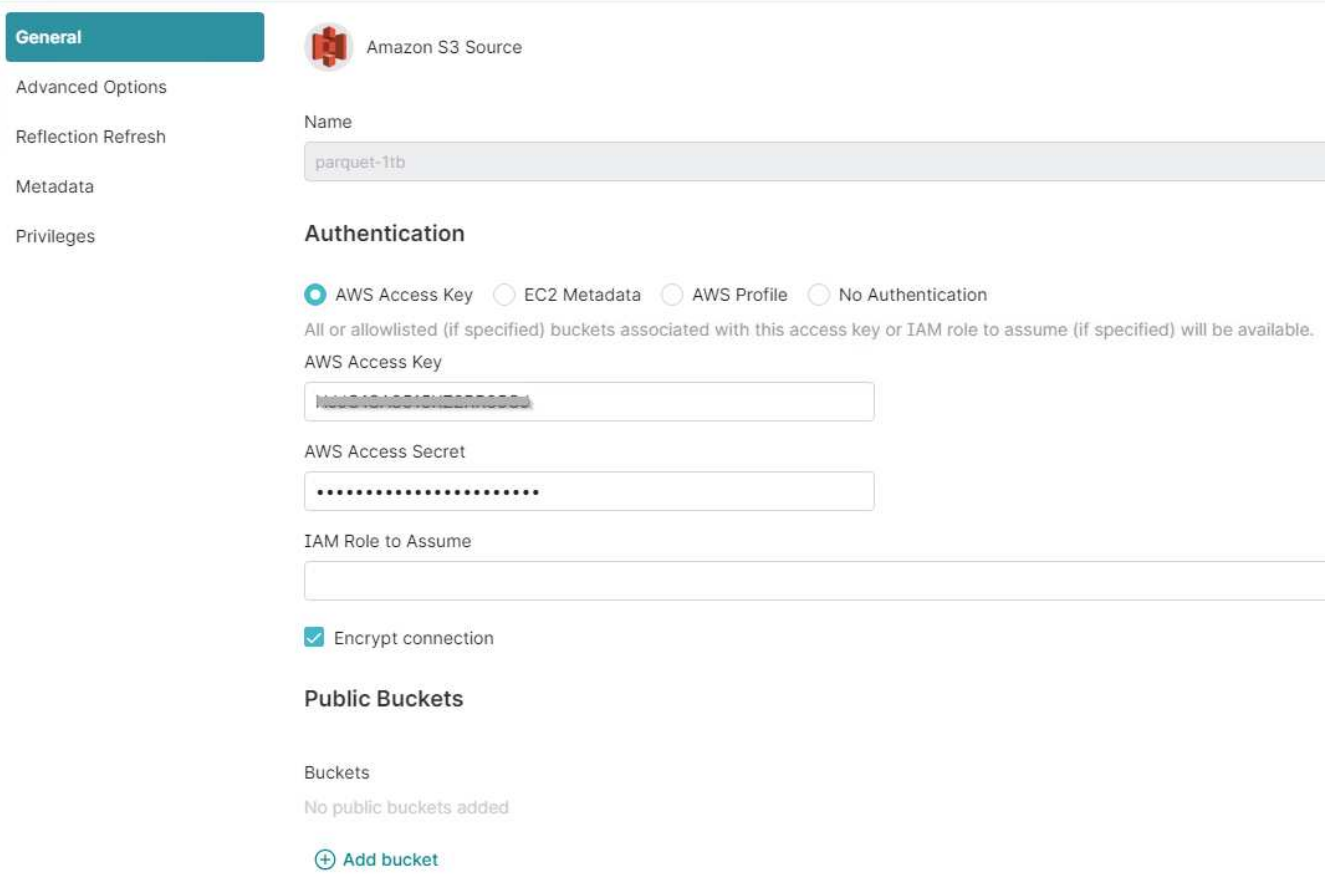
- Un URL dell'endpoint StorageGRID S3, un ID della chiave di accesso tenant S3 e una chiave di accesso segreta.
- Raccomandazione per la configurazione di StorageGRID: Disattivare la compressione (disattivata per impostazione predefinita).
  Dremio utilizza l'intervallo di byte GET per recuperare contemporaneamente diversi intervalli di byte dall'interno dello stesso oggetto durante la query. Le dimensioni tipiche per le richieste di intervalli di byte sono 1MB. L'oggetto compresso riduce le prestazioni di LETTURA DELL'intervallo di byte.

Guida di Dremio

"Connessione ad Amazon S3 - Configurazione dell'archiviazione compatibile con S3".

Istruzioni

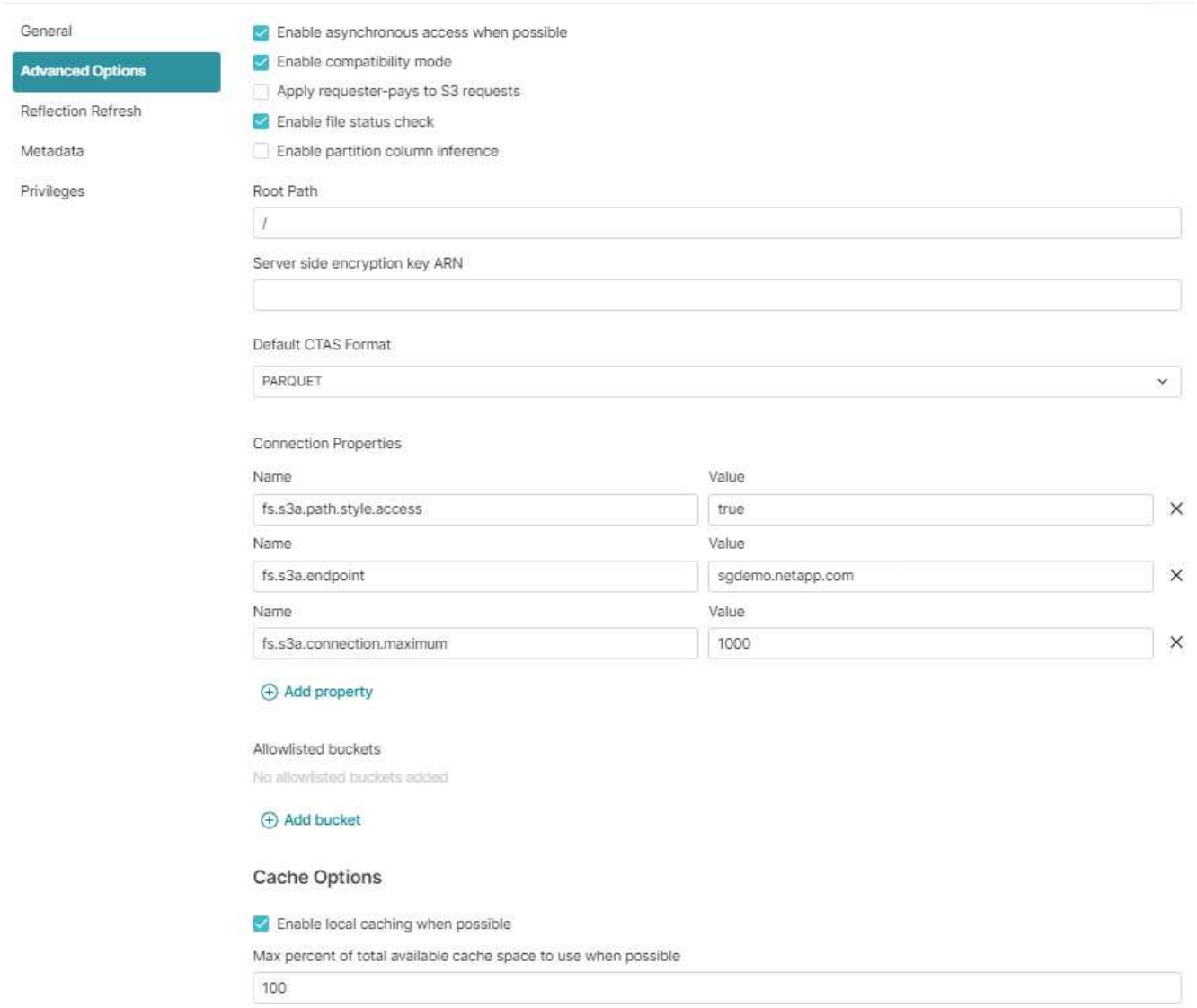
1. Nella pagina Datasets di Dremio, fare clic sul segno + per aggiungere un'origine, selezionare "Amazon S3".
2. Immettere un nome per la nuova origine dati, l'ID della chiave di accesso tenant StorageGRID S3 e la chiave di accesso segreta.
3. Selezionare la casella 'Crittografa connessione' se si utilizza https per la connessione all'endpoint StorageGRID S3.
   Se si utilizza un certificato CA autofirmato per questo endpoint S3, seguire la procedura della guida Dremio per aggiungere questo certificato CA a <JAVA_HOME>/jre/lib/Security + del server Dremio
   Esempio di screenshot



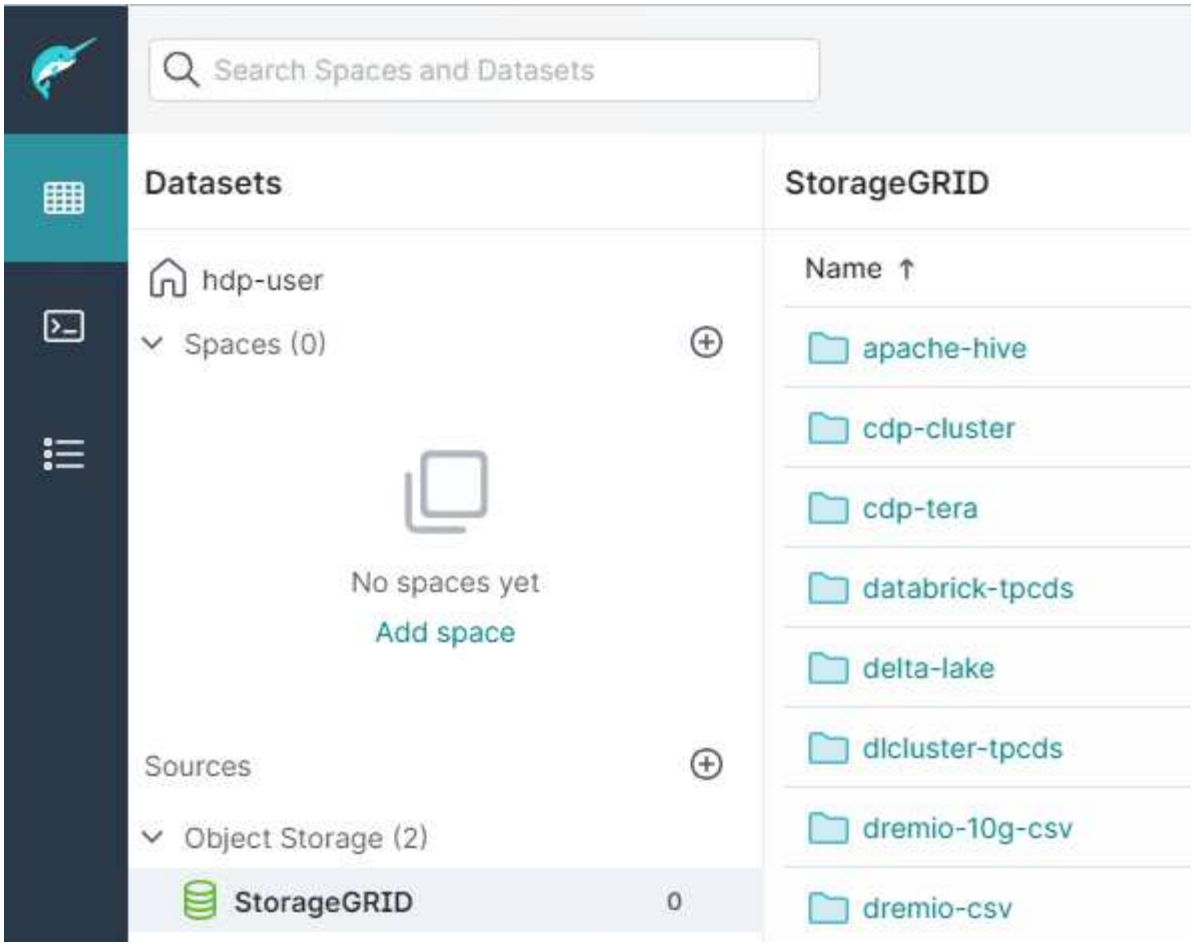
4. Fare clic su "Opzioni avanzate" e selezionare "attiva modalità di compatibilità"
5. In Proprietà di connessione, fare clic su + Aggiungi proprietà e aggiungere queste S3A proprietà.
6. fs.s3a.connection.il valore massimo predefinito è 100. Se i set di dati S3 includono file Parquet di grandi dimensioni con 100 o più colonne, è necessario immettere un valore maggiore di 100. Per questa impostazione, fare riferimento alla guida Dremio.

Nome	Valore
fs.s3a.endpoint	*<StorageGRID S3 endpoint:porta>*
fs.s3a.path.style.access	vero
fs.s3a.connection.maximum	*<un valore maggiore di 100>*

Esempio di screenshot



7. Configurare altre opzioni Dremio in base ai requisiti dell'organizzazione o delle applicazioni.
8. Fare clic sul pulsante Salva per creare questa nuova origine dati.
9. Una volta aggiunta correttamente l'origine dati StorageGRID, viene visualizzato un elenco di bucket sul pannello di sinistra.
   Esempio di screenshot



Di Angela Cheng

NetApp StorageGRID con GitLab

NetApp ha testato StorageGRID con GitLab. Vedere l'esempio di configurazione GitLab riportato di seguito. Fare riferimento a. "Guida alla configurazione dello storage a oggetti GitLab" per ulteriori informazioni.

Esempio di connessione allo storage a oggetti

Per le installazioni dei pacchetti Linux, questo è un esempio di `connection` impostazione nel modulo consolidato. Modifica `/etc/gitlab/gitlab.rb` e aggiungere le seguenti righe, sostituendo i valori desiderati:

```
# Consolidated object storage configuration
gitlab_rails['object_store']['enabled'] = true
gitlab_rails['object_store']['proxy_download'] = true
gitlab_rails['object_store']['connection'] = {
  'provider' => 'AWS',
  'region' => 'us-east-1',
  'endpoint' => 'https://<storagegrid-s3-endpoint:port>',
  'path_stype' => 'true',
  'aws_access_key_id' => '<AWS_ACCESS_KEY_ID>',
  'aws_secret_access_key' => '<AWS_SECRET_ACCESS_KEY>'
}
# OPTIONAL: The following lines are only needed if server side encryption
is required
gitlab_rails['object_store']['storage_options'] = {
  'server_side_encryption' => 'AES256'
}
gitlab_rails['object_store']['objects']['artifacts']['bucket'] = 'gitlab-
artifacts'
gitlab_rails['object_store']['objects']['external_diffs']['bucket'] =
'gitlab-mr-diffs'
gitlab_rails['object_store']['objects']['lfs']['bucket'] = 'gitlab-lfs'
gitlab_rails['object_store']['objects']['uploads']['bucket'] = 'gitlab-
uploads'
gitlab_rails['object_store']['objects']['packages']['bucket'] = 'gitlab-
packages'
gitlab_rails['object_store']['objects']['dependency_proxy']['bucket'] =
'gitlab-dependency-proxy'
gitlab_rails['object_store']['objects']['terraform_state']['bucket'] =
'gitlab-terraform-state'
gitlab_rails['object_store']['objects']['pages']['bucket'] = 'gitlab-
pages'
```

Procedure ed esempi di API

Testare e dimostrare le opzioni di crittografia S3 su StorageGRID

StorageGRID e l'API S3 offrono diversi modi per crittografare i dati inattivi. Per ulteriori informazioni, vedere "Esaminare i metodi di crittografia StorageGRID".

Questa guida illustra i metodi di crittografia dell'API S3.

Server Side Encryption (SSE)

SSE consente al client di memorizzare un oggetto e di crittografarlo con una chiave univoca gestita da StorageGRID. Quando l'oggetto viene richiesto, l'oggetto viene decrittografato dalla chiave memorizzata in StorageGRID.

Esempio SSE

- METTI un oggetto con SSE

```
aws s3api put-object --bucket <bucket>  --key <file> --body "<file>"
--server-side-encryption AES256 --endpoint-url https://s3.example.com
```

- TESTA l'oggetto per verificare la crittografia

```
aws s3api head-object --bucket <bucket>  --key <file>   --endpoint-url
https://s3.example.com
```

```
{
    "AcceptRanges": "bytes",
    "LastModified": "2022-05-02T19:03:03+00:00",
    "ContentLength": 47,
    "ETag": "\"82e8bfb872e778a4687a26e6c0b36bc1\"",
    "ContentType": "text/plain",
    "ServerSideEncryption": "AES256",
    "Metadata": {}
}
```

- OTTIENI l'oggetto

```
aws s3api get-object --bucket <bucket>  --key <file> <file> --endpoint
-url https://s3.example.com
```

Crittografia lato server con chiavi fornite dal cliente (SSE-C)

SSE consente al client di memorizzare un oggetto e di crittografarlo con una chiave univoca fornita dal client con l'oggetto. Quando l'oggetto viene richiesto, è necessario fornire la stessa chiave per decrittare e restituire l'oggetto.

Esempio SSE-C.

- A scopo di test o dimostrazione, è possibile creare una chiave di crittografia
  - Creare una chiave di crittografia

```
openssl enc -aes-128-cbc -pass pass:secret -P`
```

```
salt=E9DBB6603C7B3D2A
key=23832BAC16516152E560F933F261BF03
iv =71E87C0F6EC3C45921C2754BA131A315
```

- Inserire un oggetto con la chiave generata

```
aws s3api put-object --bucket <bucket> --key <file> --body "file" --sse
-customer-algorithm AES256 --sse-customer-key
23832BAC16516152E560F933F261BF03 --endpoint-url https://s3.example.com
```

- Testa l'oggetto

```
aws s3api head-object --bucket <bucket> --key <file> --sse-customer
-algorithm AES256 --sse-customer-key 23832BAC16516152E560F933F261BF03
--endpoint-url https://s3.example.com
```

```
            {
                "AcceptRanges": "bytes",
                "LastModified": "2022-05-02T19:20:02+00:00",
                "ContentLength": 47,
                "ETag": "\"f92ef20ab87e0e13951d9bee862e9f9a\"",
                "ContentType": "binary/octet-stream",
                "Metadata": {},
                "SSECustomerAlgorithm": "AES256",
                "SSECustomerKeyMD5": "rjGuMdjLpPV1eRuotNaPMQ=="
            }
```

Se non si fornisce la chiave di crittografia, viene visualizzato il messaggio di errore "si è verificato un errore (404) durante la chiamata dell'operazione HeadObject: Non trovata"

- Ottieni l'oggetto

```
aws s3api get-object --bucket <bucket> --key <file> <file> --sse
-customer-algorithm AES256 --sse-customer-key
23832BAC16516152E560F933F261BF03 --endpoint-url https://s3.example.com
```

Se non si fornisce la chiave di crittografia, viene visualizzato l'errore "si è verificato un errore (InvalidRequest) durante la chiamata dell'operazione GetObject: L'oggetto è stato memorizzato utilizzando un modulo di Server Side Encryption. Per recuperare l'oggetto, è necessario fornire i parametri corretti."

Crittografia lato server bucket (SSE-S3)

SSE-S3 consente al client di definire un comportamento di crittografia predefinito per tutti gli oggetti memorizzati in un bucket. Gli oggetti vengono crittografati con una chiave univoca gestita da StorageGRID. Quando l'oggetto viene richiesto, l'oggetto viene decrittografato dalla chiave memorizzata in StorageGRID.

Esempio di bucket SSE-S3

- Creare un nuovo bucket e impostare una policy di crittografia predefinita
  - Creare un nuovo bucket

```
aws s3api create-bucket --bucket <bucket> --region us-east-1
--endpoint-url https://s3.example.com
```

  - Metti la crittografia bucket

```
aws s3api put-bucket-encryption --bucket <bucket> --server-side
-encryption-configuration '{"Rules":
[{"ApplyServerSideEncryptionByDefault": {"SSEAlgorithm":
"AES256"}}]}' --endpoint-url https://s3.example.com
```

- Metti un oggetto nel bucket

```
aws s3api put-object --bucket <bucket> --key <file> --body "file"
--endpoint-url https://s3.example.com
```

- Testa l'oggetto

```
aws s3api head-object --bucket <bucket> --key <file> --endpoint-url
https://s3.example.com
```

```
{
"AcceptRanges": "bytes",
"LastModified": "2022-05-02T20:16:23+00:00",
"ContentLength": 47,
"ETag": "\"82e8bfb872e778a4687a26e6c0b36bc1\"",
"ContentType": "binary/octet-stream",
"ServerSideEncryption": "AES256",
"Metadata": {}
}
```

- OTTIENI l'oggetto

```
aws s3api get-object --bucket <bucket>  --key <file> <file> --endpoint
-url https://s3.example.com
```

Di Aron Klein

Testare e dimostrare il blocco di oggetti S3 su StorageGRID

Object Lock fornisce un modello WORM per impedire l'eliminazione o la sovrascrittura degli oggetti. L'implementazione StorageGRID del blocco degli oggetti viene valutata da Cohasset per soddisfare i requisiti normativi, supportare la modalità di conservazione legale e di conformità per la conservazione degli oggetti e le policy di conservazione predefinite dei bucket.

Questa guida illustra l'API S3 Object Lock.

Conservazione a fini giudiziari

- Object Lock legal hold è un semplice stato on/off applicato a un oggetto.

```
aws s3api put-object-legal-hold --bucket <bucket> --key <file> --legal
-hold Status=ON --endpoint-url https://s3.company.com
```

- Verificarlo con un'operazione GET.

```
aws s3api get-object-legal-hold --bucket <bucket> --key <file>
--endpoint-url https://s3.company.com
```

```
{
    "LegalHold": {
        "Status": "ON"
    }
}
```

- Disattivare la sospensione legale

```
aws s3api put-object-legal-hold --bucket <bucket> --key <file> --legal
-hold Status=OFF --endpoint-url https://s3.company.com
```

- Verificarlo con un'operazione GET.

```
aws s3api get-object-legal-hold --bucket <bucket> --key <file>
--endpoint-url https://s3.company.com
```

```
{
    "LegalHold": {
        "Status": "OFF"
    }
}
```

Modalità compliance

- La conservazione degli oggetti viene eseguita con un periodo di conservazione fino a data e ora.

```
aws s3api put-object-retention --bucket <bucket> --key <file>
--retention '{"Mode":"COMPLIANCE", "RetainUntilDate": "2025-06-
10T16:00:00"}' --endpoint-url https://s3.company.com
```

- Verificare lo stato di conservazione

```
aws s3api get-object-retention --bucket <bucket> --key <file> --endpoint
-url https://s3.company.com
+
```

```
{
    "Retention": {
        "Mode": "COMPLIANCE",
        "RetainUntilDate": "2025-06-10T16:00:00+00:00"
    }
}
```

Conservazione predefinita

- Impostare il periodo di conservazione in giorni e anni rispetto alla data di conservazione definita con l'api per oggetto.

```
aws s3api put-object-lock-configuration --bucket <bucket> --object-lock
-configuration '{"ObjectLockEnabled": "Enabled", "Rule": {
"DefaultRetention": { "Mode": "COMPLIANCE", "Days": 10 }}}' --endpoint
-url https://s3.company.com
```

- Verificare lo stato di conservazione

```
aws s3api get-object-lock-configuration --bucket <bucket> --endpoint-url
https://s3.company.com
```

```
{
    "ObjectLockConfiguration": {
        "ObjectLockEnabled": "Enabled",
        "Rule": {
            "DefaultRetention": {
                "Mode": "COMPLIANCE",
                "Days": 10
            }
        }
    }
}
```

- Metti un oggetto nel bucket

```
aws s3api put-object --bucket <bucket> --key <file> --body "file"
--endpoint-url https://s3.example.com
```

- La durata di conservazione impostata sul bucket viene convertita in un indicatore data e ora di conservazione sull'oggetto.

```
aws s3api get-object-retention --bucket <bucket> --key <file> --endpoint
-url https://s3.company.com
```

```
{
    "Retention": {
        "Mode": "COMPLIANCE",
        "RetainUntilDate": "2022-03-02T15:22:47.202000+00:00"
    }
}
```

Verificare l'eliminazione di un oggetto con una conservazione definita

Il blocco degli oggetti si basa sul controllo delle versioni. La conservazione viene definita su una versione dell'oggetto. Se si tenta di eliminare un oggetto con una conservazione definita e non viene specificata alcuna versione, viene creato un indicatore di eliminazione come versione corrente dell'oggetto.

- Eliminare l'oggetto con la conservazione definita

```
aws s3api delete-object --bucket <bucket> --key <file> --endpoint-url
https://s3.example.com
```

- Elencare gli oggetti nel bucket

```
aws s3api list-objects --bucket <bucket> --endpoint-url
https://s3.example.com
```

  - Notare che l'oggetto non è elencato.
- Elencare le versioni per visualizzare il marker di eliminazione e la versione originale bloccata

```
aws s3api list-object-versions --bucket <bucket> --prefix <file>
--endpoint-url https://s3.example.com
```

```
{
    "Versions": [
        {
            "ETag": "\"82e8bfb872e778a4687a26e6c0b36bc1\"",
            "Size": 47,
            "StorageClass": "STANDARD",
            "Key": "file.txt",
            "VersionId":
"RDVDMjYwMTQtQkNDQS0xMUVDLThGOEUtNjQ3NTAwQzAxQTk1",
            "IsLatest": false,
            "LastModified": "2022-04-15T14:46:29.734000+00:00",
            "Owner": {
                "DisplayName": "Tenant01",
                "ID": "566223993089512949 26"
            }
        }
    ],
    "DeleteMarkers": [
        {
            "Owner": {
                "DisplayName": "Tenant01",
                "ID": "566223993089512949 26"
            },
            "Key": "file01.txt",
            "VersionId":
"QjVDQzgzOTAtQ0FGNi0xMUVDLThFMzgtQ0RGMjAwQjk0MjM1",
            "IsLatest": true,
            "LastModified": "2022-05-03T15:35:50.248000+00:00"
        }
    ]
}
```

- Eliminare la versione bloccata dell'oggetto

```
aws s3api delete-object  --bucket <bucket> --key <file> --version-id
"<VersionId>" --endpoint-url https://s3.example.com
```

```
An error occurred (AccessDenied) when calling the DeleteObject
operation: Access Denied
```

Di Aron Klein

Esempio di policy di bucket e di gruppo (IAM)

Di seguito sono riportati alcuni esempi di policy bucket e di policy di gruppo (policy IAM).

Policy di gruppo (IAM)

Accesso bucket stile home directory

Questo criterio di gruppo consente solo agli utenti di accedere agli oggetti nel bucket denominato username.

```
"Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::home",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::home/?/?/${aws:username}/*"
    }

  ]
}
```

Negare la creazione del bucket di blocco degli oggetti

Questo criterio di gruppo limiterà gli utenti a creare un bucket con il blocco degli oggetti attivato nel bucket.

> Questo criterio non viene applicato nell'interfaccia utente di StorageGRID, ma viene applicato solo dall'API S3.

```
{
    "Statement": [
        {
            "Action": "s3:*",
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Action": [
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutBucketVersioning"
            ],
            "Effect": "Deny",
            "Resource": "arn:aws:s3:::*"
        }
    ]
}
```

Limite di conservazione del blocco degli oggetti

Questa policy di bucket limiterà la durata della conservazione del blocco oggetto a 10 giorni o meno

```
{
 "Version":"2012-10-17",
 "Id":"CustSetRetentionLimits",
 "Statement": [
   {
    "Sid":"CustSetRetentionPeriod",
    "Effect":"Deny",
    "Principal":"*",
    "Action": [
      "s3:PutObjectRetention"
    ],
    "Resource":"arn:aws:s3:::testlock-01/*",
    "Condition": {
      "NumericGreaterThan": {
        "s3:object-lock-remaining-retention-days":"10"
      }
    }
   }
  ]
}
```

Impedire agli utenti di eliminare gli oggetti in base all'ID versione

Questo criterio di gruppo limita l'eliminazione degli oggetti con versione in base all'ID versione

```
{
    "Statement": [
        {
            "Action": [
                "s3:DeleteObjectVersion"
            ],
            "Effect": "Deny",
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Action": "s3:*",
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::*"
        }
    ]
}
```

Questo criterio bucket limiterà un utente (identificato dall'ID utente "56622399308951294926") a eliminare gli oggetti con versione in base all'ID versione

```
{
  "Statement": [
    {
      "Action": [
        "s3:DeleteObjectVersion"
      ],
      "Effect": "Deny",
      "Resource": "arn:aws:s3:::verdeny/*",
      "Principal": {
        "AWS": [
          "56622399308951294926"
        ]
      }
    },
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::verdeny/*",
      "Principal": {
        "AWS": [
          "56622399308951294926"
        ]
      }
    }
  ]
}
```

Limitare il bucket a un singolo utente con accesso in sola lettura

Questo criterio consente a un singolo utente di avere accesso in sola lettura a un bucket e nega esplicitamente l'accesso a tutti gli altri utenti. Il raggruppamento delle istruzioni Nega in cima alla policy è una buona pratica per una valutazione più rapida.

```
{
    "Statement": [
        {
            "Sid": "Deny non user1",
            "Effect": "Deny",
            "NotPrincipal": {
                "AWS":
"urn:sgws:identity::34921514133002833665:user/user1"
            },
            "Action": [
                "s3:*"
            ],
            "Resource": [
                "urn:sgws:s3:::bucket1",
                "urn:sgws:s3:::bucket1/*"
            ]
        },
        {
            "Sid": "Allow user1 read access to bucket bucket1",
            "Effect": "Allow",
            "Principal": {
                "AWS":
"urn:sgws:identity::34921514133002833665:user/user1"
            },
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "urn:sgws:s3:::bucket1",
                "urn:sgws:s3:::bucket1/*"
            ]
        }
    ]
}
```

Limitare un gruppo a una singola sottodirectory (prefisso) con accesso in sola lettura

Questo criterio consente ai membri del gruppo di accedere in sola lettura a una sottodirectory (prefisso) all'interno di un bucket. Il nome del bucket è "studio" e la sottodirectory è "study01".

```
{
    "Statement": [
        {
            "Sid": "AllowUserToSeeBucketListInTheConsole",
```

```
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::*"
            ]
        },
        {
            "Sid": "AllowRootAndstudyListingOfBucket",
            "Action": [
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3::: study"
            ],
            "Condition": {
                "StringEquals": {
                    "s3:prefix": [
                        "",
                        "study01/"
                    ],
                    "s3:delimiter": [
                        "/"
                    ]
                }
            }
        },
        {
            "Sid": "AllowListingOfstudy01",
            "Action": [
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::study"
            ],
            "Condition": {
                "StringLike": {
                    "s3:prefix": [
                        "study01/*"
                    ]
                }
            }
        },
```

```
        {
            "Sid": "AllowAllS3ActionsInstudy01Folder",
            "Effect": "Allow",
            "Action": [
                "s3:Getobject"
            ],
            "Resource": [
                "arn:aws:s3:::study/study01/*"
            ]
        }
    ]
}
```

Report tecnici

NetApp StorageGRID e analisi dei big data

Casi d’utilizzo di NetApp StorageGRID

La soluzione di storage a oggetti NetApp StorageGRID offre scalabilità, disponibilità dei dati, sicurezza e performance elevate. Le organizzazioni di ogni dimensione e settore utilizzano StorageGRID S3 per un’ampia gamma di casi d’utilizzo. Analizziamo alcuni scenari tipici:

Analisi dei big data: StorageGRID S3 viene spesso utilizzato come data Lake, dove le aziende memorizzano grandi quantità di dati strutturati e non strutturati per l’analisi utilizzando strumenti come Apache Spark, Splunk Smartstore e Dremio.

Tiering dati: i clienti NetApp utilizzano la funzionalità FabricPool di ONTAP per spostare automaticamente i dati tra un Tier locale ad alte prestazioni in StorageGRID. Il tiering libera il costoso storage flash per i dati hot, mantenendo i dati cold altamente disponibili su storage a oggetti a basso costo. Ciò massimizza performance e risparmi.

Backup dei dati e ripristino di emergenza: le aziende possono utilizzare StorageGRID S3 come soluzione affidabile e conveniente per il backup dei dati critici e il ripristino in caso di emergenza.

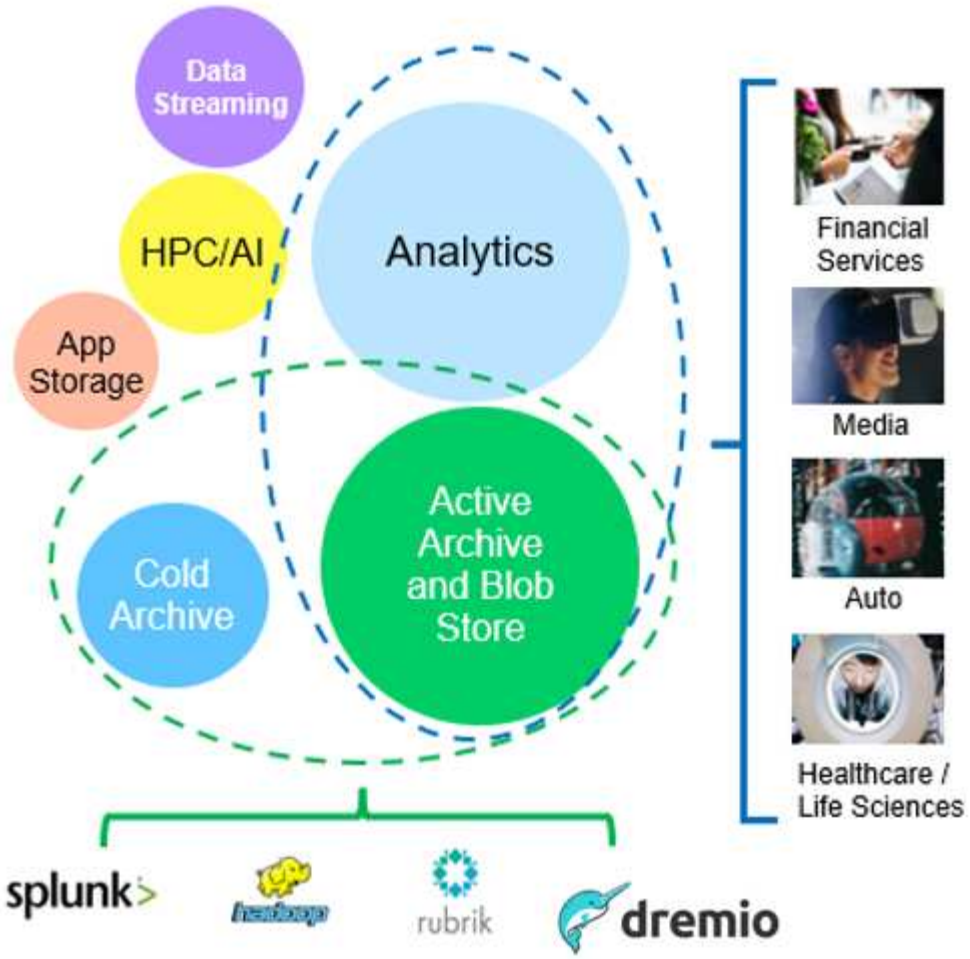
Archiviazione dei dati per le applicazioni: StorageGRID S3 può essere utilizzato come backend di archiviazione per le applicazioni, consentendo agli sviluppatori di archiviare e recuperare facilmente file, immagini, video e altri tipi di dati.

Distribuzione dei contenuti: StorageGRID S3 può essere utilizzato per archiviare e distribuire contenuti statici di siti web, file multimediali e download di software agli utenti di tutto il mondo, sfruttando la distribuzione geografica e lo spazio dei nomi globale di StorageGRID per una distribuzione dei contenuti rapida e affidabile.

Tiering dati: i clienti NetApp utilizzano la funzionalità ONTAP FabricPool per spostare automaticamente i dati tra un livello locale ad alte prestazioni in StorageGRID. Il tiering libera il costoso storage flash per i dati hot, mantenendo i dati cold altamente disponibili mediante lo storage a oggetti a costo contenuto. Ciò massimizza performance e risparmi.

Archivio dati: StorageGRID offre diversi tipi di storage e supporta il tiering in opzioni di storage pubblico a lungo termine a basso costo, rendendolo una soluzione ideale per l’archiviazione e la conservazione a lungo termine dei dati che devono essere conservati per scopi di conformità o cronologici.

Casi di utilizzo dello storage a oggetti

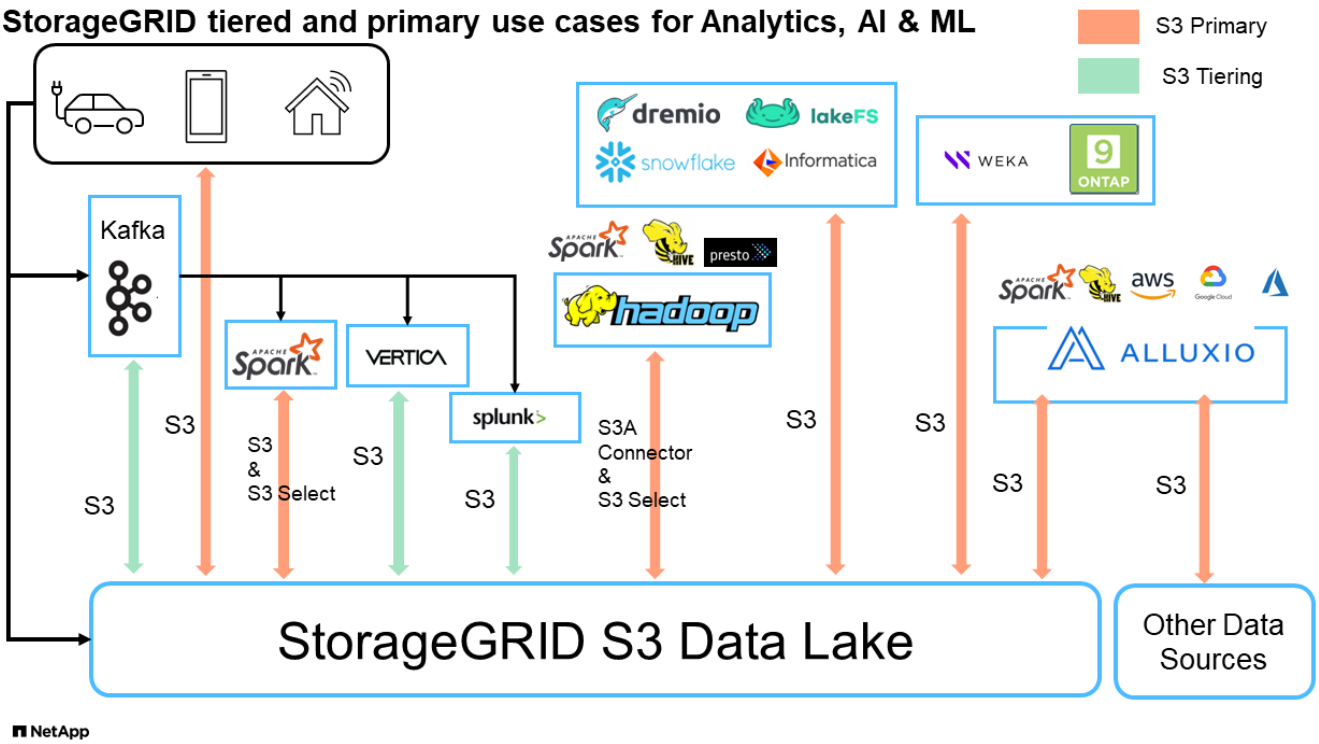


Tra questi, l'analisi dei big data è uno dei casi di utilizzo più importanti e l'andamento del suo utilizzo sta aumentando.

Perché scegliere StorageGRID per i data Lake?

- Maggiore collaborazione - massiccia condivisione multi-sito, multi-tenancy con accesso API standard del settore
- Costi operativi ridotti: Semplicità operativa di una singola architettura scale-out automatizzata con riparazione automatica
- Scalabilità: Diversamente dalle tradizionali soluzioni Hadoop e data warehouse, lo storage a oggetti StorageGRID S3 separa lo storage dalle risorse di calcolo e dai dati, consentendo al business di scalare le proprie esigenze di storage man mano che crescono.
- Durata e affidabilità: I StorageGRID offrono una durata del 99,999999999%, il che significa che i dati memorizzati sono altamente resistenti alla perdita di dati. Inoltre, offre un'elevata disponibilità per garantire che i dati siano sempre accessibili.
- Sicurezza: StorageGRID offre varie funzionalità di sicurezza, tra cui crittografia, policy per il controllo degli accessi, gestione del ciclo di vita dei dati, blocco degli oggetti e versioni per proteggere i dati archiviati in bucket S3

StorageGRID S3 Data Lake



Quale data warehouse o data Lake funziona meglio con lo storage a oggetti S3

NetApp ha messo a confronto StorageGRID con tre ecosistemi data warehouse/Lake house - Hive, Delta Lake e Dremio. "Apache Iceberg: La guida definitiva" include una breve introduzione di data warehouse e data lake house e pro/contro di queste due architetture.

- Strumento benchmark - TPC-DS - https://www.tpc.org/tpcds/
- Ecosistemi di big data
  - Cluster di 5 VM, ciascuna con 128G GB di RAM e 24 vCPU, storage SSD per disco di sistema
  - Hadoop 3.3.5 con Hive 3.1.3 (1 nodi nome + 4 nodi dati)
  - Delta Lake con Spark 3.2.0 (1 master + 4 dipendenti) e Hadoop 3.3.5
  - Dremio V23 (1 master + 4 esecutori)
- Storage a oggetti
  - NetApp® StorageGRID^® 11,6 con bilanciamento del carico 3 x SG6060 + 1x SG1000
  - Protezione degli oggetti - 2 copie
- Dimensioni del database 1000GB
- Cache disabilitata in tutti gli ecosistemi 3 per ottenere risultati coerenti per ogni test di query.

TPC-DS include 99 query SQL complesse per l'analisi comparativa delle query. Abbiamo misurato i minuti totali per completare tutte e 99 le query e ci siamo accorti di aver suddiviso il tipo e il numero di richieste S3 per analizzare il risultato. La prima tabella riportata di seguito mostra la durata totale di tutte le 99 query e la seconda tabella riassume il numero e i tipi di richieste S3 inviate a StorageGRID da ciascun ecosistema.

Risultato query TPC-DS

Ecosistema	Alveare	Lago Delta	Dremio
Layer di storage	NetApp® StorageGRID^®	NetApp® StorageGRID^®	NetApp® StorageGRID^®
Tipo di disco	DISCO RIGIDO	DISCO RIGIDO	DISCO RIGIDO
Formato tabella	Parquet	Parquet	Parquet [1]
Dimensione del database	1000G	1000G	1000G
TPCDS 99 query minuti totali	1084 [2]	55	47

[1] ha testato sia il formato della tabella Parquet che Iceberg, il risultato è simile.

[2] Impossibile completare la query numero 72.

Query TPC-DS - S3 richieste di disaggregazione

S3 richieste	Alveare	Lago Delta	Dremio
OTTIENI	1.117.184	2.074.610	4.414.227
osservazione: Tutta la gamma	80% range get di 2KB a 2MB da 32MB oggetti, 50 - 100 richieste/sec	Il range del 73% è inferiore a 100KB da 32MB oggetti, 1000 - 1400 richieste/sec	90% 1M byte range get from 256MB objects, 2000 - 2300 requests/sec
Elenca oggetti	312.053	24.158	240
TESTA (oggetto inesistente)	156.027	12.103	192
TESTA (oggetto esistente)	982.126	922.732	1.845
Richieste totali	2.567.390	3.033.603	4.416.504

Dalla prima tavola, possiamo vedere Delta Lago e Dremio sono molto più veloce di Hive. Dalla seconda tabella, si nota che Hive ha inviato molte S3 richieste list-objects, che in genere sono lente in tutte le piattaforme di storage a oggetti, soprattutto se si tratta di un bucket contenente molti oggetti. Ciò aumenta notevolmente la durata complessiva delle query. Un'altra osservazione è stata Dremio in grado di inviare un elevato numero di richieste GET in parallelo, da 2.000 a 2.300 richieste al secondo contro 50 - 100 richieste al secondo in Hive. Il file system hive e Hadoop S3A mimico standard contribuisce alla lentezza di Hive nello storage a oggetti S3.

L'utilizzo di Hadoop (su storage a oggetti HDFS o S3) con Hive o Spark richiede un'estesa conoscenza di Hadoop e Hive/Spark e del modo in cui interagiscono le impostazioni di ogni servizio, insieme hanno più di 1000 impostazioni. Molto spesso, le impostazioni sono correlate e non possono essere modificate da sole. Per trovare la combinazione ottimale di impostazioni e valori da utilizzare sono necessari tempi e sforzi enormi.

Dremio è un motore di data Lake che utilizza Apache Arrow end-to-end per aumentare drasticamente le prestazioni delle query. Apache Arrow fornisce un formato di memoria colonnare standardizzato per una condivisione dei dati efficiente e analisi rapide. Arrow adotta un approccio indipendente dal linguaggio, progettato per eliminare la necessità di serializzazione e deserializzazione dei dati, migliorando le prestazioni e l'interoperabilità tra sistemi e processi di dati complessi.

Le prestazioni di Dremio dipendono principalmente dalla potenza di elaborazione del cluster Dremio. Sebbene

Dremio utilizzi il connettore S3A di Hadoop per la connessione di storage a oggetti S3, Hadoop non è richiesto e la maggior parte delle impostazioni fs.S3A di Hadoop non sono utilizzate da Dremio. Ciò semplifica l'ottimizzazione delle prestazioni di Dremio senza dedicare tempo ad apprendere e testare varie impostazioni di Hadoop S3A.

Dai risultati di questo benchmark, possiamo concludere che il sistema di analisi dei big data ottimizzato per carichi di lavoro basati su S3 è un fattore importante per le performance. Dremio ottimizza l'esecuzione delle query, utilizza in modo efficiente i metadati e fornisce un accesso senza problemi ai dati S3, garantendo prestazioni migliori rispetto a Hive quando si utilizza lo storage S3. Fare riferimento a questo "pagina" Per configurare l'origine dati Dremio S3 con StorageGRID.

Visita i collegamenti riportati di seguito per scoprire come StorageGRID e Dremio collaborano per fornire un'infrastruttura di data Lake moderna ed efficiente e come NetApp è passata da Hive + HDFS a Dremio + StorageGRID per migliorare in modo significativo l'efficienza dell'analisi dei big data.

- "Migliora le performance dei tuoi big data con NetApp StorageGRID"
- "Infrastruttura di data Lake moderna, potente ed efficiente con StorageGRID e Dremio"
- "In che modo NetApp sta ridefinendo l'esperienza del cliente con l'analisi dei prodotti"

Tuning di Hadoop S3A

Il connettore Hadoop S3A facilita un'interazione perfetta tra le applicazioni basate su Hadoop e lo storage a oggetti S3. La messa a punto del connettore Hadoop S3A è essenziale per ottimizzare le performance quando si lavora con lo storage a oggetti S3. Prima di entrare nei dettagli di messa a punto, cerchiamo di comprendere di base Hadoop e i suoi componenti.

Che cos'è Hadoop?

Hadoop è un potente framework open-source progettato per gestire l'elaborazione e lo storage di dati su larga scala. Permette lo storage distribuito e l'elaborazione parallela tra cluster di computer.

I tre componenti principali di Hadoop sono:

- **Hadoop HDFS (Hadoop Distributed file System)**: Gestisce lo storage, suddividendo i dati in blocchi e distribuendoli tra i nodi.
- **Hadoop MapReduce**: Responsabile dell'elaborazione dei dati dividendo le attività in blocchi più piccoli ed eseguendole in parallelo.
- **Hadoop YARN (Yet Another Resource negoziator):** "Gestisce le risorse e pianifica le attività in modo efficiente"

HDFS Hadoop e connettore S3A

HDFS è una componente vitale dell'ecosistema Hadoop, ricoprendo un ruolo critico nell'efficiente elaborazione dei big data. HDFS consente storage e gestione affidabili. Garantisce l'elaborazione parallela e lo storage dei dati ottimizzato, accelerando l'accesso e l'analisi dei dati.

Nell'elaborazione dei big data, HDFS è eccellente per fornire storage con tolleranza di errore per grandi set di dati. Ottiene questo attraverso la replica dei dati. Consente di memorizzare e gestire grandi volumi di dati strutturati e non strutturati in un ambiente di data warehouse. Inoltre, si integra perfettamente con i principali framework di elaborazione dei big data, come Apache Spark, Hive, Pig e Flink, consentendo un'elaborazione dei dati scalabile ed efficiente. È compatibile con i sistemi operativi basati su Unix (Linux), il che lo rende la scelta ideale per le organizzazioni che preferiscono utilizzare ambienti basati su Linux per l'elaborazione dei

big data.

Con la crescita del volume dei dati nel tempo, l'approccio all'aggiunta di nuove macchine al cluster Hadoop con risorse di calcolo e storage proprie è diventato inefficiente. La scalabilità lineare crea delle sfide per l'utilizzo efficiente delle risorse e la gestione dell'infrastruttura.

Per affrontare queste sfide, il connettore Hadoop S3A offre i/o dalle performance elevate rispetto allo storage a oggetti S3. L'implementazione di un workflow Hadoop con S3A consente di sfruttare lo storage a oggetti come repository di dati e consente di separare calcolo e storage, il che consente di scalare calcolo e storage in modo indipendente. Il disaccoppiamento tra calcolo e storage ti consente inoltre di dedicare la giusta quantità di risorse per i tuoi job di calcolo e di fornire capacità in base alle dimensioni del set di dati. Pertanto, è possibile ridurre il TCO complessivo per i flussi di lavoro Hadoop.

Tuning del connettore Hadoop S3A

S3 si comporta in modo diverso da HDFS e alcuni tentativi di preservare l'aspetto di un file system sono decisamente non ottimali. È necessario un'accurata messa a punto/test/sperimentazione per utilizzare al meglio le risorse S3.

Le opzioni Hadoop di questo documento si basano su Hadoop 3,3.5, fare riferimento a. "Hadoop 3.3.5 core-site.xml" per tutte le opzioni disponibili.

Nota – il valore predefinito di alcune impostazioni di Hadoop fs.S3A è diverso in ogni versione di Hadoop. Assicurati di controllare il valore predefinito specifico per la tua attuale versione di Hadoop. Se queste impostazioni non sono specificate in Hadoop core-site.xml, verrà utilizzato il valore predefinito. È possibile ignorare il valore in fase di esecuzione utilizzando le opzioni di configurazione Spark o Hive.

Dovete andare a questo "Pagina di Apache Hadoop" per capire ogni opzione fs.s3a. Se possibile, testarle in un cluster Hadoop non di produzione per trovare i valori ottimali.

Si dovrebbe leggere "Ottimizzazione delle prestazioni quando si lavora con il connettore S3A" per altre raccomandazioni di sintonizzazione.

Analizziamo alcune considerazioni chiave:

1. Compressione dati

Non attivare la compressione StorageGRID. La maggior parte dei sistemi di big data utilizza la funzione GET della gamma di byte invece di recuperare l'intero oggetto. L'utilizzo dell'intervallo di byte Get con gli oggetti compressi riduce significativamente le prestazioni di GET.

2. S3A committer

In generale, si raccomanda il committer Magic S3A. Fare riferimento a questo "Pagina delle opzioni comuni di committer S3A" per avere una migliore comprensione di magic committer e delle relative impostazioni s3a.

Magic Committer:

Magic Committer si affida specificamente a S3Guard per offrire elenchi di directory coerenti sull'archivio di oggetti S3.

Con S3 coerente (che è ora il caso), il Magic Committer può essere utilizzato in modo sicuro con qualsiasi secchio S3.

Scelta e sperimentazione:

A seconda del caso d'uso, è possibile scegliere tra il committer di staging (che si basa su un filesystem HDFS del cluster) e il committer magico.

Sperimenta entrambi per determinare la soluzione più adatta al tuo carico di lavoro e ai requisiti.

In sintesi, i S3A committer forniscono una soluzione alla sfida fondamentale di un impegno coerente, ad alte prestazioni e affidabile nei confronti del S3. Il design interno garantisce un trasferimento efficiente dei dati, mantenendo al contempo l'integrità dei dati.

Option	Meaning	Default (Hadoop 3.3.5)
fs.s3a.committer.name	Committer to create for output to S3A, one of: "file", "directory", "partitioned", "magic".	file
fs.s3a.buffer.dir	Local filesystem directory for data being written and/or staged.	${env.LOCAL_DIRS:-${hadoop.tmp.dir}}/s3a
fs.s3a.committer.magic.enabled	Enable "magic committer" support in the filesystem.	true
fs.s3a.committer.abort.pending.uploads	list and abort all pending uploads under the destination path when the job is committed or aborted.	true
fs.s3a.committer.threads	Number of threads in committers for parallel operations on files.	8
fs.s3a.committer.generate.uuid	Generate a Job UUID if none is passed down from Spark	false
fs.s3a.committer.require.uuid	Require the Job UUID to be passed down from Spark	false
mapreduce.fileoutputcommitter.marksuccessfuljobs	Write a _SUCCESS file on the successful completion of the job.	true
mapreduce.outputcommitter.factory.scheme.s3a	The committer factory to use when writing data to S3A filesystems. If mapreduce.outputcommitter.factory.class is set, it will override this property. (This property is set in mapred-default.xml)	org.apache.hadoop.fs.s3a.commit.S3ACommitterFactory

3. Filettatura, dimensioni pool di connessione e dimensione blocco

- Ogni client **S3A** che interagisce con un singolo bucket ha un proprio pool dedicato di connessioni HTTP 1,1 aperte e thread per operazioni di upload e copia.
- "È possibile ottimizzare le dimensioni di questi pool per ottenere un equilibrio tra prestazioni e utilizzo di memoria/thread".
- Quando si caricano i dati su S3, questi vengono divisi in blocchi. La dimensione predefinita del blocco è 32 MB. È possibile personalizzare questo valore impostando la proprietà fs.S3A.block.size.
- Blocchi di dimensioni maggiori possono migliorare le performance per il caricamento di grandi dati, riducendo l'overhead di gestione di parti multiparte durante il caricamento. Il valore consigliato è pari o superiore a 256 MB per set di dati di grandi dimensioni.

Option	Meaning	Default (Hadoop 3.3.5)
fs.s3a.threads.max	The total number of threads available in the filesystem for data uploads *or any other queued filesystem operation*.	64
fs.s3a.connection.maximum	Controls the maximum number of simultaneous connections to S3. This must be bigger than the value of fs.s3a.threads.max so as to stop threads being blocked waiting for new HTTPS connections. Why not equal? The AWS SDK transfer manager also uses these connections.	96
fs.s3a.max.total.tasks	The number of operations which can be queued for execution. This is in addition to the number of active threads in fs.s3a.threads.max.	32
fs.s3a.committer.threads	Number of threads in committers for parallel operations on files (upload, commit, abort, delete...)	8
fs.s3a.executor.capacity	The maximum number of submitted tasks which is a single operation (e.g. rename(), delete()) may submit simultaneously for execution -excluding the IO-heavy block uploads, whose capacity is set in "fs.s3a.fast.upload.active.blocks" All tasks are submitted to the shared thread pool whose size is set in "fs.s3a.threads.max"; the value of capacity should be less than that of the thread pool itself, as the goal is to stop a single operation from overloading that thread pool.	16
fs.s3a.fast.upload.active.blocks (see also related fs.s3a.fast.upload.buffer option)	Maximum Number of blocks a single output stream can have active (uploading, or queued to the central FileSystem instance's pool of queued operations. This stops a single stream overloading the shared thread pool.	4
fs.s3a.block.size	Block size to use when reading files using s3a: file system. A suffix from the set {K,M,G,T,P} may be used to scale the numeric value.	32MB (tested 1TB data set with 256MB and 512MB block size shows significant improvement in both read and write)

4. Caricamento multiparte

S3A committer **Always** utilizza MPU (upload multiparte) per caricare i dati nel bucket S3. Ciò è necessario per consentire: Errore di attività, esecuzione speculativa di attività e interruzione di processi prima del commit. Di seguito sono riportate alcune specifiche chiave relative ai caricamenti di più parti:

- Dimensioni massime oggetto: 5 TiB (terabyte).
- Numero massimo di parti per caricamento: 10.000.
- Numeri di parte: Da 1 a 10.000 (inclusi).
- Dimensioni del pezzo: Tra 5 MIB e 5 GiB. In particolare, non esiste un limite minimo di dimensioni per l'ultima parte del caricamento multiparte.

L'utilizzo di una parte di dimensioni inferiori per i caricamenti multiparte S3 presenta vantaggi e svantaggi.

Vantaggi:

- Ripristino rapido da problemi di rete: Quando si caricano parti più piccole, l'impatto del riavvio di un caricamento non riuscito a causa di un errore di rete viene ridotto al minimo. Se una parte non riesce, è sufficiente caricare nuovamente quella parte specifica piuttosto che l'intero oggetto.

- Migliore parallelizzazione: È possibile caricare più parti in parallelo, sfruttando il multithreading o le connessioni simultanee. Questa parallelizzazione migliora le prestazioni, soprattutto quando si gestiscono file di grandi dimensioni.

Svantaggio:

- Sovraccarico di rete: Le dimensioni ridotte delle parti consentono il caricamento di più parti, ciascuna delle quali richiede una propria richiesta HTTP. Un numero maggiore di richieste HTTP aumenta l'overhead dovuto all'avvio e al completamento di singole richieste. La gestione di un gran numero di piccoli componenti può influire sulle prestazioni.
- Complessità: Gestire l'ordine, tenere traccia delle parti e assicurarsi che i caricamenti vengano effettuati correttamente può risultare difficoltoso. Se il caricamento deve essere interrotto, tutte le parti già caricate devono essere monitorate e eliminate.

Per Hadoop, per fs.S3A.multipart.size si consigliano dimensioni di parte pari o superiori a 256MB. Impostare sempre il valore fs.S3A.mutlipart.threshold su 2 x fs.S3A.multipart.size. Ad esempio, se fs.S3A.multipart.size = 256M, fs.S3A.mutlipart.threshold dovrebbe essere 512M.

Utilizzare parti di dimensioni maggiori per set di dati di grandi dimensioni. È importante scegliere una dimensione della parte che bilanci questi fattori in base al caso di utilizzo specifico e alle condizioni di rete.

Un caricamento multiparte è un "processo in tre fasi":

1. Il caricamento viene avviato, StorageGRID restituisce un ID upload.
2. Le parti dell'oggetto vengono caricate utilizzando l'ID upload.
3. Una volta caricate tutte le parti dell'oggetto, invia la richiesta di caricamento multiparte completa con upload-ID. StorageGRID costruisce l'oggetto dalle parti caricate e il client può accedere all'oggetto.

Se la richiesta di caricamento multiparte completa non viene inviata correttamente, le parti rimangono in StorageGRID e non creano alcun oggetto. Ciò si verifica quando i lavori vengono interrotti, non riusciti o interrotti. Le parti rimangono nella griglia fino a quando il caricamento multiparte non viene completato o interrotto o StorageGRID elimina queste parti se sono trascorsi 15 giorni dall'avvio del caricamento. Se in un bucket sono presenti molti (da poche centinaia di migliaia a milioni) upload multiparte in corso, quando Hadoop invia "list-multipart-Uploads" (questa richiesta non filtra per id di caricamento), il completamento della richiesta potrebbe richiedere molto tempo o un timeout. È possibile impostare fs.S3A.mutlipart.purge su true con un valore fs.S3A.multipart.purge.age appropriato (ad esempio, da 5 a 7 giorni, non utilizzare il valore predefinito di 86400, ossia 1 giorno). O contattare l'assistenza NetApp per esaminare la situazione.

Option	Meaning	Default (Hadoop 3.3.5)
fs.s3a.multipart.size	How big (in bytes) to split upload or copy operations up into. A suffix from the set {K,M,G,T,P} may be used to scale the numeric value.	64M
fs.s3a.multipart.threshold	How big (in bytes) to split upload or copy operations up into. This also controls the partition size in renamed files, as rename() involves copying the source file(s). A suffix from the set {K,M,G,T,P} may be used to scale the numeric value.	128M
fs.s3a.multipart.purge	True if you want to purge existing multipart uploads that may not have been completed/aborted correctly. The corresponding purge age is defined in fs.s3a.multipart.purge.age. If set, when the filesystem is instantiated then all outstanding uploads older than the purge age will be terminated -across the entire bucket. This will impact multipart uploads by other applications and users. so should be used sparingly, with an age value chosen to stop failed uploads, without breaking ongoing operations.	false
fs.s3a.multipart.purge.age	Minimum age in seconds of multipart uploads to purge on startup if "fs.s3a.multipart.purge" is true	86400

5. Buffer: Scrittura dei dati in memoria

Per migliorare le prestazioni, è possibile inserire i dati in scrittura nella memoria prima di caricarli su S3. Riducendo così il numero di scritture ridotte e migliorando l'efficienza.

Option	Meaning	Default (Hadoop 3.3.5)
fs.s3a.fast.upload.buffer	The buffering mechanism to for data being written. Values: disk, array, bytebuffer. "disk" will use the directories listed in fs.s3a.buffer.dir as the location(s) to save data prior to being uploaded. "array" uses arrays in the JVM heap "bytebuffer" uses off-heap memory within the JVM. Both "array" and "bytebuffer" will consume memory in a single stream up to the number of blocks set by: fs.s3a.multipart.size * fs.s3a.fast.upload.active.blocks. If using either of these mechanisms, keep this value low The total number of threads performing work across all threads is set by fs.s3a.threads.max, with fs.s3a.max.total.tasks values setting the number of queued work items.	disk

Ricorda che S3 e HDFS funzionano in modi diversi. È necessario un'attenta messa a punto/test/esperimento

per utilizzare al meglio le risorse S3.

Blog di NetApp StorageGRID

Puoi trovare alcuni fantastici blog su NetApp StorageGRID qui:

- 10 maggio: "Il laboratorio on-demand è il tuo miglior tool di vendita per StorageGRID"
- 24 maggio: "Modernizza i carichi di lavoro di analisi con NetApp e Alluxio"
- 26 maggio: "StorageGRID: Memorizzazione e gestione dei dati di replica e backup on-premise"
- 9 giugno: "USA il connettore S3A di Cloudera Hadoop con StorageGRID"
- 26 luglio: "Consulta l'elenco in continua crescita di soluzioni validate dei partner per StorageGRID"
- 5 agosto: "NetApp StorageGRID ottiene la certificazione Common Criteria Security"
- 16 agosto: "Integrazione di StorageGRID con lo stack ELK open-source per migliorare l'esperienza del cliente"
- 17 agosto: "Tutto inizia con il blocco degli oggetti… Creazione di un ecosistema di storage S3 per le applicazioni di backup critiche"
- 23 agosto: "Costruisci il tuo data Lake su StorageGRID"
- 1 settembre: "Prendi queste metriche e Graph it"
- 19 settembre: "Supporto di protezione DataLock e ransomware per StorageGRID"
- 26 settembre: "NetApp StorageGRID per service provider"
- 5 ottobre: "Defrost dei dati su StorageGRID per Snowflake"
- 5 ottobre: "NetApp Cloud Insights aggiunge dashboard della galleria StorageGRID"
- 7 novembre: "Supporto di StorageGRID e ONTAP S3: Differenze, analogie e integrazione"
- 23 novembre: "Ai spiegabile con MLOPS basati su NetApp e Modzy"
- 6 dicembre: "StorageGRID ottiene la certificazione di conformità KPMG"
- Gennaio 16: "StorageGRID rinnova la certificazione di conformità NF203 e ISO/IEC 25051"
- Gennaio 18: "Blocco degli oggetti StorageGRID S3 validato per Veritas NetBackup"
- Febbraio 14: "Cosa hanno in comune cioccolato, sci, orologi e mainframe?"
- Marzo 14: "Come eseguire il backup dei database EHR di Epic Systems con un comando in un'architettura compatibile con 3:2:1"
- Marzo 30: "USA BlueXP per proteggere Epic EHR con una policy di backup conforme a 3:2:1"
- Marzo 30: "Punto di montaggio per Amazon S3 Alpha release con StorageGRID"
- 16 maggio: "Novità della famiglia di storage a oggetti StorageGRID"
- 16 maggio: "Introduzione di StorageGRID 11,7 e della nuova appliance di storage a oggetti all-flash SGF6112"
- 30 agosto: "Il punto di montaggio per Amazon S3 file System è ora GA"
- 1 settembre: "Utilizzo di Cloud Insights per monitorare e raccogliere i registri utilizzando Fluent bit"
- 17 ottobre: "Transizione da Hadoop: Modernizzazione dell'analisi dei dati con Dremio e StorageGRID"
- 7 novembre: "Ghiacciaio on-premise di Spectra Logic con StorageGRID"
- 12 dicembre: "Analisi dei big data su StorageGRID: Dremio esegue 23 volte più velocemente di Apache Hive"

- Febbraio 2: "Presentazione della descrizione della soluzione StorageGRID + LakeFS"
- Febbraio 16: "Presentazione di StorageGRID 11,8: Sicurezza, semplicità ed esperienza utente migliorate"
- Febbraio 16: "Presentazione di StorageGRID 11,8"

Documentazione di NetApp StorageGRID

La documentazione completa per ciascuna release di NetApp StorageGRID è disponibile qui:

- "Appliance StorageGRID"
- "StorageGRID 11,8"
- "StorageGRID 11.7"
- "StorageGRID 11.6"
- "StorageGRID 11.5"
- "StorageGRID 11.4"
- "StorageGRID 11.3"
- "StorageGRID 11.2"

Note legali

Le note legali forniscono l'accesso a dichiarazioni di copyright, marchi, brevetti e altro ancora.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marchi

NETAPP, il logo NETAPP e i marchi elencati nella pagina dei marchi NetApp sono marchi di NetApp, Inc. Altri nomi di società e prodotti potrebbero essere marchi dei rispettivi proprietari.

"https://www.netapp.com/company/legal/trademarks/"

Brevetti

Un elenco aggiornato dei brevetti di proprietà di NetApp è disponibile all'indirizzo:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Direttiva sulla privacy

"https://www.netapp.com/company/legal/privacy-policy/"

Open source

I file di avviso forniscono informazioni sul copyright e sulle licenze di terze parti utilizzate nel software NetApp.

https://library.netapp.com/ecm/ecm_download_file/2879263

https://library.netapp.com/ecm/ecm_download_file/2881511